VOLUME 5, 2011

ISACA® Journal

Governance, Tying Together the Three Lines of Defense

Featured articles:

IT Governance and the Cloud

IT General and Application Controls

The Impact of Governance on Identity Management Programs

And more...

ISACA®
Serving IT Governance Professionals

WWW.ISACA.ORG

Demonstrate your value without saying a word.

Résumés/CVs may *list* your experience and knowledge, but an ISACA® certification designation after your name *proves* it.

www.isaca.org/certification-journal

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

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

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

December Exam Date: 10 December 2011
Registration Deadline: 5 October 2011

ISACA®
Trust in, and value from, information systems

Volume 5, 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.

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 3 October 2011.

An Introduction to Information Security Management in Health Care Organizations
Haris Hamidovic, CIA, ISMS IA, ITIL-F, IT Project+, and Jasmina Kabil

Certification—The Answer to Cybersecurity Woes?
Derek Mohammed, Ph.D., CISA, CISSP, PMP

La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes
Jeimy J. Cano, Ph.D., CFE

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.

Discuss topics in the ISACA Knowledge Center: *www.isaca.org/knowledgecenter*

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

Join ISACA LinkedIn: ISACA (Official), *http://tinyurl.com/42vbrlz*

Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

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

The Train of Danger

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*.

Serious cyberattacks have been in the news quite a lot recently.[1] Large organizations in the United States, including Lockheed,[2] Google,[3] Citigroup[4] and the International Monetary Fund,[5] have all reported successful attempts perpetrated against them. Particularly discomforting was the attack on EMC Corp.'s RSA division, which was, in effect, a meta-attack in that what the hackers were reported to have stolen was security information related to the access control tokens used by millions of individuals around the world.[6]

BEYOND HACKING

By all indications, these are not examples of hacking, at least not as the term has been used for many years. The reported attacks were not attempted by mischievous teenagers seeking to create random damage just to show that they could do it. These were deliberate attacks with intent to cause some sort of harm. In some cases the motivation seems to have been monetary. In others, groups or individuals that are somehow aggrieved seem to have been seeking to exact revenge. Still others are said to be geopolitical in nature. There have even been incidents in which open military conflict was said to have included cyberwarfare.[7]

Allegations have also been made that cyberattacks were used as instruments of policy by one nation against another. The nation of Estonia was victimized so greatly that it found itself losing "the first war in cyberspace," described in *The New York Times* as "close to shutting down the country's digital infrastructure, clogging the web sites of the president, the prime minister, Parliament and other government agencies, staggering Estonia's biggest bank and overwhelming the sites of several daily newspapers."[8] The so-called Stuxnet worm was evidently aimed at Iran's nuclear program; "computer security specialists who have examined it were almost certain it had been created by a government and is a prime example of clandestine digital warfare."[9]

NOT REPORTED

In reading about these numerous examples of cyberwarfare in our times, I was struck by something I did *not* read. In many cases social networking services have been instrumental in what has become known as the Arab Spring, a wave of rebellions and outright revolutions across Northern Africa and the Mideast. For example, a Google executive in Egypt, Wael Ghonim, "was a quiet force behind the YouTube and Facebook campaigns that galvanized Egyptian protesters in January 2011"; when he was arrested during the uprising, "hundreds of Egyptians took to Twitter and the Internet, calling on him to become one of their new leaders."[10] It is, therefore, fair to say that many of those involved in the Egyptian events and those in other countries were computer-savvy. But, there have been no reports, of which I am aware, of cyberattacks on ruling governments (or rebels, for that matter). This startling omission leads to a train of possible conclusions that I find very disturbing, namely:

- **Maybe governments were attacked by rebels but did not report it.** If this did happen, I can understand why the governments in question would not want to publicize the fact that their systems were undermined by members of their civilian populations. But, I cannot understand why the rebels, especially those who have overthrown their rulers, would keep their exploits secret.
- **Cyberattacks are not easy to execute.** If people who are well versed in the use of computer systems have not been perpetrating such attacks as a component of their revolutionary activities, it probably is not as simple to pull off as one would believe reading the works of Steig Larsson.[11] These people in the Arab countries had more than enough incentive to undermine the systems of their countries' militaries and police forces. They had the motivation and opportunity, but apparently not the technical or intellectual means.

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.

- **Governments do have the skill to conduct cyberattacks.** Perhaps it would be more accurate to say that, as of now, only governments or organizations sponsored by governments have those skills. Therefore, if governments are actively developing these skills, they intend them to be a supplement to—or possibly a replacement for—their arsenals in full-scale shooting wars in the future.
- **Cyberattacks are not the moral equivalent of war; they *are* war.** This is not simply my opinion. General Kevin P. Chilton, the head of the US Strategic Command, told reporters that in the event of a cyberattack, "the law of armed conflict will apply," and warned that "I don't think you take anything off the table in considering a response. Why would we constrain ourselves?"[12]
- **Cyberattacks are a real, clear and present danger to many corporations and government agencies.** If it has happened, it can happen. The fact that there have been so many reported attacks on databases and web sites is indicative of the reality of the threat. The motivations of vandals are different from those of criminals, and those of warriors are very different from those of criminals. If it is governments or government-backed groups that are behind the wave of recently experienced attacks, the perpetrators are very motivated indeed, and may have the resources necessary to target the largest institutions.
- **Targeted organizations are unprepared for the dangerous train that is approaching.** The organizations that have publicly admitted to having been attacked are some of the largest and most sophisticated in the US, if not the world. They are aware of the sensitivity and criticality of their information resources and have taken extensive measures to protect them. And yet, their information resources were successfully penetrated. The type of hacking experienced in the past is substantively different from what these organizations may be facing today; this train is cannonballing down the track.
- **Security professionals are at risk.** On a personal level, if I follow this chain of conclusions to its logical end, I realize that those of us who deal with the security and control of information (and are represented among ISACA's membership) could be the targets of cyberattacks. Just as RSA was attacked to obtain the metadata of security, so the information security professionals of the world have a huge amount of sensitive information in their file drawers, their hard drives and their heads. It might be possible to piece together bits of information that would open their employers' databases to malicious misuse by those who have the wherewithal to make the most of it.

I said that the train of conclusions in this article was disturbing. It is particularly disturbing to realize that the last stop on that train is me and many people I know.

ENDNOTES

[1] This was written in June 2011. I'm certain there will be many more such reports by the time this is read.
[2] Drew, Christopher; "Stolen Data Is Tracked to Hacking at Lockheed," *The New York Times (NYT)*, 2 June 2011. *The New York Times* is often referred to as the US paper of record. Accordingly, where there is no primary source, I quote the *Times*. For this reason, there is a bit of an American perspective to the incidents cited, but it is also clear that this is not solely an American problem.
[3] Markoff, John; David Barboza; "F.B.I. to Investigate Gmail Attacks Said to Come From China," *NYT*, 2 June 2011
[4] Citigroup, "Updated Information on Recent Compromise to Citi Account Online for Our Customers," *www.citi.com/citi/press/2011/110610c.htm*
[5] Sanger, David E.; John Markoff; "I.M.F. Reports Cyberattack Led to 'Very Major Breach'," *NYT*, 11 June 2011
[6] RSA, "Open Letter to RSA SecurID Customers," *www.rsa.com/node.aspx?id=3891*
[7] Markoff, John; "Georgia Takes a Beating in the Cyberwar With Russia," *NYT*, 11 August 2008
[8] Landler, Mark; John Markoff; "Digital Fears Emerge After Data Siege in Estonia," *NYT*, 9 May 2007
[9] Markoff, John; "A Silent Attack, but Not a Subtle One," *NYT*, 26 September 2010
[10] "Wael Ghonim," Times Topics, *NYT*, 8 February 2011
[11] And, if you have not read his works, I am certainly not going to give away anything here.
[12] Sanger, David; Elisabeth Bumiller; "Pentagon to Consider Cyberattacks Acts of War," *NYT*, 31 May 2011

AUTHOR'S NOTE

As ever, I invite readers to send me e-mails at *stross@riskmastersinc.com* with any comments or questions on this column. There is also a comments tab on the Journal article pages of the ISACA web site (*www.isaca.org/journal*) where readers may enter comments. I promise to check this area regularly and respond to both sources of dialog with *Journal* readers.

Prepare for the **2011** CISA Exam

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 December 2011 exam, 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.*

The Three Lines of Defence Related to Risk Governance

Ken Doughty, CISA, CRISC, CBCP, is a senior manager, governance and transformation, at OnePath Australia (formerly ING Australia). He has more than 25 years of risk management experience gained from IT auditing, business continuity, project management, IT management and operational risk management in the public and private sectors. Doughty lectures part time at Macquarie University (Sydney, Australia) and has had a large number of papers (and a book) published in leading auditing, business continuity and enterprise risk management journals in the US. He is an internationally recognised speaker at seminars and conferences and has won a number of awards, including ISACA's 2002 International Best Speaker Award, itSMF Australia President's Medal for Best ITIL Project in 2003, and ISACA's 2006 Harold Weiss Award in recognition of his dedication to the IT governance profession.

Enterprise risk management (ERM) facilitates management's desire to effectively govern and manage the enterprise's approach to risk management and to create sustainable value to its stakeholders through business objectives such as capital growth (i.e., share value), increased dividend stream and satisfactory customer service. No enterprise operates in a risk-free environment, and implementation of ERM does not create such an environment. Rather, enterprises operate in environments filled with uncertainty, requiring proactive action to address risks in order to survive and prosper.

Effective ERM involves the strategic implementation of three lines of defence as the first principle of the risk management framework (refer to **figure 1**). At each line of defence there needs to be risk goverance guidance to support the ERM framework.

FIRST LINE OF DEFENCE

The first line of defence is the front-line employees who must understand their roles and responsibilities with regard to processing transactions and who must follow a systematic risk process (such as that documented in ISO 31000, see **figure 2**) and apply internal controls and other risk responses to treat the risks associated with those transactions.

Depending upon the size of the organisation, the enterprise's business unit (division) may have a risk management committee. This risk management committee is the first line of defence of the risk governance framework. This committee is empowered with the responsibility and accountability to effectively plan, build, run and monitor its department's day-to-day risk environment. The committee provides direction regarding risk response (i.e., treatment) for those risks that are outside of the business unit's risk tolerance.

Line management has the responsibility to identify and assess risks and to ensure that the control activities and other responses that treat risk are enforced and monitored for compliance. The information that line management should report to the business unit's risk management committee to enable it to achieve this objective includes:

- Risk footprint, heat map (critical and highly rated residual risks)
- Key risk issues, planned mitigation actions and person to act (PTA)
- Status of existing mitigation actions to mitigate risk
- Key risk indicators (red or amber)
- Control effectiveness indicators (red or amber)
- Incidents and breakages (including historical/trend analysis/statistics, status of mitigation actions and lessons learned)

Figure 1—Risk Management Three Lines of Defence

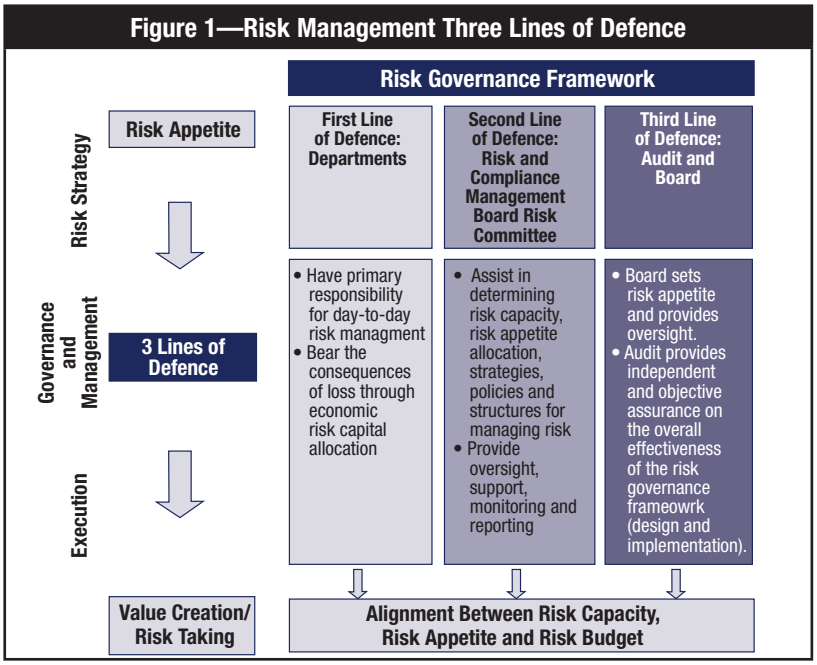
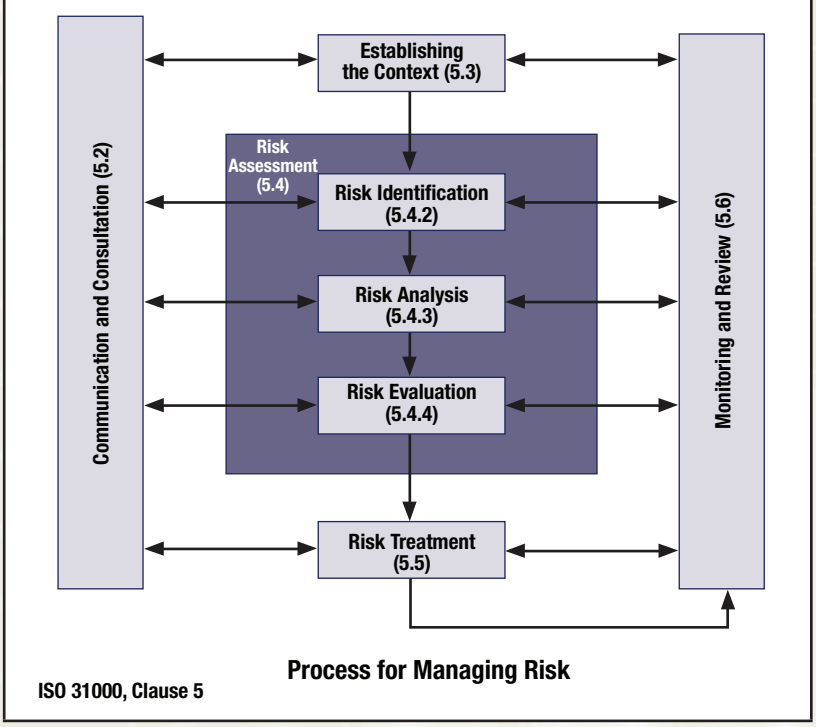


Figure 2—ISO 31000 Risk Process



ISO 31000, Clause 5

- Outstanding Sarbanes-Oxley-related deficiencies or internal/external audit items that are past their action due date

The risk report and minutes of the business unit's risk committee are forwarded to the enterprise risk management function for review. This information is then collated with other risk reports and assessed and reported, both independently and directly, to either the second- (executive risk committee) and/or third-line risk governance committees (board risk committee), who are charged with the role of representing the enterprise's stakeholders in respect to risk issues.

The second (risk and compliance) and third (audit) lines of defence often request the same information as the first-line management and governance committees. In practice, often this independently assessed risk information conveys a mixed message with the result that there is an arc of miscommunication, i.e., what is reported does not always align with the risk reality as perceived by front-line management. This difference in perspective is what adds value to the enterprise as a whole and to the ERM framework in particular. It is for the senior enterprise risk governance committee to evaluate the reports from these multiple sources and determine (or advise the main board on) the direction the enterprise should take.

SECOND LINE OF DEFENCE

The second line of defence is the enterprise's compliance and risk functions that provide independent oversight of the risk management activities of the first line of defence. The compliance and risk functions may have their own management and governance committees that are part of the ERM framework, or they may have direct reporting lines into appropriate ERM framework structures.

The responsibilities of these second-line functions typically include participating in the business unit's risk committees, reviewing risk reports and validating compliance to the risk management framework requirements, with the objective of ensuring that risks are actively and appropriately managed.

Depending upon the size and complexity of the enterprise and its business, there may be a management board risk committee (MBRC), which serves as the second line of risk governance. The enterprise's compliance and risk functions report to the MBRC. The MBRC is to have a charter, which sets out its role mandate and authority to manage the enterprise's risk environment.

For many enterprises, the reaction to the global financial crisis (GFC) has been to question its second line of defence—the compliance and risk functions. In so doing, the following are being questioned:

- The risk management culture
- The understanding of the ERM framework
- The business unit's risk capacity
- The risk appetite and tolerance allocation for each risk category
- The adequacy of the risk budgets
- The skill and capabilities of its risk resources
- The risk governance approach
- The risk monitoring and reporting activities
- The risk metrics to alert the business of the emergence of risk
- The capability to adjust the business unit's risk capacity, appetite and risk tolerances for changing economic conditions

As part of the first line of defence, these are aspects of the ERM arrangements set by the MBRC charged with the role of representing the enterprise's stakeholders in respect to risk issues. However, should the MBRC be questioning the

effectiveness of its own risk decision making based on the information that was provided by the second line of defence? Enterprises have invested heavily in their risk and compliance functions, including the use of complex risk models; however, very few have invested in identifying why they received poor risk information, or in the quantum, the timing or the relevance of the information, to enable themselves to make adequately informed and, therefore, effective risk decisions.

Alternatively, should executive management have a closer look at itself? Would it find that it is at fault? Does executive management have the necessary experience, skills and authority to make the decisions? Is it too strongly influenced by rewards, such as bonus incentives, and the fear of shareholder demands to ignore or take risks that may lead to regulatory intervention or, even worse, financial failure?

THIRD LINE OF DEFENCE

The third line of defence is that of internal and external auditors and the US Sarbanes-Oxley Act compliance team (where applicable) who report independently to the senior committee charged with the role of representing the enterprise's stakeholders relative to risk issues.

The internal and external auditors and Sarbanes-Oxley teams regularly review the first and second line of defence activities and results, including the risk governance functions involved, to ensure that the ERM arrangements and structures are appropriate and are discharging their roles and responsibilities completely and accurately.

The results of these independent reviews need to be effectively communicated to executive management and, more important, to the board of directors in cases in which these groups ensure that appropriate action is taken to maintain and enhance the ERM framework.

As stated earlier, the body that has the highest level of risk governance is the senior committee (such as the enterprise's board of directors or some other body, e.g., the audit committee or a specific risk committee) that is charged with the role of representing the enterprise's stakeholders in respect to risk issues. This committee has the responsibility and accountability to provide effective oversight of the enterprise's risk profile. In particular, this committee should ensure that the enterprise's executive management is effectively governing and managing the enterprise's risk environment.

The senior committee charged with the role of representing the enterprise's stakeholders relative to risk issues is ideally composed of directors and non-executive directors (where appropriate), with the committee chair reporting to the chair of the board of directors. The enterprise's chief risk officer reports to the chair of the senior committee on a periodic basis (typically recommended to be no less than quarterly). The chair of the senior committee reports to the board of directors on the status of the enterprise's risk environment on a periodic basis (typically recommended to be no less than biannually).

The senior committee is typically required to have a charter that clearly sets out its role, responsibilities and accountabilities in providing risk governance to effectively discharge the requirements delegated by the board of directors.

The critical issue facing the senior committee is risk information. Too often, there is too much information (i.e., risk noise), which overwhelms the committee. The committee members need to know the critical risk issues that require their attention. The senior committee needs to state clearly what risk information it requires (i.e., relevance), and the format and timing of such information.

CONCLUSION

For many enterprises, the setting up of a risk governance structure and supporting ERM arrangements is relatively simple. The real challenge is ensuring that the expectations and perceptions of risk governance and management and the senior risk committee are aligned, and that risk-related information is effectively and consistently obtained, analysed and used. In reality, there is often an arc of misconception, i.e., management has its view of the enterprise's risk profile, and the added value of the second and third lines of defence is not incorporated effectively within the overall governance approach to optimise achievement of enterprise objectives.

Governance in the Cloud

Joseph Kirkpatrick is a certified specialist in data security, IT governance and regulatory compliance. He has delivered auditing and security assessment services to service providers for more than 11 years. As a managing partner in the KirkpatrickPrice auditing firm, Kirkpatrick provides assurance to clients and stakeholders seeking to understand compliance and regulatory requirements by helping the industry navigate a complex world of data security topics.

The most frequently used technology phrases in recent history have stemmed from the proliferation of cloud services. Service providers are developing and relabeling services to capitalize on the attention and movement to the cloud as a method to outsource processes, maintain technological advantages and reduce costs. Cloud service offerings have grown exponentially and continue to gain traction because of the promised benefits that cloud computing delivers.

Many companies are now selecting hosting providers that offer infrastructure in the cloud for their customers. These companies reap the benefits of access to advanced technology at a fraction of the cost of making capital investments in dedicated systems. Shared services can deliver improved capabilities to multiple clients who make a shared investment in the technology. However, many of the users of these systems assume that they are outsourcing risk to the cloud as well. I call this "security by abdication." Security by abdication is when a company decides that rather than accept the responsibility of securing and maintaining systems, people or processes, it will abdicate the responsibility by moving to the cloud.

OUTSOURCING RISK?

During an audit, we often hear the phrase, "they handle that." In other words, the company has signed an agreement for Software as a Service or Infrastructure as a Service and breathes a sigh of relief because its responsibility for security on those systems is supposedly in the hands of the service provider. In actuality, the company's responsibility for governing security has not been removed, it is merely different, and must be evaluated in the context of the cloud service, the cloud provider and the purpose for which the company is utilizing the service.

American Health Centers Inc. (AHCI) is an example of an organization that chose to outsource its critical infrastructure function, choosing independenceIT, a cloud IT vendor. The AHCI risk assessment determined that the benefits of hosting data in a secure off-site data center would outweigh the risk of outsourcing management of the systems. It also determined that, given proper governance, security would be improved because the monitoring of access controls provided by independenceIT was at a level that ACHI would not have been able to provide itself. Security governance is problematic for companies that do not wish to absorb the various matters that must be considered when evaluating risk and managing security. For a company in the business of, for example, producing widgets—and not in the business of securing systems, applications and people—the security function is overwhelming, to say the least.

> "The company's responsibility for governing security has not been removed, it is merely different."

OVERSEEING SECURITY AND GOVERNANCE

It has been difficult to ask senior executives to oversee a topic with which they are uncomfortable because of the rapid changes taking place with technologies and persistent risks. Governing other departmental goals and objectives is more natural for business leaders and audit committees. Overseeing an information security program that permeates every department and requires a grasp of rapidly transforming subjects has not been as easily adopted.

Many organizations have appointed an information security officer or a different position to oversee the security function and report back to the board of directors. This arrangement has been generally accepted as satisfactory governance even while security incidents are on the rise in the corporate environment.

While governing the risks that it faces, AHCI chose to oversee independenceIT as a service

provider by analyzing its risk management results and audit findings to evaluate the effectiveness of control mechanisms that protect the data and restrict access by unauthorized parties. Whether AHCI built and maintained the technology itself or outsourced the capability to independenceIT, AHCI still has an obligation to govern the information security program that will safeguard patient data.

> "Many organizations' current information security programs do not adequately address outsourced services."

It is important to note that many organizations' current information security programs do not adequately address outsourced services because the expertise or ability to assess the risks associated with an outsourced provider have not been considered.

CHOOSING A COMPLETE CLOUD VENDOR

The business reasons for choosing a cloud services provider are clear. AHCI was able to provide its employees with cutting-edge technology and remote access to applications by using independenceIT's remote desktop client, *Freedom Desktop,* thereby reducing the investment in processing speed and memory requirements. Additionally, the promise of managed security for these remotely accessed systems, applications and data means that the company will not have to monitor, update and test systems on a regular basis, as it would if it were managing all of the systems itself.

However, organizations must consider several other factors when choosing a cloud vendor. Without proper governance of the cloud service provider, an information security program is incomplete, major risks are not considered, and breaches will continue to occur due to misinformation or false expectations placed on the cloud service provider.

Governance of any service provider should include monitoring its risk assessment results to evaluate whether or not its policies and procedures are comprehensive enough to identify threats to its systems, physical locations, employees and vendors. A closer look at a service provider's risk assessment and audit program discloses the matters that should be known by a customer using its services to host and manage sensitive data.

Enjoying this article?

- Read *IT Control Objectives for Cloud Computing.*

  www.isaca.org/ITCOCloud

- Read *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives.*

  www.isaca.org/cloud

- Consider attending ISACA's Information Security and Risk Management Conference in Las Vegas, Nevada, USA; San Juan, Puerto Rico; or Barcelona, Spain, where there will be multiple cloud-related sessions.

  www.isaca.org/isrm

Finally, organizations should also review a vendor's service organization control report because it details the provider's risk assessment process, the controls it has placed in operation and the third-party tests performed to report on operating effectiveness. An organization must accept the responsibility of governing its service providers and what they provide to the company.

CONCLUSION

When outsourcing to a cloud vendor, all of these risks must be evaluated, and governance must be properly implemented, without the assumption that the cloud service is actually doing what it has promised. Due to the rapid expansion and adoption of cloud services, governance is needed more than ever to control and manage the risks.

Auditing IT Risk Associated With Change Management and Application Development

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*.

Using a risk-based approach (RBA) to the IT audit begins with the IT auditor assessing the inherent risk (IR) of the relevant technologies. Some IT risks are generally high, maybe very high, regardless of the industry, type of organization or nature of the individual entity. Some examples of those risks are data transferring between information systems, using a spreadsheet for critical applications and performing customized application development in-house. This article focuses on the last item: change management for custom application development (AppDev).

The next step by the IT auditor is to investigate the control environment to see if the entity has mitigating controls for change management associated with AppDev. The IT auditor needs to assess the control risk (CR) to assess an overall risk associated with AppDev and the audit/review being undertaken. COBIT and other ISACA tools contain a rich set of knowledge and techniques related to this important risk.

This article provides the IT auditor with concepts, techniques, processes and structures that can mitigate the change management risk associated with AppDev. It also provides questions and possible sources of evidence regarding the assurance that mitigating controls could provide.

COBIT AI6 MANAGE CHANGE

The COBIT 4.1 process associated with AppDev risk is AI6 *Manage change*. This process is described as follows:

> *All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following the implementation. This process assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.*[1]

In COBIT, the control objectives related to the *Manage change* process are:

- AI6.1 *Change standards and procedures*
- AI6.2 *Impact assessment, prioritization and authorization*
- AI6.3 *Emergency changes*
- AI6.4 *Change status tracking and reporting*
- AI6.5 *Change closure and documentation*

These control objectives can be achieved through various practices depending on the capability of the enterprise and the technology involved. One possible set of such practices for AI6 is documented in the *COBIT® Control Practices* publication.[2] The *IT Assurance Guide: Using COBIT®*[3] provides auditors with guidance on how to assess the adequacy of their enterprises' design and implementation of their change management processes, based on the COBIT control objective/control practice content.

Control over the change management process is measured by metrics such as:

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Amount of application of infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

Other metrics are suggested for consideration in the COBIT AI6 process content.

The benefits of the COBIT control objectives, control practices, assurance guidance and related metrics examples are that they provide the IT auditor with guidance on appropriate questions to ask in relation to change management processes and activities, suggested sources of evidence of control activities and risk mitigation, and audit procedures to perform.

For instance, in regard to AppDev, is the application programming change:

- Authorized?
  - For example, the programming change is authorized by a sponsor who is a business unit manager. That is, there is a signed and completed change management request along with an official business case.
  - Another example is that an approval document is signed by the IT steering committee or an alternate authorized body.
- Subjected to a risk-impact assessment?
  - If so, there should be documentation of that assessment. Also, a formal structure such as a steering committee could have this step as a standard process for all changes.
  - It is *critical* that all applications be assessed for impact due to the high nature of IR.
  - Has the risk of errors been properly assessed? Programming errors are probably the primary or most common IT risk in AppDev.
  - If a significant business application is involved, and a large number of lines of code are being changed, deleted or added, the change is, by nature, high-risk. Has the entity properly assessed this IR, and provided an appropriate mitigation?
- Handled effectively and formally when it is an emergency change?
  - Some emergencies require the change to be made first, and then the documentation and structured, formal processes completed, for the most part, after the emergency has been addressed.
  - There should be some documented definition of "emergency," and documented processes for handling emergency changes.
- Prioritized among other IT changes in a manner that is effective for the entity as a whole?
  - Many times, the prioritization of IT changes defaults to the IT department, probably its director or the chief information officer (CIO). This situation is not the one preferred, nor the one suggested by COBIT (see PO4.3 *IT steering committee*).
  - Look for a formal structure that makes these decisions.
  - Look for a direct and interactive link between prioritizing major IT changes and the board of directors (BoD)/executive level of management (i.e., good IT governance).
- Tracked by a formal process?
  - The status of all AppDev changes is updated in a timely and consistent manner.

  - Tracking should be a formal process, such as an application that requires entry of an AppDev change, authorization of that change before work begins, and testing documentation.
  - Change-related problems are identified and handled in a timely and proper manner by the tracking system, or reported to the appropriate committee, or both.
  - Reporting on AppDev progress and changes in status is done in a formal, structured format with regular consistency, e.g., reporting to a project management office (PMO) or change management committee (see following discussion).

The IT auditor needs procedures to address these questions and the COBIT-related content referenced previously supports this need. One audit procedure is to pull a sample of AppDev projects for the period under review to see if evidence exists (via inspection or observation) to obtain some assurance that the entity has mitigated the high IR of AppDev by establishing effective control of the enterprise's change management process by achieving the control objectives described in COBIT AI6.

As a specific focus, the IT auditor should examine enterprise documentation for evidence of the employment of best practices of systems development life cycle (SDLC), which are generally considered mitigating controls for AppDev risks.[4]

The maturity model for AI6 described in COBIT provides a scale and supporting attributes by which the IT auditor could assess the maturity of an enterprise's change management process.

In the process of completing the IT audit for AppDev, the IT auditor should remember that change management is enabled by an organizational structure with roles and responsibilities as well as by a process and metrics (measurements). COBIT AI6 acknowledges this multifaceted aspect by supporting process control objectives and performance measurement aspects. The structure aspect specifically related to change management activities is dealt with by the responsible, accountable, consulted and informed (RACI) chart related to AI6. The RACI chart provides guidance on change management roles and responsibilities related to generic change management process activities that support the broader organizational structure considerations addressed by COBIT in another process—PO4.

COBIT PO4 DEFINE THE IT PROCESSES, ORGANIZATION AND RELATIONSHIPS

Another way the entity can mitigate AppDev risks is to have a formal structure to deal with some of the previously mentioned responsibilities and accountabilities that enable process activities to occur in a controlled manner (e.g., authorization, prioritization, alignment with business strategy, entity to whom reports are made).

A Steering Committee

COBIT process PO4 *Define the IT processes, organization and relationships* applies to AppDev controls by providing a necessary formal structure. As part of COBIT's Plan and Organize (PO) domain, this process is necessarily about the entity as a whole and the general (management) controls over IT.

PO4.3 provides one of the formal structures that is beneficial to mitigating AppDev risks. According to COBIT 4.1, PO4.3 establishes an IT steering committee (or equivalent) composed of executives, business managers and IT management (i.e., it is cross-functional). Its purpose is to:

- Prioritize IT investments and projects and align them with the enterprise's business strategy and priorities
- Track the status of projects and resolve resource conflicts
- Monitor service levels and service improvements

Other PO4 control objectives such as PO4.5 (*IT organizational structure*) and PO4.6 (*Establishment of roles and responsibilities*) should also be taken into consideration.

As can be seen, these purposes fit the risks and needs to direct and control AppDev. Thus, the IT auditor may want to gather information and evidence about the existence of a steering committee and its operating effectiveness.

An Ideal Structure

Because a steering committee is strategic in nature, and because reporting and tracking of AppDev changes is tactical in nature (i.e., lots of things happen in a week's time and problems need relatively immediate attention), there is a need to consider another level of structure for change control. An ideal structure would be for the BoD to establish a steering committee (or its equivalent) as a cross-functional group responsible for IT projects at the strategic level. This body would, for instance, be responsible for prioritizing and funding IT projects.

But the tactical aspects of AppDev (and other similar IT changes) are probably better suited to a tactical committee that meets more often (probably weekly, but not less than monthly) and is dedicated to solving problems and managing the IT changes hands-on. It may be appropriate for the enterprise to consider using a change management committee to oversee IT-related changes (not just AppDev) from the tactical perspective. The committee should be made up of the business sponsors, representatives of the user groups and the IT function. Tracking the status of changes and resolving conflicts might be better suited at the tactical level than the strategic level (steering committee).

A side benefit of such an organizational approach is that business-unit managers have the opportunity to see changes initiated in other units that have consequences—maybe unintentional—that affect their unit. The change management committee provides the opportunity to vet changes across the business units before certain problems occur.

This proposal is consistent with some other principles and bodies of knowledge in the IT profession. For example, a PMO performs this type of service, function and oversight for IT projects. In Capability Maturity Model Integration (CMMI) from the Software Engineering Institute, there is a hierarchy structure for software development that includes the strategic level (BoD), the middle management level (tactical) and the ground level, where programmers work. So, the change management committee idea could be integrated with a PMO or CMMI-based structure.

CONCLUSION

AppDev is an area of IT that generally is considered to be high in IR because of the probability of errors or fraud in programs when written and deployed. There need to be some reasonable mitigating controls to provide assurance that changes made to business applications do not adversely impact achievement of business objectives. The COBIT processes AI6 and PO4, and supporting materials, provide specific guidance and information to the IT auditor that can be used to gather evidence and make an assessment about the effectiveness of controls in place.

But beyond just ensuring the adequacy of the process controls that are being, and have been, employed, the auditor should also consider the adequacy of the process and organization to support the business objectives. COBIT materials support such an assessment through the guidance offered in relation to process activities, roles and responsibilities, goals and metrics, maturity levels, control practices and assurance testing.

ENDNOTES

[1] IT Governance Institute, COBIT 4.1, USA, 2007

[2] IT Governance Institute, *COBIT Control Practices: Guidance to Achieve Control Objective for Successful IT Governance, 2nd Edition*, USA, 2007

[3] IT Governance Institute, *IT Assurance Guide: Using COBIT*, USA, 2007

[4] For more on SDLC and IT audits, see the IT Audit Basics column: Singleton, Tommie; "Systems Development Life Cycle and IT Audits," vol. 1, *Information Systems Control Journal*, 2007.

Hongwen Zhang, Ph.D.

Hongwen Zhang is the chief executive officer (CEO) and cofounder of Wedge Networks, as well as the co-inventor of Wedge Networks patented technology WedgeOS. He has had a long career as a technologist, inventor and entrepreneur. Zhang was a cofounder of 24C Group Inc., which developed the first digital receipt infrastructure for secure electronic commerce (acquired by Axway Corp.), as well as a principal of Servidium Inc. (now ThoughtWorks Inc.), a global leader in agile development methodology. He also served as the chief technology officer of Wedge until early 2009, during which time he brought WedgeOS from a technology concept to an award-winning network security product line.

Zhang has a doctorate in computer science from the Department of Computer Science, University of Calgary (Alberta, Canada); a masters of computer science in computer engineering from the Institute of Computer Technology—Chinese Academy of Sciences (Beijing, China), and a bachelor's degree in computer science from Fudan University (Shanghai, China).

Away from the office, Zhang spends his time reading on a variety of topics such as history, science, information technology and security. In addition, he loves the mountains, and, in his spare time, he enjoys exploring the hiking trails in the Canadian Rockies with his family.

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

A There are all sorts of businesses, and each may have a unique perspective on what the biggest risks are. At a very high level, you can think of a business as a household in terms of managing risks: You do not want your valuables to leak out, and you do not want your house to be vandalized. These are exactly the kind of risks that businesses have to deal with.

For example, in the Sony Playstation Network security breach incident, users' information was stolen. The financial damage to Sony has been estimated to be as high as US $2 billion, not to mention the damage done to the Sony brand and reputation. As another example, the Stuxnet malware, which targets industry control systems, demonstrates how critical infrastructure can be damaged by IT security breaches.

How can businesses protect themselves? Well, there are many best practices and viewpoints. Knowing that almost all attacks are coming in from network connectivity, the most important thing is to make sure that bad things do not sneak in from the network. Most businesses, especially enterprises and service providers, will tell you that they already have all the gears that guard the network pathways, e.g., firewalls, and intrusion detection and prevention systems. The truth is: Breaches are still happening. Why? Because many successful attacks are embedded into content, i.e., data-in-motion, that comes in via legal ports from sources that are either spoofed or reputable. Hence, technologies that detect the intent of the data-in-motion are becoming more and more important. Businesses also need to understand that when digital assets are stolen, they are usually snuck out via the network. Data leakage prevention (DLP) refers to approaches that make sure no valuable data can be stolen. How do you enforce DLP at the network pathway? You need to have technology that can understand what is embedded in the outbound data-in-motion and stop the leakage of confidential information.

Q **How do you see information management practices in business changing in the short and long term? What are the biggest concerns with cloud computing, and how do you see them being addressed?**

A From IT's point of view, there are three major drivers in the industry: the adoption of consumer-grade tools and applications, such as social networks, peer-to-peer (p2p) and file sharing, in businesses; the ubiquity of mobile computing; and the big pull from the cloud.

In the short term, I see IT practices trying to cope with these forces of change. There will be confusion caused by the lack of adequate ontology to understand and describe the changes. Skin-deep technology that deals with the symptoms of these pains will be developed, such as next-generation firewalls, which will block the usage of social media in the workplace or limit application usage on mobile devices. As a result, new policies will be developed on how information shall be stored, moved or audited.

In the long term, I see IT practices helping businesses take advantage of these changes. So, instead of the CEO coming to IT demanding to get his/her iPad connected to the company's network and IT struggling to cope with security

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.

implications, IT will recommend and implement better ways for the business to operate anyplace and anywhere.

The biggest concern with cloud computing is data security across space and time: Organizations are questioning if their data are safe in the cloud, what happens to the data, who has access to the data and many other unknowns. The Cloud Security Alliance has been doing a good job of defining the many elements of cloud security issues, such as who has what responsibilities and what the government regulatory compliance requirements are in different geographical regions. From a pure technology point of view, security measures need to be taken to secure both the data-at-rest in the cloud and the data-in-motion to and from the cloud.

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

A With IT assets moving to and from so many places, predators will have ample opportunities to make kills. In the last several years, the dark side has certainly progressed significantly. It is alarming to notice that some recent attacking techniques are very stealthy and are aimed at bypassing or disabling the defense mechanisms on which we rely. IT security has traditionally been divided into two parts: infrastructure security, which is managed by the network group, and data security, which is managed by the management information system (MIS). Given today's blended attacks, there is no doubt that security professionals need to be well versed in both aspects.

Today's security professionals should not only focus on the traditional IT security topics, but also be familiar with risk management. And, to do so, they must have a better understanding of the business as a whole.

Hence, the role of the security professional has evolved from that of a technical specialist of a particular area to that of a business professional who understands the system that supports business operations, its vulnerabilities, and the measures and costs to guard the system.

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

A ISACA is working on COBIT 5, which will cover many aspects of this topic. From the view of a practitioner, I can see that IT will no longer be an issue dealt with by a group of technicians, but rather by people who understand the business objectives and processes. If you take the view that enterprise IT is the automation and innovation of business processes, you can also see that chief information officers (CIOs) will play more important roles in organizations. In many organizations, they will be reporting to CEOs and be in the driver's seat to execute business objectives.

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

A My career has led me down many paths from a programmer, to a software architect, to a product manager and marketer, to a chief executive. Each stage has its own "biggest" challenges. At the meta level, the biggest challenge has been to communicate a clear vision, gain support from stakeholders, and have the team members sing from the same song sheet to push toward the ideal state. I believe success comes through fostering a culture with the following core values:

- Determination to succeed: **We can do it**
- Thoroughness and diligence to deliver **accountability**
- Inquiring minds that are always **learning**
- Accumulative **innovation**
- The business as a platform for all team members' **personal growth**

IT Governance and the Cloud:
Principles and Practice for Governing Adoption of Cloud Computing

Ron Speed, CISA, CRISC, CA, is an IT executive with more than 20 years of experience in IT, risk management, governance, security and consulting. He has led and advised on strategic transformation initiatives in Australia and the US. His areas of specialty include the financial service industry and Asia-Pacific regulatory compliance.

Businesses around the world are witnessing a flood of new cloud computing services entering the market. These offerings are making it easier for almost anyone to engage and access, and they cover everything from personal file backup to major production server and application services.

Will cloud computing deliver lasting economic benefits to businesses? What is the best use of cloud services and can they be adopted in ways that do not put a business's risk profile in peril? These are questions that will, and should, be debated in boardrooms for some time to come. One thing for sure is that the cloud computing trend is putting pressure on traditional IT governance processes to adapt. For businesses to make prudent decisions regarding the adoption of cloud services, IT governance and risk managers need to work closely with business managers to promote understanding of key cloud computing principles and to help establish effective governance practices.

WHAT IS ALL THE FUSS ABOUT?

For those not familiar with the term, "cloud computing" describes Internet-based technology (either software, platform, infrastructure or a combination) that stores and processes information and is provided as an on-demand service.

So what is so new and revolutionary about this? On the surface, it sounds like an Internet version of IT outsourcing. Well, in a way, it is, but with a few important differences. To explain, it helps to use an analogy: Take people who commute to work by driving their own cars, but arrive late due to traffic, roadwork delays and frequent breakdowns (as their cars are old and poorly maintained). Now, they might choose to address this situation by buying navigational devices, upgrading their cars, securing regular maintenance services or even by hiring professional drivers to take them to and from work. This approach would be similar to delivering an outcome using traditional IT service models, with the use of a driver similar to traditional IT outsourcing.

An alternative approach for addressing the situation could be for people to trade in their cars and buy yearly tickets to take the train to work. By doing this, people would essentially be giving up the individualistic approach to commuting and adopting a standardized, technologically agnostic approach to achieving the same outcome. The whole problem with unreliable cars and the costs of driving are replaced with a solution with a completely different cost structure as well as different risks and opportunities. This approach is analogous to transitioning to the use of cloud computing services.

Similar to this analogy, there are several important trade-offs that occur when transitioning to cloud computing from traditional IT (whether in-house or traditional outsourcing). Exactly what these trade-offs are depend on the specifics of the services being engaged, but the typical ones to be aware of are:

- **Flexibility**—When using traditional IT, businesses have almost complete flexibility as to what they do with it because they are in charge of how it is used. With cloud computing, however, flexibility is likely to be more constrained by the way the services are supplied. For example, many Platform as a Service (PaaS) cloud services are kept up to date with current operating system versions, so if a business wants to operate using an older version, it may not be possible or may require negotiation of a more customized (and more costly) service. Some cloud services, such as Amazon's EC2, offer a lot of flexible options; however, setting them up and maintaining the configurations takes more effort and skill than other out-of-the-box offerings. As a benefit though, a flexible feature of cloud services is the ability to switch them on and off quickly without buying and selling expensive infrastructure and software.

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?

- Read *IT Control Objectives for Cloud Computing*.

www.isaca.org/ITCOCloud

- Read *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*.

www.isaca.org/cloud

- Consider attending ISACA's Information Security and Risk Management Conference in Las Vegas, Nevada, USA; San Juan, Puerto Rico; or Barcelona, Spain, where there will be multiple cloud-related sessions.

www.isaca.org/isrm

- Learn more and collaborate on Cloud Computing and Governance of Enterprise IT.

www.isaca.org/knowledgecenter

- **Security**—With traditional IT, businesses are in charge of security—how tightly their systems are locked up, who has access to them, and who else (if anybody) can share their processing and storage capabilities. In the cloud, the service provider controls many of these aspects. They may actually do as good a job or a better job than many businesses, but customers may not have much visibility as to how secure the service is. Cloud customers will also most likely share resources with other businesses without knowing who the other businesses are. For many businesses, this means a major rethink about the way security is governed.
- **Reliability and availability**—Similar to the analogy, the promise of more reliable and available services is one of the major reasons why businesses are attracted to the cloud. While (arguably) cloud services are potentially more reliable, issues do not completely go away, and there is also less visibility to customers regarding the causes of outages or the issues of reliability. This too requires a different governance approach.
- **Scalability**—Undoubtedly, this is where cloud computing claims its largest advantage over traditional IT—the ability to readily scale up and down processing and storage requirements without large changes in overhead costs. For many businesses, this capability can lead to major risk reduction, but, again, governance approaches need to adapt to take advantage.

Clearly there are pros and cons of both traditional IT and cloud-based services. But one of the great aspects of the flood of new services coming onto the market is that almost all businesses can benefit—through cost reduction, risk mitigation or both—from the increase in choices available. For this reason, it makes sense to keep an eye on new services as they emerge.

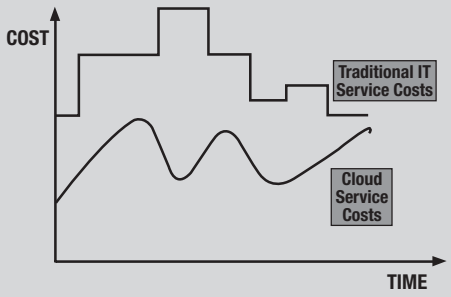
CLOUD ECONOMICS BASICS

To understand the risk and reward profiles of cloud services, it is important to understand the economics behind them. Here is a brief outline of the basics. Essentially, cloud providers are able to deliver services less expensively than in traditional IT service models due to two key factors:

1. Through standardization and abstraction of technologies (e.g., use of virtual machines), they can upscale and downscale storage and processing capability more efficiently. This reduces costs of adding and removing systems as service demands change.
2. Through sharing of IT capabilities across multiple clients with different demand cycles, they can eliminate underutilization of resources. This reduces overhead costs associated with idle capacity.

Figure 1 depicts how these cost savings may look for a business that undergoes periodic peaks and troughs and has high unpredictability in its demand for IT services.

Figure 1—Basic Cloud Computing Economics



Cost savings derived from:
- Efficiency of upscaling/downscaling as demand changes
- Reduced underutilization from sharing services

Note: Potential savings are greater when more layers of the IT stack are transitioned to the cloud, e.g., greater cost savings for SaaS than for IaaS.

The potential cost differential between the two models is even greater when more layers of the IT stack are transitioned to the cloud. For example, for Software as a Service (SaaS), where software, platform and infrastructure layers are bundled into a single cloud service, cost savings are potentially greater than with Infrastructure as a Service (IaaS), where only hardware layers (e.g., storage, CPU, network) are provided. This is because efficiency increases as more and more components are standardized and bundled together.

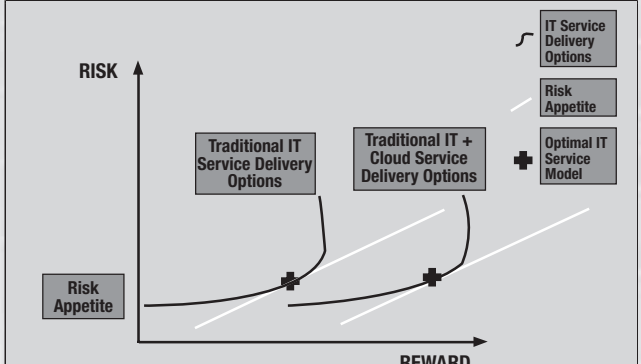
As with the transportation analogy, neither approach (traditional IT nor cloud computing) will always be superior to the other. Cloud computing has introduced additional options for IT service delivery. For many businesses, an optimal approach that leverages the best of both models will achieve an improved risk-reward trade-off. **Figure 2** depicts how this may occur.

Also, over time, cloud providers are aiming to create even greater cost savings as they capture larger market share and capitalize on economies of scale.

DECIDING TO DRIVE OR RIDE (OR MAYBE A MIX OF BOTH)

So if the cost savings from transitioning to the cloud are that compelling, why do businesses not move all their IT to the cloud? This is a fair question that is coming up regularly in boardrooms around the globe. But, unfortunately, the answer is not as simple as it might seem, as there are several other factors to consider, not the least being those relating to risk management, compliance and security.

Figure 2—How Cloud Options Can Improve Risk-required Trade-off

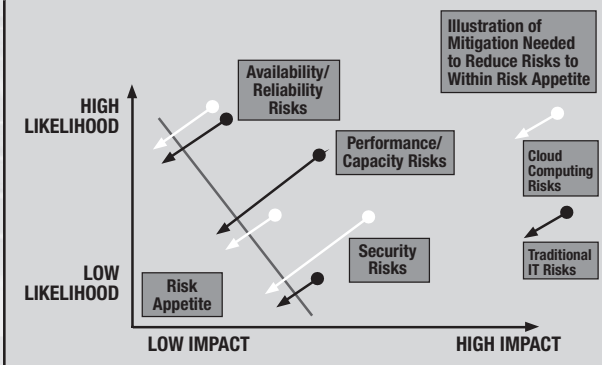


Consider that cloud computing options can shift the optimal service delivery model and improve risk-reward trade-off.

Therefore, the right answer to the question, "Should I drive or ride?" is: "It depends." It depends on the nature of the IT service, future growth expectations, the business's risk appetite, legal and regulatory compliance requirements, and cost. With all these factors to consider, it is essential that businesses carefully think through their IT service delivery strategy and prepare a business case that covers all of these factors. **Figure 3** illustrates an approach to measuring risk-mitigation costs so that they can be compared for different delivery models and reflected in a business case that might incorporate cloud services.

Figure 4 shows some examples of IT service delivery strategies, incorporating cloud computing and some of the key considerations.

Figure 3—Creating a Cloud Computing Business Case



Cloud NPV = (PV cloud cost savings) – (cloud risk mitigation costs) + (traditional IT risk mitigation costs) – (costs to transition to cloud)

CONSIDERING CLOUD COMPUTING CONTROL OPTIONS

The potential benefits of cloud computing are compelling, but it also brings a number of new and worrying risks. Following are typical control requirements or opportunities that businesses may need to consider when contemplating a move to the cloud. Keep in mind that, like the cloud itself, new technologies and techniques are emerging all the time.

- **Riding in private**—For businesses that dread the thought of their applications and data sitting on a public server right alongside who knows what, a private cloud may be the option for them. Think of a private cloud as the Internet's equivalent of travelling in a private compartment on a train; there are many of the benefits of riding the public carriages, but with additional security and privacy. Of course, this may

Figure 4—IT Service Delivery Strategies

Service Model Examples Using Cloud Computing	Key Benefits	Key Risks to Consider
1. Operate the entire production application using public cloud-based PaaS or SaaS, including customer interface, data transmission, processing and storage.	• Significantly lower operation and support costs • Potentially more reliable and resilient service than on-premise model • Reduced exposure to site-specific threats (e.g., disaster) by use of distributed sites • Services rapidly scalable, as and when required • Better able to avoid future risks of end-of-life architecture and technological obsolescence	• Consider incident response and recovery arrangements in the event of loss of cloud service. • Consider protection of data in the cloud, such as by encryption. • Consider other measures to protect the security of cloud-based assets and services. • Consider strategies to revert or to switch providers if needed.
2. Operate the production environment using traditional on-premise servers, and use cloud IaaS for development, test and failover/recovery environments.	• Reduced costs of maintaining redundant environments that are only in use periodically • Better service quality through the ability to scale for volume and stress testing and/or recovery during peak processing times	• Consider data protection in the cloud when testing the use of live data or undertaking recovery activities.
3. Operate the production environment using traditional on-premise servers, and use cloud IaaS for additional CPU and storage during periods of peak demand.	• Reduced costs of maintaining production capacity that is underutilized during nonpeak periods • Reduced capacity risks, as better able to scale up and down when peak processing demand is higher or lower than predicted	• Make similar considerations to scenario 1, although risks are limited to periods of peak demand processing.
4. Use cloud IaaS or PaaS for developing new services during early release iterations, as features are evolving and demand is scaling.	• Greater flexibility in access to IT resources as services evolve and grow; less concern about acquiring resources that may become redundant later	• Consider risks regarding the security of intellectual property (e.g., software, algorithms) stored in the cloud. • Consider the increased criticality of incident response and recovery provisions as services scale.

cost more, but it is still potentially cheaper than traditional IT systems. Private clouds can be provided to businesses in generally two ways: either by having the business's systems firewalled off from everyone else's, or by having the business's systems virtually separated from others using an authenticated and encrypted environment within a public cloud (known as a virtual private cloud).

- **Preparing to revert**—Preparing to revert might be one of the last things on the minds of business managers when engaging cloud services, but it is often one of the most important things to think about. The Satyam collapse[1] a few years ago illustrates how a service provider may outwardly seem fine, but can unpredictably be brought down by unforeseen circumstances. Such situations are hard to predict, let alone prevent, and when relying on obscured cloud services, the uncertainty and risks can seem even greater. Businesses need to prepare themselves for what to do if and when a cloud provider fails. That is, they need a revert strategy to ensure that they can readily switch to an alternate IT service model at any time. This includes:
  - Maintaining knowledge of all critical information and processing assets held in the cloud
  - Maintaining sufficient skills (in-house or with a vendor independent of the provider) to be able to repatriate and reestablish systems and services
  - Regular backups of critical cloud-based assets held with facilities independent of the provider
  - Regular rehearsals, possibly by running services in-house or with an independent vendor for a period (potentially even with another cloud provider)

  Revert strategies cost time and money, but they are important to mitigating the risk of a cloud provider failing. Additionally, they put cloud customers in a much stronger position when renegotiating a cloud service contract because cloud customers know that they could readily switch from the provider if needed.
- **When in public, keep valuables under lock and key and stay alert**—The need to protect sensitive data or intellectual property is particularly important when using a public cloud service. Typically, the best way to protect these assets is to use encryption technologies. In recent years, encryption has become more readily available, inexpensive and easier to setup, but it is complex, and there are many aspects to consider. Here are a couple key points to be aware of:
  - Protecting data at rest and in transmission in the cloud can be readily achieved using encryption, but protecting data during processing in the cloud is problematic. Essentially, this is because when data are decrypted for processing, they are at risk, even if for a nanosecond. Basically, most

businesses wishing to perform processing on sensitive data in the cloud would be best advised not to use a public cloud model.

– Encryption is only as strong as the key management practices used around it. Many businesses have struggled to establish good processes for creating, distributing and renewing encryption keys. With a move to the cloud, where distribution of keys may be even greater, getting these processes in place becomes even more critical. Businesses not accustomed to implementing key management practices would be well advised to seek expert advice.

Businesses need to use encryption and stay alert. With traditional IT services, use of intrusion detection, alerting and prevention techniques has become common. But in terms of moving to the cloud, many of these tools are now in the hands of cloud providers, who may use these techniques to protect their networks and servers from attack. But, this does not mean that cloud providers will alert customers if a threat comes close to compromising customers' assets. In fact, unless businesses tell cloud providers that they want to receive security-event alerts, cloud providers might assume that customers do not want to know.

Fortunately, many cloud providers offer their customers the ability to receive security-event alerts and even to flag the specific assets that they want to be monitored. Should a security event occur on a cloud provider's network, businesses might still be reliant on the cloud provider to block an attack. They can, however, take their own evasive action to protect their assets, such as by bringing them offline.

KEEP THE LAW IN MIND WHEN TRAVELLING IN THE CLOUD

Before engaging with a cloud provider, there is another major area that warrants consideration: legal and regulatory requirements. In the old (pre-European Union [EU]) days of pan-European train travel, every time a train reached a border, government officials would come on board and check passenger passports before passengers could proceed. And, just because passengers purchased tickets to a particular destination did not mean that they would be allowed to get there if they did not have the right visas, for example.

The cloud can operate similarly. Just because a business purchases a service that operates across data centers around the globe does not mean that the business is allowed to send its data around the globe. Data privacy and sovereignty laws and requirements have sprung up around the world over recent decades. If businesses handle data covered by these requirements, they need to travel in the cloud with great care, or risk breaching the requirements.

Adherence to these laws and regulations can be complex, as there are many gray areas and legally untested situations, such as what constitutes export of data. The best recommendation is to obtain legal advice before entering into any cloud arrangements, particularly when operating in heavily regulated industries, such as financial services or health care, or where systems involve personally identifiable information (PII). In some cases, businesses may want to (or even be required to) consult with regulatory authorities directly.

For businesses subject to strict data-privacy or export laws, there are measures that can be put in place. For example, they can seek a cloud provider that offers geo-specific services, i.e., services in which operations are confined within certain jurisdictional boundaries.

Depending on the circumstances, there are many other areas of potential legal complexity, too. For example, what happens if an incident occurs in the cloud? Does the customer have the right to conduct a forensic investigation? Who will be liable for damages? Clearly, obtaining good legal advice is paramount for businesses to protect their rights and meet their obligations.

SELECTING A SERVICE PROVIDER—TRANSPARENCY AND TRUST

When it is time for a business to start evaluating service providers against its needs, there is a very important factor to consider: transparency. Cloud computing is much more than just buying IT hardware or software. It is about engaging a service that may be entrusted to manage critical assets and services, and there may be little day-to-day visibility of how this occurs. But, businesses can and should ensure a level of transparency.

With a traditional IT model (either on-premise or for many outsource arrangements), getting visibility is usually a case of commissioning an audit, either by internal auditors or by an outside party. But, for cloud services, this option is much less likely to be available or even practical, as the cloud service provider's processing may be distributed throughout the world.

Therefore, alternative methods of gaining visibility of security and control will often be needed. There are several methods available, and, recognizing the need to establish trust, cloud providers are investing more and more in providing the information their customers need. This is an area that is likely to grow and evolve, and maybe one day a single common standard will be in place. However, in the meantime, here are some typical methods used by cloud providers to provide transparency. Each has pros and cons; therefore, often the best approach is to seek a combination of these:

- **Nondisclosure agreements**—Understandably, many cloud providers are protective of information about their architecture, security and controls. But, recognizing a prospective customer's legitimate need to know these details, they will share limited information upon signing a nondisclosure agreement. If offered, this is definitely worth

taking because it will most likely shed valuable light on the provider's services. However, it is important to bear in mind that this information may or may not have been independently verified.

- **Independent auditor reports**—Many service providers are now engaging independent auditors to assess the design and operation of their controls and to make these assessments available to their customers in the form of an independent audit report. Sometimes generically referred to as "SAS 70 reports," there is a range of reports available. In the US, these include Statement on Auditing Standard (SAS) No. 70, Service Organization Control (SOC) 1, SOC-2 or SOC-3 reports, based on the American Institute of Certified Public Accountants (AICPA) standards. There are equivalent standards in other parts of the world.[2]
- **Certifications**—While independent audit reports are valuable, the scope and nature of controls can vary from provider to provider. One way to more easily compare providers is to look for industry certifications. Some of the more common and relevant certifications to look for are:
  - ISO 27001 and 27002 certifications provide assurance that the provider has implemented a set of security controls as well as a system of management practices to oversee the controls.
  - ISO 31000 certification means that the provider has established a framework and practices for managing its operational risks around delivery of its key services.
  - Payment Card Industry Data Security Standard (PCI DSS) compliance means that the provider has established security controls sufficient to enable credit card data to be stored, processed and transmitted using their systems. This requirement is quite stringent and valuable to a business that is looking to use a service for handling its sensitive information.

A note of caution: It is important not to take any audit report or certification at face value without examining its details. It is important to review its purpose, scope and any major exceptions, and to assess these against the business's critical compliance, risk management and control needs.

CONCLUSION

Recently, news broke of Dropbox allegedly misleading customers regarding the levels of data protection provided by its service. This occurred shortly after Amazon's EC2 service experienced major outages. With these and other events, media reports are asking, "Is this the end of the innocence of the cloud computing ideal?" The reality is that, as cloud services continue to grow and mature, there will be some derailments along the way. But the economics appear to be sound and compelling, and many of the technologies underpinning the cloud are maturing and proliferating quickly. So, it seems that cloud computing is an industry trend that is here to stay. That said, there are clearly a number of risks and uncertainties in transitioning to the cloud, so strong governance and control are an essential part of any decision to transition to the cloud.

But, for business managers who only glance at media headlines or skim glossy marketing materials, the path ahead may well be confusing and, at times, frightening. There are major opportunities here for IT governance and risk managers to educate and guide their business leaders on prudent ways to take advantage of the cloud. IT governance and risk managers can provide immense value in developing strategies that leverage the positive economic and risk-mitigation benefits of the cloud while also adopting control and assurance methods that help avoid the risks.

REFERENCES

Armbrust, Michael; *et al*; "Above the Clouds: A Berkeley View of Cloud Computing," University of California at Berkeley, USA, February 2009

Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing v2.1*, December 2009

Wright, Dave; "Selecting a Hosting Partner for Your Software Plus Services Application," Microsoft Communication Sector, August 2008

ENDNOTES

[1] Kumar, Manoj; "Scandal at Satyam: Truth, Lies and Corporate Governance," India Knowledge@Wharton, January 2009

[2] A good comparison of the reports can be found at *www.aipca.org.*

IT General and Application Controls:

The Model of Internalization

Emanuele Palmas, CISA, has been part of the internal audit team at Guess Europe Group, based in Lugano, Switzerland, since 2008. He has gained experience in external auditing for medium and large companies within the industrial sector at PricewaterhouseCoopers, with mandates including the US Sarbanes-Oxley Act and support to IT audit. At Guess Europe Group, Palmas has had the opportunity to improve his IT audit skills and has followed the implementation of IT general controls (ITGC) and IT application controls (ITAC) at the enterprise, supporting the external auditors when required. An important task during his practice has been the ITGC performance in Hong Kong for Guess Asia. Palmas holds the COBIT 4.1 Foundation Certificate and ITIL v3 Foundation Certificate. He can be contacted at *emanuele.palmas@ch.guess.eu.*

Industrial and financial companies sometimes find themselves faced with the choice of outsourcing IT audit services related to IT general controls (ITGC) and IT application controls (ITAC). The decision to outsource is most likely due to financial reasons, timing and/or insufficient resources, or an uncertain (if not absent) level of competency related to the enterprise that is being audited. In particular, the technical and practical knowledge of ITGC/ITAC goes well beyond the theoretical point of compliance contained in texts such as *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition* (a strict reference for most companies subject to the US Sarbanes-Oxley Act), rather than management process models such as COBIT 4.1 or the IT Infrastructure Library (ITIL). In fact, it is not just a compliance matter. The practice of implementing ITGC/ITAC provides added value in identifying and correctly understanding risks and, practically, in immediately establishing an appropriate audit strategy for the entire year.

Therefore, a certain degree of experience is mandatory, but not always available, among internal audit services. To account for this deficit, companies can choose to outsource the service (at best)—unconsciously deciding to miss an important educational goal that would be achieved over time, in favor of achieving an immediate and practical objective. That choice is not farsighted given the considerable risk taken.

In fact, the main risks are precisely that: incorrectly identifying all the risks and, more than likely, having a process limited to an operational, a financial or a compliance vision—any vision except IT, which is often the first, essential means by which all the processes are structured. It could also mean missing the opportunity to create the foundations for the futuristic "integrated audit," a model that every mature audit department aims to utilize.

MISSED OPPORTUNITIES WHEN INTERNAL AUDIT IS OUTSOURCED

Outsourcing does not give audit services the opportunity to understand business processes in their entirety. Internal auditors cannot grasp the true meaning of all business processes if they cannot understand how the information is managed across the company. All data are information used in the company to create and manage the business. Handling and understanding the information systems framework and its availability, origin and nature give the auditor a mastery of the knowledge of the risks, which represents an omnipresent goal in achieving the view of the integrated audit business model that is being discussed.

The first and last structural unit of the corporate world is represented by the data themselves. All processes are moving through the dense cluster of IT, and those processes are effective due to the efficient governance of the data. COBIT effectively summarizes this concept in its references to the research of strategic alignment between IT and business. Although the IT department can be seen as a holding company (with its budget, customers, internal suppliers and strategic objectives)—fully independent and well structured—IT can become a winning factor positioned within the strategic business. IT strategies, projects, objects and goals are the goals of the company; they support the enterprise, at minimum, and, at best, enable the enterprise to realize its success. Thus, the entire budget for IT projects is spent to support the business. All projects should come out of the business strategy and be approved and identified by the board of directors or management at the highest levels possible. No discrepancy or quantifiable or identifiable differences should exist between core business and IT strategies. The best strategy should minimize the differences as much as possible.

It is clear that, very often, internal auditors perform a lot of testing, and especially in terms of outsourcing, the complete definition of ITGC/ITAC and the evaluation control results that rely on other audits are often forgotten. However, starting with a certain degree of awareness and an established approach to ITGC can enable auditors to immediately see what was and what will be the company's business strategy, the structural changes, the process change that concerns the data, and the information (and, therefore, the business process) during the period. For example, just checking the number and significance of program changes performed during the period is helpful. Therefore, outsourcing these control tests can create a gap of knowledge that is not always immediately or easily remedied.

THE IT DEPARTMENT—A COMPANY WITHIN THE COMPANY

From the issuance of a client order, accounts payable (AP) and wire transfers to suppliers and payroll, all company processes move through the structure and substance of the information data.

An IT department can be defined as a company within the company. The IT department usually has its own portfolio of suppliers and customers (generally subsidiaries, branches or even single departments of the holding company itself), which, of course, rarely coincide with the suppliers and clients of the holding company as a whole. For example, the finance department can become a "customer" of the IT department when there is an assistance request or when support is needed to create a new computer program in-house. Perceiving a management information system (MIS) department as a company within a company contributes to the change from the old "data center" into a value-added business unit that is business-oriented and strategically aligned and guided by principles of effectiveness and efficiency.

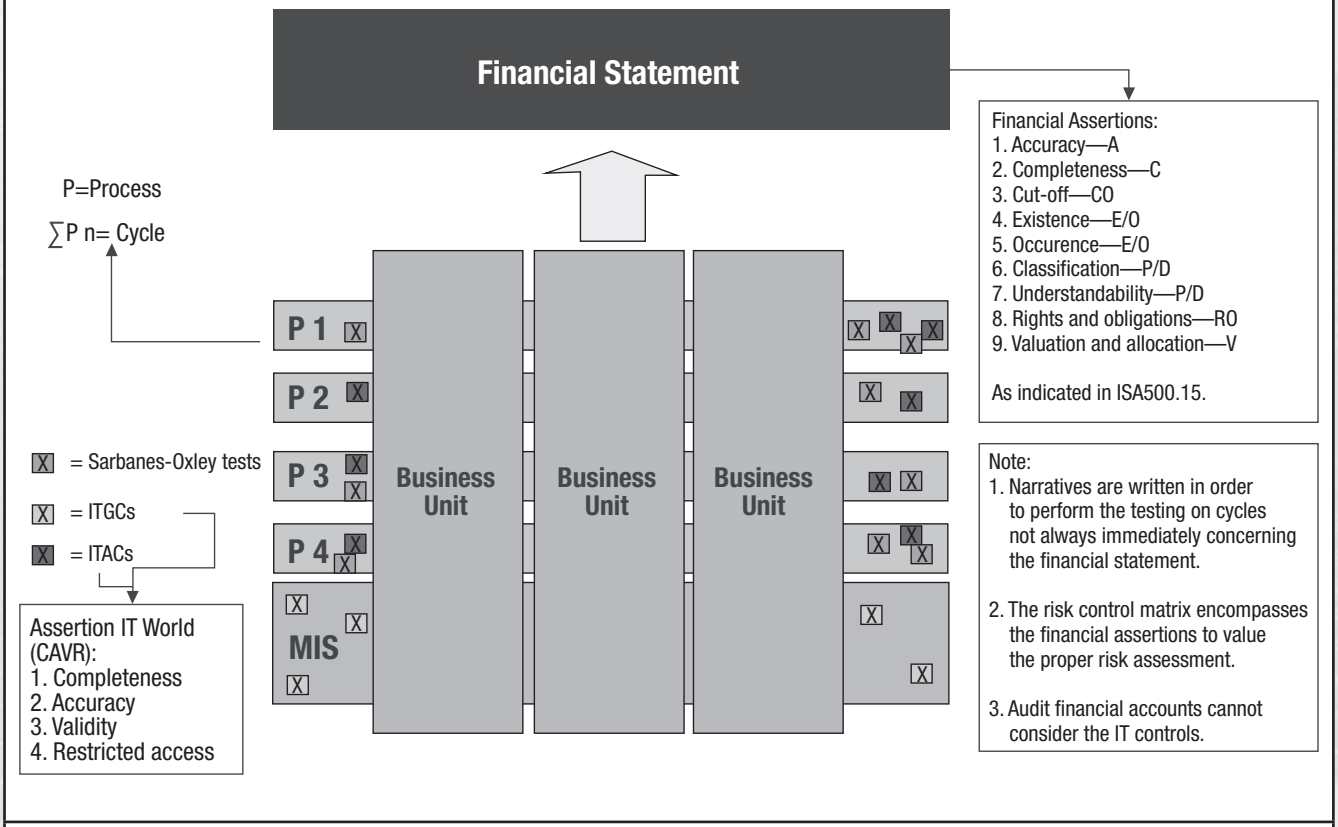
In the end, the opportunity to create an IT department to support the business is surely a management task that needs to be approved through the corporate governance of the board of directors, which should always remain independent.

It is also true that the internal audit department, unlike external audit and consulting, has a full commitment to corporate knowledge, which tends to focus on a standard of achievement and not on mere compliance with relevant laws and regulations. The knowledge of business risks in their entirety, of the control environment, of the company tone and culture, and of possible operational gaps gives a relevant opportunity for assessment that possibly only internal auditors can best use in the performance of their duties. For example, when experiencing a change in the supply chain process (awareness acquired during a specific internal audit), a risk concerning particular ITGC or ITAC could easily arise. Indeed, the impact of such a change may not be obvious within the mapping of the IT process, but it can be very significant when linked to the information received. Sometimes, interviews with IT management or the head of the finance department could be insufficient to detect changes because one cannot assert *a priori* that the communication inside the organization is efficient and effective. Thus, it is possible for an auditor to have a full understanding of a company (as COBIT recommends) only when an enterprise has applied the specific strategic alignment between IT and business.

> "The internalization of ITGC/ITAC is an important path to the integration of fundamental IT governance knowledge within corporate assets."

It is the risk of failure in strategically aligning IT and business that is actually under scope within ITGC/ITAC, and it is through the operational infrastructure that one can actually "feel" the company beat and seize its tone and culture. The veracity of strategic alignment is, therefore, established according to a top-down approach. If the understanding of the company passes through the information infrastructure (that is, the box that conceptually contains the company), an enterprise can be

Figure 1—An Integrated Approach: Mix of Controls



Source: Guess Europe, "ITGC & ITAC at Guess Europe Group: FY2010, July 2010," Switzerland, 2010

fairly assured that the business processes that go through the corporate network have a chance to be concretely realized. If the understanding of the company does not pass through the information infrastructure, it is probable that the entire business processes and relative risks cannot be understood completely.

ITGC/ITAC provide value immediately in terms of IT governance knowledge and the maturity model of the processes that the auditor has to test. Furthermore, testing ITGC/ITAC gives the enterprise the chance to assimilate fundamental requirements on controls and related risk, creating added value and knowledge on IT governance.

It can be said that the internalization of ITGC/ITAC is an important path to the integration of fundamental IT governance knowledge within corporate assets. The development of synergies between corporate governance and IT governance creates the opportunity to discover an interesting map of risks, and obviously, these synergies are applicable only within the company. This is an incredible opportunity for the auditor to use rigorously during the audit cycle. This renewed awareness will provide companies with immediately visible benefits in the form of an annual audit plan that is strategically built on a fully integrated understanding of risk.

During an audit plan, the auditor needs to verify that internal controls are effective to assure stakeholders of the true and fair representation of the financial statement. **Figure 1** depicts that, although the financial statement has its financial measurements and evaluations as financial assertions externally, within the company all data come out of the process cycles of the company. The company is a group of business units crossed by processes; summaries of processes can create process cycles. With ITGC, the auditor tests the processes related to the MIS department, which is a business unit that supports all business units and processes. For this reason, ITGC are reliable for other processes and audits. ITAC concern processes and, with US Sarbanes-Oxley Act test controls, give evaluations of the validity of the controls on process cycles. The controls are implemented by management to cover the risks identified by the company. To have a good knowledge and evaluation of all the risks, it is necessary to

test IT governance through ITGC/ITAC and, then, through the business processes. The most in-depth audit concerns IT controls; performing this audit correctly enables enterprises to see more easily the interconnections of business processes and the related risks. The sequence of ITGC/ITAC and other audits is qualified and improves the audit quality when a systemic and methodological approach is followed when performing audits.

CONCLUSION

Implementing in-house ITGC/ITAC is a great opportunity for auditors to improve their knowledge of the company, and for the company, it is a chance to build IT governance that strengthens corporate governance. The internalization of ITGC/ITAC is an important path to the integration of fundamental IT governance knowledge within corporate assets, and it allows the auditor to become a proficient catalyst of knowledge. This is especially true when the auditor follows the entire audit process, including the basic and important evaluation of IT controls. There are no particular reasons to outsource IT controls except for the lack of knowledge or expertise. However, every cloud has a silver lining, and internalization of knowledge, in this case, could be an investment in increased professionalism rather than in not-so-proficient outsourcing.

REFERENCES

ISACA, *CISA® Review Manual 2010*, USA, 2010

ISACA, *IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition*, USA, 2007

IT Governance Institute (ITGI), *COBIT® Control Practices, 2nd Edition*, USA, 2007

ITGI, *IT Assurance Guide: Using COBIT®*, USA, 2007

ITGI, *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, USA, 2006

KPMG; Geneva & Universität Zürich Institut für Rechnungswesen und Controlling "Objectifs de Contrôle Pour l'Information et les Technologies Associées (COBIT)," 2005

Laudon, Ken; Jane Laudon; *Management of Information Systems*, Prentice Hall, USA, 2006

Leleu, Eric; "Le COBIT: L'état de l'Art, Socle de la Gouvernance des SI," January 2009, *http://home.nordnet.fr/~ericleleu/cours/cobit/cobit.pdf*

Analyzing IT Value Management at KLM Through the Lens of Val IT

Steven De Haes, Ph.D., is an associate professor of information systems management at the Antwerp Management School (UAMS) and the University of Antwerp (UA) (both in The Netherlands). He is academic director of the IT Alignment and Governance (ITAG) Research Institute and can be reached at *steven.dehaes@ua.ac.be*.

Dirk Gemke is director of value management and alliances at Air France-KLM and program manager of service-oriented architecture at SkyTeam. Gemke can be reached at *dirk.gemke@klm.com*.

John Thorp, CMC, ISP, is a management consultant with close to 45 years of experience in the information management field. He can be reached at *john_thorp@thorpnet.com*.

Wim Van Grembergen, Ph.D., is a full professor at UA and UAMS, where he teaches information systems at the undergraduate, graduate and executive levels. He is academic director of the ITAG Research Institute and can be reached at *wim.vangrembergen@ua.ac.be*.

A common and critical dilemma confronting enterprises today is how to ensure that they realize value from their large-scale investments in IT and IT-enabled change. IT-enabled investments can bring huge rewards, but only with the right value management approaches.

The ISACA Val IT framework offers a broad set of good practices that support the adoption of such value management processes. This article describes a case study on how the Dutch airline company KLM introduced value management for its IT-enabled investments, analyzed through the lens of Val IT. As such, the goal of this article is to provide insight to practitioners regarding how to introduce better value management approaches.

FROM IT GOVERNANCE TO GOVERNANCE OF ENTERPRISE IT AND VALUE MANAGEMENT

After the emergence of IT governance concepts in the late 1990s, the notion of IT governance received a lot of attention. However, due to the focus on "IT" in the naming of the concept, the IT governance discussion mainly remained a discussion within IT. In the field, many IT governance implementations are still mainly an issue within IT, while one would expect that the business would and should take a leading role here as well. It is clear that business value from IT investments cannot be realized by the IT function, but will always be created by the business through its use of IT. Therefore, IT-enabled investments should always be treated as business programs, composed of a collection of business and IT projects delivering all the capabilities required to create and sustain business value.[1, 2]

The IT governance discussion clarifies the need for the business to take ownership of, and be accountable for, governing the use of IT in creating value from IT-enabled business investments. Acknowledging the prime accountability of the business in value creation initiated a shift in the definition of IT governance, focusing on the business involvement, toward governance of enterprise IT (GEIT) (instead of IT governance). GEIT is an integral part of corporate governance and addresses the definition and implementation of processes, structures and relational mechanisms in the organizations that enable both business and IT personnel to execute their responsibilities in support of business-IT alignment and the creation of business value from IT-enabled investments.[3]

GEIT clearly goes beyond IT-related responsibilities and expands toward (IT-related) business processes needed for business value creation. The topic of business value creation is high on the agenda of many organizations, and in both academic and professional literature, the concept of value management is addressed often. In response to the need, ISACA launched a framework that addresses these value management issues: Val IT.[4]

VAL IT AS A FRAMEWORK FOR GEIT AND VALUE MANAGEMENT

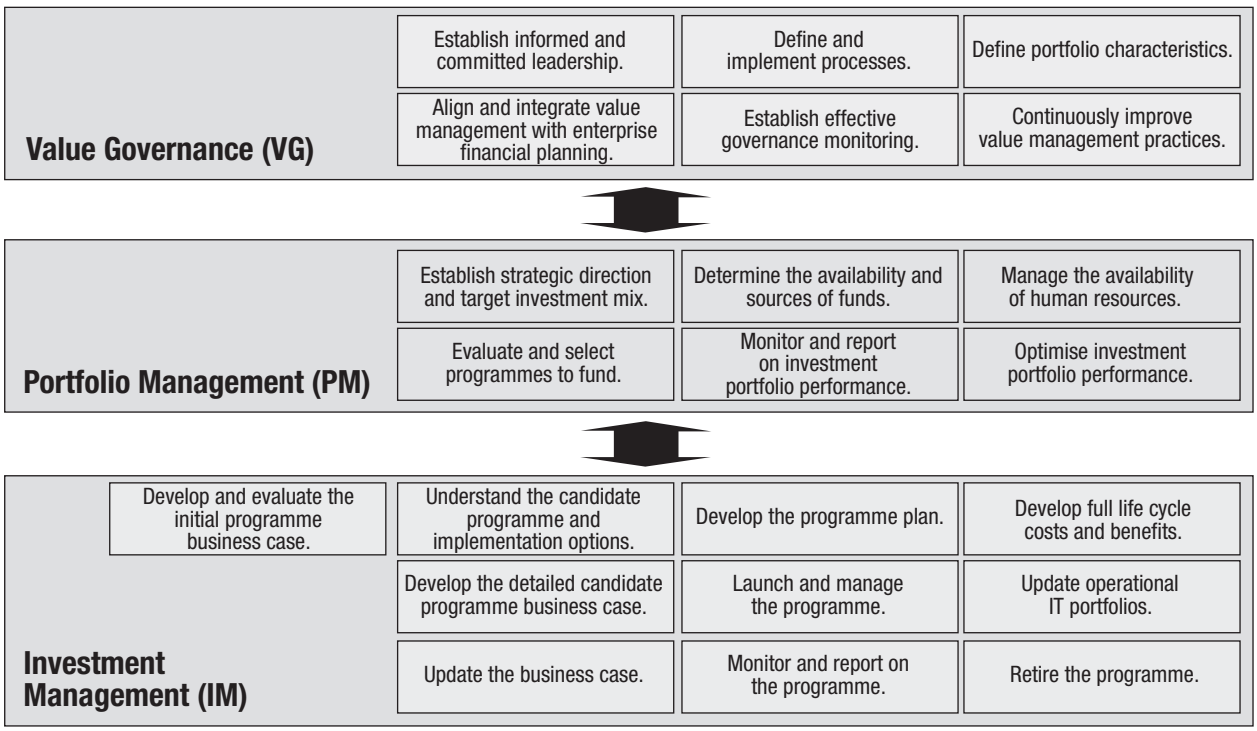
A recent and an important framework that addresses GEIT, Val IT has a specific focus on value management and creation. This framework starts from the premise that value creation out of IT investments is, in the first place, a business responsibility. To support business personnel in organizing and developing these responsibilities, Val IT presents a set of 22 IT-related business processes and associated key management practices, management guidelines and maturity models. Val IT is complementary to COBIT and follows the same structure and templates as provided in the COBIT manuals.

Val IT presents 22 processes categorized in three domains (**figure 1**):

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

The VG domain addresses the structures and processes required to ensure that value management practices are embedded in the organization. The domain deals with

Figure 1—Val IT Domains and Processes



Source: IT Governance Institute (ITGI), *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008, figure 9

the engagement of leadership (VG1), the definition and implementation of value management practices (VG2), and the integration of the latter into the organization's financial management processes (VG4). It also addresses that portfolio types and criteria need to be defined by the business (VG3), that effective governance monitoring should be established over the value management practices (VG5), and that there should be a continuous improvement cycle through implementing lessons learned (VG6). It is clear that these processes are defined at a higher level in Val IT and encompass "necessary conditions" to enable a value-based approach in portfolio and investment management.

The PM domain addresses the processes required to manage the whole portfolio of IT-enabled investments. This domain states that the strategic direction of the organization should be clarified and that the target portfolio mix should be defined (PM1). Also, available resources in terms of funding (PM2) and human resources (PM3) need to be inventoried. Based on detailed business cases arising from the IM processes (IM1-IM5), investment programs are selected and moved into the active portfolio (PM4). The performance of this active portfolio needs to be continuously monitored, reported on (PM5) and optimized (PM6), based on performance reports coming out of the IM processes.

The processes in the IM domain are situated at the level of a single IT-enabled investment. The first five processes in this domain focus on the emergence of new investment opportunities in the organization (IM1) and the development of detailed business cases (IM5) for the approved opportunities, including analyses of alternative courses of action (IM2), a definition of a detailed program plan (IM3) and full cost-benefit analysis (IM4). After approval of detailed business cases (PM4), investment programs need to be launched (IM6) and monitored (IM8) and, if required, business cases need to be updated (IM9). All investment programs need to be retired (IM10), bringing programs to an orderly closure when there is agreement that the desired business value has been achieved or when it is clear it will not

be achieved. Also, changes to operational IT portfolios, as a result of the investment program, need to be incorporated in the portfolios of IT services, assets or resources (IM7).

RESEARCH APPROACH

The goal of the KLM case study was to gain an in-depth understanding of how one organization adopted GEIT practices during the past decade in search of more value creation out of IT-enabled investments and to learn to what extent this mapped to the Val IT framework. Due to the exploratory nature of this study, a qualitative research approach was adopted based on in-depth case study research. Data were captured through multiple interviews, discussions and conversations with KLM's director of value management and alliances, who also provided access to other internal information such as internal reports, presentations and minutes. To further triangulate the data, other in-depth interviews were completed and tape recorded with the vice president (VP) of the chief information officer (CIO) office, the VP of finance and control ground services, the VP of the business development office (BDO) for passenger operations, and the director of finance and control IT operations at the premises of KLM in Amsterdam Schiphol Airport (The Netherlands).

ANALYZING IT VALUE MANAGEMENT AT KLM

Although KLM did not specifically use Val IT to introduce value management, KLM was involved in the development of Val IT 2.0, and as a result, there was some knowledge sharing in both directions between KLM and the Val IT development team. In this section, the focus of the case description is on understanding how a real-life organization "implemented" the intent of these good practices.

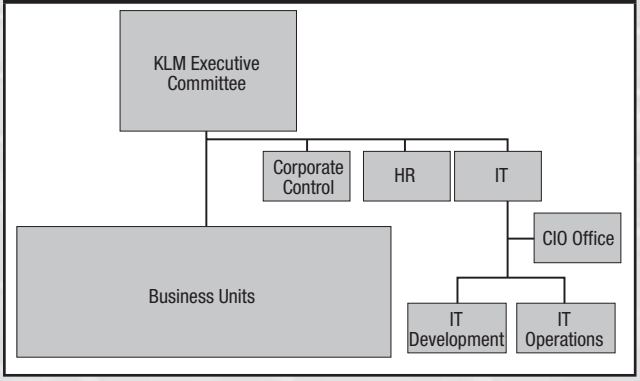
The Case Company: KLM

KLM was founded in 1919 and has its home base and hub in Amsterdam Schiphol Airport. KLM currently employs more than 33,000 people worldwide and manages a fleet of about 200 aircraft. In 2004, KLM merged with Air France, after which both companies continued to operate as separate airlines—each with its own identity and brand and each benefiting from the other's strengths. In financial turnover, Air France-KLM is the world's largest airline group, transports the most passengers and is the world's second-largest cargo transporter. In 2009, Air France-KLM operated flights to 255 destinations in 115 countries on four continents.

This case study focuses on the KLM activities within the Air France-KLM group. The KLM executive committee (**figure 2**) is composed of the chief executive officer (CEO), chief financial officer (CFO), managing director and executive VPs (EVPs) of the major business units and services (commercial, in-flight services, operations, ground services, cargo, engineering and maintenance, IT, and human resources). In 2009–2010, KLM's IT department employed close to 1,000 (internal and external) full-time employees (FTEs), with an IT budget of approximately €300 million. As shown in **figure 2**, KLM's IT is organized around IT development and operations activities with the CIO office addressing aspects of the enterprise/IT architecture, IT strategy, value and portfolio management, sourcing strategy, and risk and security. The mission of the KLM IT department is to "create business value by delivering reliable IT services to the business processes and innovative IT solutions to enable and support business changes." The following strategic goals for IT support this mission:

- IT is a world-class information services provider and will be able to deliver the best value to the company.
- The IT cost levels will be at a competitive industry level.
- The IT architecture and infrastructure will enable the growth ambitions of Air France-KLM.

Figure 2—KLM Structure



IT is a business-critical enabler for KLM; yet, at the same time, it can be a source of both success and discontent. In 2001, the balance had tilted toward discontent due to a lack of trust in what was perceived as a costly and unresponsive

IT department. This occurred in a business climate that was increasingly challenging and that became dramatically more so after the 11 September 2001 terrorist attacks on the US. After that event, KLM's CEO seized the opportunity to make a structural break with the past and to reexamine and transform KLM's business and IT governance.

The EVP of the operations control center was appointed the new CIO. It was believed that having a CIO from the "real business" would help get the IT governance discussion out of the IT area and have it put on the business executive's agenda. The newly appointed CIO received three clear priorities:

1. Provide the reasons why, or why not, to outsource IT.
2. Create a business/IT board to organize joint success.
3. Design simple governance principles to restore control, enabling steering by the EVPs and CIO.

To respond to these requirements, the CIO office was established as a support function to the CIO, consolidating a number of already existing, loosely coupled and different functions such as the IT strategy office, program management and business/IT liaison roles. In the words of the VP of the CIO office:

> *In the scenario that we would outsource IT, both IT operations and development would mainly be sourced outside KLM, but the activities of the CIO office would be kept internally as it governs IT strategy, architecture, security, business/IT alignment, etc. The goal of the CIO office is to enable effective IT, in support of business needs.*

Value Governance at KLM

It was decided that, ahead of the first priority given to the CIO, the primary focus should be to introduce better governance principles and practices (priority three). A project titled "IT: A Collaborative Effort" was launched and focused on enabling all stakeholders to better understand the cost and value of IT, which, in turn, would enable them to make more informed decisions about what and how to potentially outsource (priority one). In support of priority two, a business/IT board was established, composed of the CEO, CIO and all business unit EVPs, who met every quarter to discuss and decide on strategic issues involving IT.

With regard to priority three, the CIO office, in collaboration with the business, designed a set of principles that would significantly simplify IT-related governance. The starting premise was that these principles should put the business in full control of all IT demand and IT spend. In support of these principles, a number of governance practices were introduced in the business and IT organizations, including the establishment of the business/IT board and demand management functions for each business domain. These governance principles and practices were introduced as the "only way of working" between business and IT for all business units and activities. These practices also supported the creation of portfolio management processes driven by the business units. The portfolio management processes evolved from being driven by IT resource and supply toward being driven by business demand with an innovative and rigorous approach to evaluation and selection.

The definition of the first draft set of governance principles and practices was mainly driven by the CIO office. These principles were later refined with the involved business parties and are now shared in the organization through its intranet. According to the director of value management and alliances (a member of the CIO office):

> *These principles and practices are still challenged from time to time. Our position is that we are always open for discussion for each of these principles and practices, but up till now, we have each time, in the end, reconfirmed them.*

The stated principles and practices apply for all business units and are presented in internal KLM presentations as shown in **figure 3**. The involved parties acknowledge that this list does not really distinguish between principles and practices, but presents them in a mixed way. However, it was believed to be a pragmatic and practical list that was workable for KLM. The CIO office developed more detailed background information and internal documentation to explain the impact and consequences of each of these principles and practices.

Referring back to Val IT 2.0, the goal of the Val IT VG domain is to ensure that value management practices are embedded in the enterprise, enabling it to secure optimal value from its IT-enabled investments. Val IT proposes six processes in this domain, as shown in **figure 4**. Mapping these processes to the KLM approach described previously makes it clear that the adoption of some of these processes is nicely illustrated at KLM. KLM's definition of the governance practices and principles (**figure 3**) ensures informed and committed leadership (VG1), appropriate governance

Figure 3—Governance Principles and Practices

1. For the business, there should be no difference between working with an internal or external IT provider.
2. Differentiate between *what* and *how* (and *why*).
3. Improve the demand function by creating a business demand office per business domain.
4. Improve the supply function by creating an innovation organizer and a service manager per business domain.
5. Create monthly decision meetings of *what* and *how* (management and IT).
6. Focus on the costs that can be influenced in full and those that can be influenced in part: split between innovation and continuity.
7. Each innovation (investment) has one business owner to whom all costs are charged.
8. Each service (continuity) has one business owner to whom all costs are charged.
9. Create a top-down budget framework and simplified budget process.
10. Activity-based costing is applied to process primary cost to product cost.

monitoring (VG5), and the implementation of value management processes (VG2). Also, some of these principles address specific issues, such as VG4 being covered in principles 9–10 (**figure 3**).

Figure 4—Val IT Processes Illustrated at KLM

Val IT Management Processes	Illustrated at KLM
Value Governance	
VG1 Establish informed and committed leadership.	X
VG2 Define and implement processes.	X
VG3 Define portfolio characteristics.	
VG4 Align and integrate value management with enterprise financial planning.	X
VG5 Establish effective governance monitoring.	X
VG6 Continuously improve value management practices.	

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

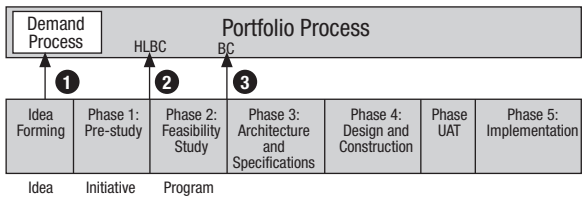
Portfolio Management and Investment Management at KLM

The previously mentioned governance principles and practices were needed as key building blocks in support of having effective portfolio and investment management processes driven by the business units. The design of these portfolio and investment management processes was created by the portfolio management office (part of the CIO office) and is shown in **figure 5**. Three approval stages were defined, going from "idea selection" to "program go" and "investment approval." For each of these phases, clear decision thresholds were defined. For investments between €150,000 and €500,000, the EVP, director of finance and control, and BDO of a business unit could approve the go/no-go decision in each phase. Investments greater than €500,000 are approved by the business unit investment committee (BIC), which comprises the business unit chief operations officer (COO), EVP, director of finance and control, and BDO. Investments greater than €5 million are approved by the executive committee (EC).

The initial phase addresses the initiation of the investment proposals or idea generation. In this phase, all business ideas are gathered and captured by the BDOs (demand process) and turned into potential initiatives for which a high-level business case (HLBC) will be developed. These HLBCs include descriptive information, classifications, and high-level cost and benefit estimates, and risk. The VP of BDO for passenger operations clarifies:

> *It is often hard to quantify some benefits at this stage. For example, the cost avoided of an aircraft not needing to land on another location because of better support systems, but still, we try to make as good as possible educated estimations.*

Figure 5—Portfolio and Investment Management Process



If an initiative is approved, it is turned into a program for which a full business case (BC) is developed based on a detailed feasibility study. To enable common and comparable BCs, a BC template was developed as a mandatory instrument for all investments greater than €150,000.

To be able to prioritize all these BCs, it is crucial to know what the organization's business drivers are. The director of value management and alliances makes this clear:

> *Our experience was that it was often difficult to obtain a clear list of business priorities from a business unit. However, we needed these priorities to enable the selection of "the right things," and for that reason, we used a methodology to help us and the business in making these business priorities transparent.*

To enable this process, the business drivers of a business unit were captured and ranked by the CIO office through interviews with the business unit executives. Next, for each incoming investment proposal, the contribution to each of these ranked business drivers was determined, ranging from "low" to "extreme." The result of this exercise is an initial portfolio containing a ranked, but still unconstrained, list of all investment proposals at the business unit level. The VP of BDO for passenger operations explains the importance of this process:

> *These priorities are the basis to build a "business plan" for the BDO of a specific business unit, describing all the things that the BDO office of a business unit can be held accountable for. I have even turned this business plan into a video clip on YouTube to demonstrate to all our business and IT stakeholders our commitment for the next year.*

After this prioritization, total demand of all business units typically exceeds the budget made available by the EC. The director of value management and alliances describes how this is handled:

> *Instead of using a "cheese slicer" and, for example, forcing all business units to cut 30 percent out of the project portfolio, a process of informal discussions is initiated between the BDOs to determine how the portfolio can best be optimized. As long as this process works, this approach is preferred instead of escalating to the next management level.*

This consensus-building process generally works well, and as a result, the business/IT board receives an overview of the major program and only needs to endorse the outcome of the portfolio management process. The director of value management and alliances concludes, "Through a good portfolio management process, we strive for seamless decision making."

Once the portfolio of programs is optimized, the BIC (for projects greater than €500,000) or the EC (for projects greater than €5 million) still has to release the funding before design, construction, user-acceptance testing (UAT) or implementation can start. This may appear as a duplicated decision structure, but it acts as a final check and also gives the final authority and decision power back to the business executives. The VP of BDO for passenger operations explains:

> *In the end, the business executives decide. This approach helped in getting them engaged in the portfolio management process because they get their control back, although, until now, they have never "used" it. Another important aspect in this context is that we try to make the time between the business idea and approval on the investment committee as short as possible as this period is perceived as "IT being slow."*

Referring back to Val IT, the goals of the Val IT PM and IM domains are, respectively, to ensure that optimal value is secured by the enterprise across its investment portfolio and to ensure that individual investments contribute to optimal value. The KLM approach described previously illustrates the adoption of some of the processes that Val IT proposes in these areas. The way the business drivers are defined for a business unit and how this leads to a prioritized list of programs in line with the available budget clearly illustrate PM1–PM3 (**figure 6**).

Reported Benefits, Lessons Learned and Future Challenges

During the onsite interviews, the following benefits, lessons learned and future challenges were reported.

In terms of benefits, the implementation and ongoing assurance of GEIT has restored trust between business and IT and resulted in an increased alignment of investment to strategic goals. The communication and discussions on portfolio management have also improved management

Figure 6—Val IT Processes Illustrated at KLM

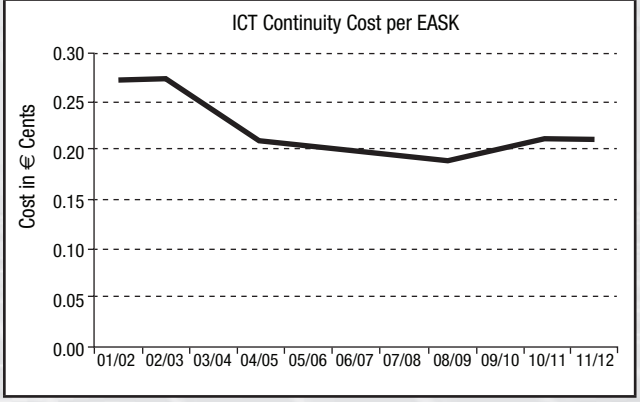
Val IT 2 Management Processes	Illustrated at KLM
Portfolio Management	
PM1 Establish strategic direction and target investment mix.	X
PM2 Determine the availability and sources of funds.	X
PM3 Manage the availability of human resources.	
PM4 Evaluate and select programmes to fund.	X
PM5 Monitor and report on investment portfolio performance.	
PM6 Optimise investment portfolio performance.	
Investment Management	
IM1 Develop and evaluate the initial programme concept business case.	X
IM2 Understand the candidate programme and implementation options.	X
IM3 Develop the programme plan.	X
IM4 Develop full life-cycle costs and benefits.	X
IM5 Develop the detailed candidate programme business case.	X
IM6 Launch and manage the programme.	X
IM7 Update operational IT portfolios.	
IM8 Update the business case.	
IM9 Monitor and report on the programme.	
IM10 Retire the programme.	

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

awareness and understanding and have supported the transformation from a cost toward a value culture. Also, more tangible benefits were reported, including lowered IT continuity costs per business production unit and increased innovation capacity.

A key metric used to monitor airline production is the relationship between all IT continuity costs and equivalent available seat kilometers (EASK), which represents the total number of seats and cargo capacity multiplied by the total number of kilometers flown by the airline fleet. **Figure 7** shows that, although many business investments involving IT (such as e-tickets, additional web-based sales and web-based check-ins) resulted in a year-on-year increase in the total IT budget, the unit cost of providing IT services (IT continuity cost) per airline production unit decreased by more than 20 percent. (The slight upward curve for the next three years is due to a temporary decrease of production in response to the world economic crisis.) This substitution of labor by IT also resulted in lower business cost per unit because IT is cheaper than labor.

Figure 7— Lower IT Continuity Costs

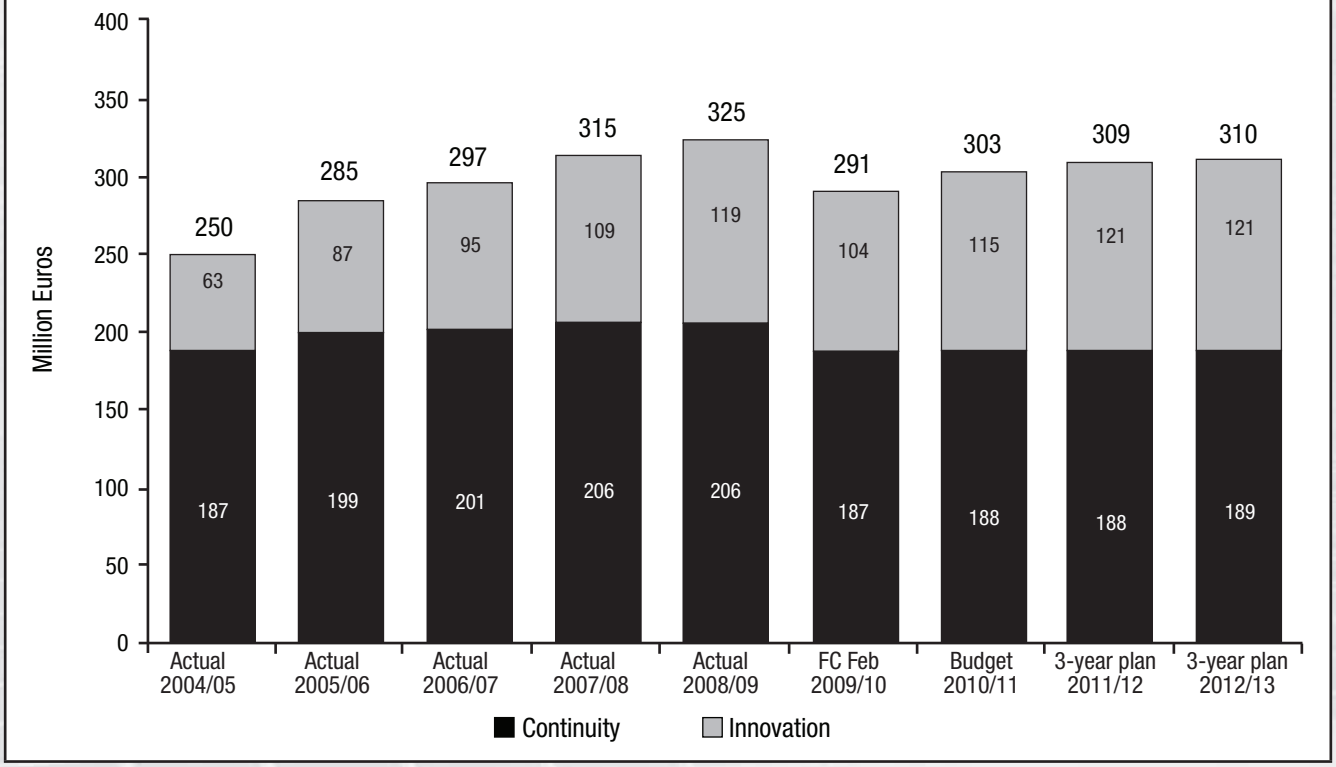


In addition to direct cost savings, the innovation capacity has increased as lower, or at least stable, IT continuity costs contributed to freeing up financials for IT-based innovation. Again, the CIO office develops metrics to demonstrate this outcome. As an example, **figure 8** shows a relatively stable IT continuity budget, enabling the increase of the total IT budget to go almost entirely to new innovation, which increased from 25 percent in 2004–2005 to 39 percent in 2010–2011.

So far, in the course of KLM's journey, a number of lessons have been learned. These lessons include the importance of senior management commitment and business engagement; change management; provision of adequate and appropriate support resources; and adoption of a pragmatic, practical and evolutionary approach.

KLM still has challenges ahead in further maturing GEIT and value management. These challenges include a better process for measuring and managing the benefits realization, continuous alignment of required business and IT resources, and consolidation of the whole investment portfolio at the group level.

Figure 8—Increased Innovation Capacity



CONCLUSION

To better understand how such Val IT practices can be adopted in an organization, this article mapped KLM's approach to specific Val IT processes. Insights from this case can help in better understanding implementation approaches in the Val IT domains: Value Governance, Portfolio Management and Investment Management. KLM clearly looked for pragmatic solutions in seeking full business engagement and senior management commitment. An important success factor in value management adoption at KLM was the maturity of the CIO office, which focused heavily on managing change and ensured that all the necessary support resources were available to achieve this.

Although all organizations, including KLM, face unique challenges, concerns about effective GEIT and the realization of real business value from today's significant and increasingly complex investments in IT are a universal concern. Other organizations can certainly benefit from the experiences of and lessons learned by KLM.

ENDNOTES

[1] Thorp, John; *The Information Paradox: Realizing the Business Benefits of Information Technology*, McGraw-Hill Ryerson, USA, 2003

[2] De Haes, Steven; Wim Van Grembergen; "An Exploratory Study Into IT Governance Implementations and Its Impact on Business/IT Alignment," *Information Systems Management*, vol. 26, no. 2, 2009

[3] Van Grembergen, Wim; Steven De Haes; *Enterprise Governance of IT: Achieving Strategic Alignment and Value*, Springer Science+Business Media LLC, USA, 2009

[4] IT Governance Institute (ITGI), *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008, *www.isaca.org/valit*

The Impact of Governance on Identity Management Programs

Rafael Etges, CISA, CRISC, CIPP/C, CISSP, is the director for security consulting services at TELUS, directing the organization's governance, risk and compliance (GRC) and identity and access management consulting practices. He is a member of the ISACA Toronto (Ontario, Canada) Chapter.

Anderson Ruysam, CRISC, CISSP, ITIL, is a senior IT risk advisor at the Government of Ontario, Canada, specializing in IT GRC and business management. Ruysam brings more than 14 years of extensive experience in IT governance, risk management and security operations.

Recently, the interest of organizations in identity and access management initiatives has increased dramatically, mostly led by the government, retail and financial sectors' concerns with data leakage, fraud and regulatory compliance and by management's interest in optimizing IT processes and reducing spending. The benefits associated with role and identity programs include improved management of access to information systems (IS) and data, which leads to better security and risk management; portability and reusability of role definitions across the organization; an ability to meet and demonstrate regulatory compliance; improved business continuity; and, equally important, cost efficiencies in administration and integration of business applications.

As the average annual budget required by enterprises to deploy identity management (IDM) solutions approaches the seven-figure range,[1] significant management involvement and diligence is vital to properly allocate resources. In addition to the business justification for such an investment, solid IDM governance must be applied to ensure that the relevant stakeholders are involved in the definition of principles and goals governing how business roles are managed within the organization. The ongoing message must be that IDM is a business issue affecting compliance, risk, privacy and cost-efficiencies, and that the main driver remains the proper management of business roles and processes supported by complex technology—and not the opposite.

This article focuses on two questions: What are the governance elements required to ensure the success of an IDM deployment in a complex enterprise environment? What is the bottom-line impact of having—or not having—these elements in place?

IDM, ROLE AND ACCESS GOVERNANCE

The identity and access governance discipline is rapidly evolving, and best practices and standards are still being developed.[2] Discussions among industry leaders are taking place, and best practices are being promoted by research institutes such as Forrester,[3] the Burton Group[4] and Gartner,[5] which further expand on specific approaches, solutions and products that address these new requirements and their respective areas of value.

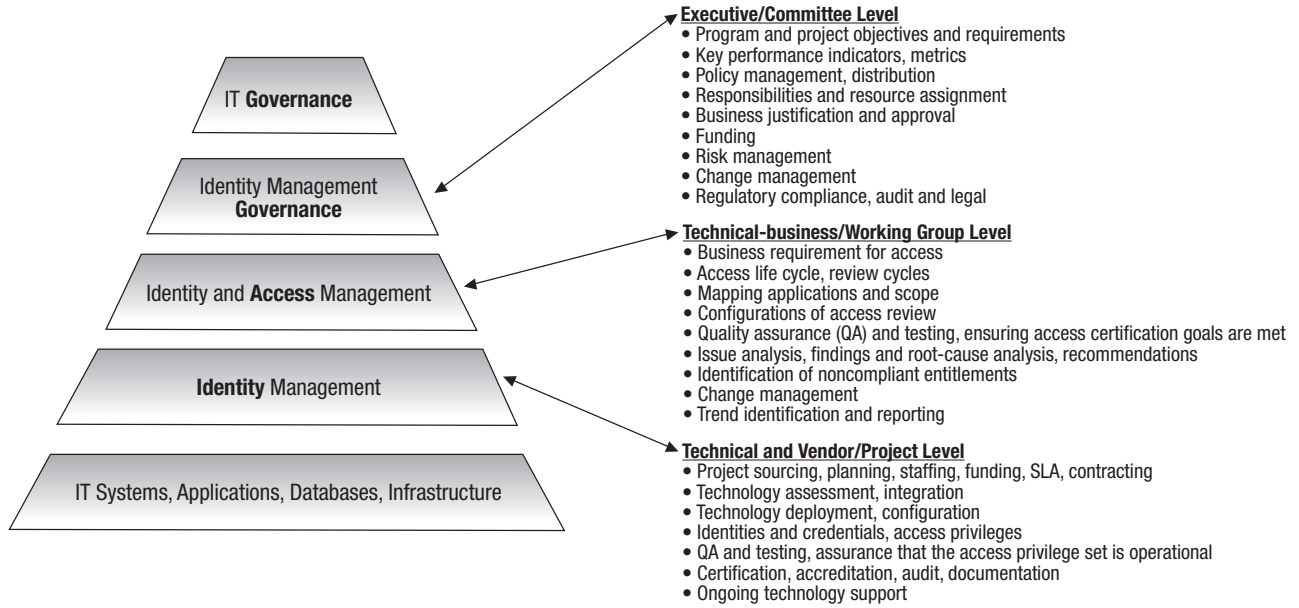
Different terminology is being created and used as the industry practices evolve around the management of roles, access and identities. In general, "role" represents a set of responsibilities needed to conduct business operations or transactions, "access" represents the privileges and resources used by someone within a role, and "identity" represents someone with a given role at a certain point in time.[6] The clear distinction among these terms is paramount since the management of each of these elements is evolving into discrete disciplines of their own. While identity management solutions focus on the automated provisioning and deprovisioning of identities/access to system resources, they have little to offer in terms of access governance (which roles should be granted access to what resources and how) or identity governance (how the organization defines roles and identities with the involvement of business leaders responsible for operations and revenue streams that rely on those roles to function).

Figure 1 shows a sample framework used to differentiate these elements and address the needs and requirements at each level.

THE BENEFITS OF GOVERNANCE

Different entities and individuals tend to defend different views and definitions of governance. A complete and impartial definition of "enterprise governance" reads: "Governance is the framework, principles, structure, processes and practices to set direction and monitor compliance and performance aligned with the overall purpose and objectives of an enterprise."[7]

Figure 1—Sample Role and Identity/Access Management Framework



Organizations that originally deployed IDM solutions to drive automation and better provisioning and deprovisioning capabilities within IT are now challenged with new requirements. They must leverage the same technology to demonstrate compliance with regulatory standards and enhance the visibility into "who has access to what," "why" and "approved by whom" at a more granular level than the existing IDM solutions were initially designed to provide. An additional layer of governance related to IDM is required to address these needs. These requirements are also related to IT governance and compliance and speak to the needs of business functions being serviced by IT.

The benefits presented by recognizing the need for and managing the governance and access management layers on top of the IDM technology are many, and can be summarized as:

- Automation of the entire entitlement and role review process, in alignment with business needs and requirements as stated by business leaders and managers
- Enterprisewide visibility into all user access privileges. Reviews are easy for business users to understand and can be configured to accommodate unique processes.
- Oversight in the form of dashboards reconciling and centralizing information for immediate insight into the status of the review and certification processes
- Certification and remediation of user entitlements; archived certifications and complete audit trail of historical changes that provide the evidence required by auditors
- Integration with the user provisioning infrastructure to track all entitlement changes; simplified role and access definitions at every stage of the user life cycle
- Change request workflows triggered by a change event or revocation of entitlements or event-driven workflows initiated by a change event requiring an incremental review of a user's access

These benefits cannot be realized by the deployment of IDM technology alone, and in some cases, the enterprise can be oversold on the provisioning technology by a vendor. Without oversight, the technology will not resolve business issues. The access management and governance layers must be in place to ensure that the full value of the investment is realized. This is not always the case.

THE IMPACT OF IDM GOVERNANCE ON STAKEHOLDERS

Figure 2 shows the positive impacts of governance elements applied to an IDM deployment to varying stakeholders affected by the technology within a typical organization.

CONCLUSION

IDM solutions offer an incredible value proposition for organizations. Like other complex technologies, such as customer relationship management (CRM) and enterprise resource planning (ERP), they touch and influence the way key revenue-generating business processes function. To a higher degree than CRM and ERP, IDM has the potential to affect any business process of an enterprise as roles, identities and access to IS are managed by the solution. And, as the technology becomes more pervasive in the organization, the potential for IDM—properly or poorly deployed—to deliver a positive or negative impact on stakeholders is immense.

The main factor affecting these outcomes is governance. Technology vendors will have a limited ability to understand the business issues driving the acquisition of the IDM solution by an organization, and will not have insight into its business

Figure 2—Impact of Identity and Access Governance on Organizational Functions

Stakeholder	Governance Elements	Impact
Chief information officer (CIO)	• Reduced complexity • Increased productivity • Scalability • Reduced costs • Improved audit readiness	• Service desk—Visibility and control over user and access change, provisioning and termination; reduced incidence of password reset cases • System development life cycle (SDLC)/Software as a Service (SaaS)—Standardized methods for identification and authentication, authorization and access for internal and external clients and partners; code reusage • IT support—Local databases in individual systems eliminated and replaced by a centralized access repository. Fewer cycles and resources are required to maintain and authorize access to applications and systems. • Auditing and compliance—Formalized, repeatable and documented identity and access processes that are ready for validation; reduced costs responding to audits
Chief information security officer (CISO)	• Risks managed to an acceptable level • Implementation and monitoring of controls	• Risk and control assessments—Facilitated by clear rules governing access to sensitive data, enabling the prompt identification of violations
Internal audit	• Faster audit exercises with limited resources • Accurate findings • Improved attestation	• Audit hours—Reduced effort in the validation of controls • Automated and reliable evidence • Comparable audit results—Trend mapping of control gaps, gap ownership and gap remediation
Business lines	• Reduced costs • Increased productivity • Maximized profitability and bottom-line results • Fraud and loss prevention	• Reduced cycles spent on system revisions, troubleshooting and QA related to access reviews • Consistency in business-system access rules • Visibility into who has access to business data at any point in time • Reduced fraud and losses due to improperly configured access rules, which would not be prevented by the IDM technology alone
Chief financial officer (CFO)	• Maximized revenue • Managed costs • Optimized bottom line • Maximized value for shareholders/owners • Compliance, audit and liability sign-offs	• Reduced operational expenditures—Optimized headcount, reduced consulting/contractor expenses • Budgeting—Reduced requests for *ad hoc*/emergency funding due to poor visibility into IT systems and infrastructure • Risk reduction—Enforcement of segregation of duties and due diligence • Expedited audits, reduced audit costs, and accurate and predictable findings

processes or the skill sets required to integrate and adjust its existing systems. The acquiring organization must be prepared to assess its own capabilities and gaps against best practices for managing roles and identities in areas such as access certification, entitlement management, access requisitions, and tracking and reporting, and it must be prepared to prioritize the closure of those gaps accordingly.

At a very high level, the main areas of activity include documenting a program charter (e.g., communications plan, responsibilities); determining which processes are to be considered; and identifying associated roles and IS, applicable policies, and related standards to be performed by selected subject matter experts in the organization and coordinated by a program manager in consultation with the relevant business areas.

Timing can also be a critical factor: If the solution is implemented too soon, it may not be understood by the user community and IT functions; if implemented too late, the investment fails to deliver value within the expected timelines. Technology deployment, process adjustment, learning and knowledge absorption, and oversight and management must be carefully synchronized to ensure a successful IDM implementation.

These elements are not simple to manage; however, when they are included in the planning process and considered during all stages of implementation, identity and access management solutions can deliver immense value to any organization that relies on technology to deliver business value.

ENDNOTES

[1] Kampman, Kevin; "Role Management in the Enterprise: Street Scenes," Burton Group, 23 August 2007, *www.burtongroup.com/Research/PublicDocument.aspx?cid=1126*

[2] Identity Management Forum, The Open Group, *www.opengroup.org/idm*

[3] Cser, Andras; Bill Nagel; Stephanie Balaouras; Nicholas M. Hayes; "Identity and Access Management Adoption in Europe: 2009—Uptake of Individual Technologies Is Low, But Cloud Options Hold Promise," Forrester Research, 14 May 2010, *www.forrester.com/rb/Research/identity_and_access_management_adoption_in_europe/q/id/56811/t/2*

[4] Kampman, Kevin; "Characteristics of an Effective Identity Management Governance Program," Burton Group, 22 January 2010, *www.burtongroup.com/Research/PublicDocument.aspx?cid=1731*

[5] See the keynote addresses and the "IAM Foundations: Assessing the Maturity of Your IAM Program" session from the 2010 Gartner Identity & Access Management Summit, *www.gartner.com/technology/summits/na/identity-access/index.jsp.*

[6] These terms are being defined by the authors for the sake of this article. Different etymology is used in the industry, reflecting the lack of maturity and clarity around identity and access management disciplines.

[7] Stachtchenko, Patrick; "Taking Governance Forward," *ISACA Journal*, vol. 6, 2008, *www.isaca.org/archives*

A Framework for Estimating ROI of Automated Internal Controls

Angsuman Dutta is the unit leader of the marketing and customer acquisition support teams at Infogix. Since 2001, he has assisted numerous industry-leading enterprises in their implementation of automated controls by providing assessment, advisory, implementation and support services.

Dan Dopp joined Infogix in 1998 and is responsible for the North American Expansion Initiative. He is a group leader and continues to support the Customer Development Unit responsible for establishing and maintaining relationships with Infogix's European customers. Previously, Dopp held positions at Zurich American Insurance, SunGuard Investment Systems and Northern Trust Co.

Organizations are information-driven and operate in an interconnected economy. With increasing automation of critical business processes, information has become the lifeblood of any business.

In the past, organizations were able to manually verify and audit the accuracy, consistency and reliability of the information they used and exchanged due to low-volume and relatively stable monolithic, mainframe-based information processing environments. With the advent of distributed technology and the adoption of a service-oriented architecture (SOA), data volume and compliance requirements have increased exponentially. The use of manual controls, or semiautomated or homegrown controls, has become costly, obsolete and simply not sustainable. A recent study by KPMG's 404 Institute revealed the prevalence of manual controls in large organizations.[1] More than 50 percent of the companies (the total sample size was more than 1,000) reported that 80 percent of their key controls are manual. About 24 percent of the companies reported that 60 percent of their key controls are manual.

Standardized, independent and automated controls have become business necessities, rather than options. While the value of automated controls in reducing costs, mitigating risks, improving processes and streamlining compliance[2, 3, 4, 5] is unquestionable, organizations need to make investments to develop an infrastructure to support automated controls and to establish a culture of proactive information risk management.

With the exception of controls in a few progressive organizations, controls in most organizations are compliance-driven and often implemented following a risk event. In the absence of any recent, glaring information-error event, control automation projects take a backseat and compete among many organizational priorities. However, the situation changes when executives can establish a strong business case that articulates short- and long-term value propositions of automated controls. The case for automated controls becomes even stronger when presented with appropriate financial metrics such as net present value (NPV), return on investment (ROI) and payback period.

This article establishes the key concepts that can be used as the building blocks of an ROI model. A typical ROI model has two components: time evolution of benefits (the expected benefits of automated controls over time) and time evolution of costs (the initial cost of deployment and recurring costs of operation and maintenance).

EXAMPLES OF INTERNAL CONTROL AUTOMATION

Internal controls are automated for several reasons: cost reduction, risk reduction, efficiency gains and transparency. The following examples[6] showcase how some leading companies use automated manual controls to achieve a positive ROI:

- **General ledger (GL) reconciliation**—A regional bank has about 2,400 GL accounts that it reconciles with its subledger at the end of each month. Prior to automation, the bank had four full-time employees (FTEs) who used data extraction and an Excel-based, manual matching process to reconcile the accounts. In addition to the costs of FTEs, the bank experienced challenges closing its books on time. Typical month-end reconciliation activities took three days because of reliance on manual data capture and manual matching. An automated control solution was deployed to capture data automatically from the subledger and GL systems and to perform automated matching. As a result, the bank was able to reassign three of its resources to research mismatched transactions.
- **File monitoring**—A credit card transaction processing company had a total of 12 FTEs

monitoring the transmission of more than 600 settlement files to more than 400 financial institutions. The timely delivery of the settlement files is critical for the payment settlement process. Failure to deliver the files on time could result in hefty fines and customer dissatisfaction. This particular organization deployed an automated control solution to monitor the file transmission process against a predefined control list, which eliminated the need to manually watch the file transmission process. As a result of this control, the total number of required resources was reduced to three (one for each shift). In addition to FTE-related savings, this organization was able to save close to US $300,000 per year that it had previously incurred due to fines related to service level agreements (SLAs).

- **Duplicate payment detection**—A health insurance company wanted to eliminate the risk of duplicate claims payments. Prior to control automation, the organization sampled 10 percent of its claims payable transactions to detect the presence of duplicates. By deploying an automated controls solution, this organization was able to examine each payable transaction against the current data set and the last 90 days paid transaction data to detect duplicates and fraudulent transactions. This organization was able to detect more than US $5 million in fraudulent transactions. Unlike manual sampling and the audit process, the automated control solution enabled implementation of complex logic to detect duplicate, split and fraudulent transactions.

Typically, areas in which information exists in electronic format are prime candidates for control automation.

ESTIMATING THE BENEFITS OF AUTOMATED CONTROLS

The benefits of automated controls fit broadly in two categories: quantitative and qualitative. While the quantitative benefits make the most powerful argument in a business case, the value of the qualitative benefits should not be ignored. **Figure 1** depicts the four dimensions of benefits, which were developed based on a literature review[7, 8, 9, 10] and the authors' experience in assisting Fortune 500 organizations in developing a business case for automated controls.

The four dimensions of benefits are:

1. **Cost reduction**—Cost reduction refers to all direct and indirect cost savings that are realized as a result of the control automation. At a minimum, the following three types of costs must be considered:

Figure 1—Benefits of Automated Controls

Cost Reduction • Cost of controls • Cost of research • Cost avoidance	**Risk Reduction** • Revenue risk • Cost risk • Reputational risk
Compliance • Lower cost of audit • Reduction in penalties • Increased control effectiveness and coverage	**Process Improvement** • Process cycle time • Complete validation and enterprise visibility • Decision effectiveness

   - Cost of controls—Automated controls can reduce or eliminate the cost of existing manual controls. A typical reduction includes the number of resources needed to perform a required control activity. For example, in the file-monitoring example described previously, the credit card transaction processing company estimates a total savings of US $720,000 per year as a result of nine FTE reductions.
   - Cost of research—Organizations spend time and effort to research and resolve exceptions detected by controls. Automated controls preserve the complete audit trail and streamline the research-and-resolve process. For example, a property and casualty insurance company had engaged two resources to research and resolve issues identified through its general ledger reconciliation process. By automating the reconciliation process, this company was able to identify and isolate all mismatched transactions, resulting in a 50 percent reduction in its research and resolution effort.
   - Cost avoidance—The high cost of manual and internally built controls forces many organizations to accept risks. For example, organizations may resort to sampling only techniques because verifying the entire data set is costly and time-consuming. Automated controls enable organizations to avoid the costs that they would otherwise incur if they chose to address the identified risks. For example, a wealth management financial organization used to engage five resources to validate the accuracy of its monthly statements produced for its high-net-worth customers. Prior to automation, this organization used to sample only 10 percent of the statements. With control automation, this organization was able not only to reduce the number of FTEs required for statement validation, but also to verify 100 percent of the statements.

2. **Risk reduction**—Risk is defined as any event that can negatively impact the intended outcome, and is estimated as the product of the impact and the probability of the adverse event. Automated controls reduce information risk by reducing either the impact (by detecting an error early in the process) or the probability (by detecting errors). In addition to financial impacts, risks can adversely affect the reputation of the company in the long term. At a minimum, the following three types of risks must be considered:
   - Revenue risk—Organizations lose revenue due to information risks present in their revenue chain. Examples of such risks include missed billing and underbilling.
   - Cost risk—Organizations incur additional costs due to information errors in their core processes. Examples of such risks are duplicate payments and overpayments.
   - Reputational risk—Errors in information exchanged with customers, suppliers, business partners, regulators and the public result in loss of reputation and, in some cases, penalties. Examples include financial restatements and customer complaints.
3. **Compliance**—Compliance costs continue to rise due to internal and external audits, changing regulation standards, a greater need for risk containment, and the need to ensure material accuracy in financial statements and other reporting. The cost of the audit and violations of SLAs are examples of the cost of compliance. Automated controls reduce the cost of compliance by reducing the cost of the control audit and testing, by reducing the penalties from compliance failure, and by providing better coverage to mitigate risks throughout the organization. At a minimum, the following three types of compliance-related costs must be considered:
   - Lower cost of audit—Automated controls are less costly to audit because appropriately designed automated controls are required to be tested only once during the testing period, compared to several times for manual controls. In addition, automated controls reduce the total time required for the audit because they provide a complete audit trail of control execution and resolutions when errors are detected. For example, prior to control automation, one health insurance company spent approximately 50 hours per year for testing each key US Sarbanes-Oxley Act control. Through automation, this organization was able to reduce the control testing time to less than 10 hours per year per control. Given that this organization has more than 200 Sarbanes-Oxley controls to support multiple lines of business in multiple states, it was able to save approximately 8,000 hours of control testing effort through control automation.
   - Reduction in penalties—Automated controls reduce the cost of penalties by detecting errors early and enabling organizations to take corrective actions. This type of savings was exemplified in the file monitoring example described previously.
   - Increased control effectiveness and coverage—Automated controls are more effective for risk mitigation because they are standardized and reusable, which provides a better coverage for mitigating risks throughout the organization. For example, most organizations do not focus on deploying controls in processes that are deemed to be low to medium risks because of the cost of the manual or internally developed controls. The low incremental cost of deploying automated controls in these processes enables organizations to mitigate these risks in an effective manner.
4. **Process improvement**—Automated controls simplify and speed up processes by automating manual steps and manual validations. While the financial value of process improvements is difficult to quantify, their value in developing the business case should not be ignored. Expected process improvements need to be clearly articulated in the business case, and, as applicable, appropriate assumptions need to be made to estimate value. While considering process improvements, the following three types of improvements need to be taken into account:
   - Process cycle time—Automated controls drastically reduce the amount of time required for performing

the control activity. In the GL reconciliation example described earlier, the bank was able to automate data capture and the data-matching process for its GL accounts. As a result, the total time for monthly reconciliation was reduced from three days to 10 minutes.

- Complete validation and enterprise visibility—Automated controls increase stakeholder confidence by validating 100 percent of the transactions and by providing enterprise visibility into control actions. An auditor/business-process owner can go to one central monitoring portal to validate that the controls are running as designed. In cases in which control exceptions occurred, the auditor/business-process owner will see what went wrong, when it went wrong, who was alerted and how it was resolved.
- Decision effectiveness—Accurate trustworthiness of information with a complete audit trail provides better insight for making effective decisions.

SUMMARIZING THE BENEFITS OF AUTOMATED CONTROLS FOR ROI

Once all dimensions of the benefits of automated controls are analyzed, the benefits need to be quantified using a template similar to what is shown in **figure 2**. Financial numbers presented in this template are representative of the

Figure 2—Sample Automated Controls Benefits Template

Value of Controls	Yearly Savings	Comments
Cost Savings		
Control automation savings	1,000,000	Currently, there are 10 FTEs.
Exception research savings	500,000	Currently, there are 5 FTEs.
Cost of paper and postage	100,000	Estimated
Cost of computer resources usage for reruns	100,000	Estimated
Cost of call center spikes resulting from errors	100,000	Estimated
Cost of recovery services	100,000	Estimated based on historical data
Subtotal	**1,900,000**	
Risk Reduction		
Average amount of underbilled	100,000	Estimated
Excess costs incurred due to overpayments	100,000	Estimated based on historical data
Value of protecting company brand	10,000	Estimated
Avoided public relations expenses	10,000	Estimated
Value of information accuracy assurance	10,000	Estimated
Cost of acquiring new customers	10,000	Estimated
Subtotal	**240,000**	
Compliance-related Benefits		
Number of manual controls to be audited	200	
Audit cost savings	520,000	Estimated based on historical data
SLA-related cost savings	200,000	Estimated based on historical data
Value of increased controls effectiveness	10,000	Estimated
Value of avoided regulatory attention	-	Estimated
Anticipated cost of regulatory fines	-	Estimated
Value of avoided restatements	25,000	Estimated
Subtotal	**755,000**	
Improvement of Business Process(es)		
Value of higher throughput and speed	10,000	Estimated
Subtotal	**10,000**	
Total recurring yearly savings	2,905,000	

estimations made by a leading Nordic bank to automate more than 5,000 internal controls in its technology, operation and financial processes.

ESTIMATING THE COSTS OF AUTOMATED CONTROLS

Accurate and complete estimations of costs associated with controls are as important as the benefits estimated in developing a reliable business case. Each element of the cost should be evaluated. Care should be taken in estimating a one-time cost and a recurring cost. Critical cost components that need to be considered include:

- **Cost of hardware and supporting software**—Initial cost of hardware and supporting software. Not only are initial hardware costs a factor, but the costs for continued support and software updates need to be considered as well.
- **Cost of automated control software**—Yearly license cost of the automated controls software
- **Cost of implementation**—Cost of the initial implementation and ongoing maintenance
- **Cost of training**—Cost of training resources for controls development and operation

SUMMARIZING THE COSTS OF AUTOMATED CONTROLS FOR ROI

Once all dimensions of the costs are analyzed, the costs of automated controls must be quantified using a template like the one shown in **figure 3**.

FINANCIAL MODEL FOR ESTIMATING THE ROI

The cost-benefit analysis estimated earlier needs to be presented using appropriate financial models. Most organizations are interested in the following financial information:

- **Initial investment**—Maximum amount of investment required to start seeing benefits
- **NPV**—Net present value of all estimated future benefits
- **Break-even period**—Time required for offsetting the project cost/investments
- **Internal rate of return**—Average annual ROI earned through the life of the investment

To estimate the previously mentioned key indicators, one should build a 10-year cash-flow statement that captures the benefit and cost of automated controls. In **figure 4**, it was assumed that the organization started realizing the benefits of automation from the third quarter of the second year.

Figure 3—Sample Automated Controls Costs Template

Cost Estimation		Automated Information Controls	
Type of Cost		First Year	Recurring
Hardware		100,000	20,000
Software:			
	Control software license	500,000	500,000
	Third-party software license	100,000	100,000
	Support	0	50,000
Initial implementation:			
	External consultants	500,000	0
	Internal resources	250,000	0
Training		20,000	20,000
Ongoing management		0	200,000
Total Cost		**1,470,000**	**890,000**

Assuming a 3 percent inflation rate and 10 percent cost of capital, one can use **figure 4** to estimate the following key financial indicators:

- Initial investment required: US $1,470,000
- NPV: US $10 million
- Break-even period: 30 months
- Internal rate of return: 94 percent

UNDERSTANDING NONFINANCIAL VALUES

In addition to the ROI, it is important to capture the key nonfinancial values:

- Increased confidence in the financial information
- Enterprisewide view of the controls and controls results
- Enhanced information exception management process

CONCLUSION

With the accelerating changes in the source systems that support business needs, increasing reliance on information for critical business operation and decisions, and an expanding (and ever-changing) array of regulations and compliance requirements, the use of automated controls is no longer an option. It is the only way to ensure information accuracy across the enterprise. To develop a compelling business case, organizations should follow the following steps:

- Quantify the benefits of automated controls.

Figure 4—Sample 10-year Cash Flow Statement											
	Automated Controls Cash Flow Statement (in thousands)										
	Year										
Value Statement	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**9**	**10**
Cost reduction	0	950	1957	2016	2076	2138	2203	2269	2337	2407	2479
Risk reduction	0	120	247	255	262	270	278	287	295	304	313
Compliance cost	0	378	778	801	825	850	875	902	929	956	985
Process improvement	0	5	10	11	11	11	12	12	12	13	13
Total Value	**0**	**1453**	**2992**	**3083**	**3174**	**3269**	**3368**	**3470**	**3573**	**3680**	**3790**
Cost Statement											
Hardware	100	20	21	21	22	23	23	24	25	25	26
Software	600	650	670	690	710	732	754	776	799	823	848
Implementation	750	0	0	0	0	0	0	0	0	0	0
Training	20	21	21	22	23	23	24	25	25	26	27
Ongoing management cost	0	200	206	212	219	225	232	239	246	253	261
Total Cost	**1470**	**891**	**918**	**945**	**974**	**1003**	**1033**	**1064**	**1095**	**1127**	**1162**
Cash Flow	-1470	562	2074	2138	2200	2266	2335	2406	2478	2553	2628

- Articulate the intangible benefits of automated controls.
- Quantify the costs of automated controls. Consider both one-time cost and recurring costs.
- Develop a financial model to project the ROI.
- Summarize key findings using a business case.
- Present the business case to all key stakeholders.

ENDNOTES

[1] 404 Institute, *Maintaining Your Control Environment in Turbulent Times, Fifth Annual Benchmark Study*, KPMG LLP, USA, 2009

[2] Whitehouse, Tammy; "The Next Goal in SOX Compliance: Automation," *Compliance Week*, 1 April 2008

[3] Miller, Danny; *Automated Controls Strategy, Implementation & Practical Examples*, Grant Thornton LLP, USA, 2008

[4] Ronald, Holly; "Operational Excellence through Internal Controls," *Financial Executive*, 1 November 2007, *www.allbusiness.com/company-activities-management/management-risk-management/5844373-1.html*

[5] Scott, Mitchell; "Automated Controls And Risk Management," *Compliance Week*, 27 March 2007

[6] These examples are taken from the authors' experiences in the field.

[7] *Op cit*, Whitehouse

[8] *Op cit*, Miller

[9] *Op cit*, Ronald

[10] *Op cit*, Scott

The Significance of the Dodd-Frank Act

Larry Marks, CISA, CGEIT, CRISC, CFE, CISSP, PMP, is a member of ISACA's Governmental and Regulatory Agencies Regional Area 4 Subcommittee, and is also a member of the following US Technical Advisory Groups (TAGs): International Organization of Standardization (ISO)/ Technical Committee (TC) 236—Project Management Institute (PMI)—Program Management, ISO/ International Electrotechnical Commission (IEC)/Joint Technical Committee (JTC)/Working Group (WG) 6—Information Security, and ISO/TC 247—Fraud Countermeasures and Controls. He is also a member of the Association of Certified Fraud Examiners (ACFE) Editorial Advisory Review Committee and is vice chair of the ACFE Foundation Scholarship Committee.

In 2008, the global financial system was melting down. A result of the crisis was the US Dodd-Frank Act, which arose from numerous congressional hearings, commissions and other proposals. At more than 2,300 pages, the Act requires that new formal rules be adopted by 11 different regulatory agencies, all within a year and a half of its passage.[1] The new requirements are being phased in over time. No time frame for implementation of Dodd-Frank has been set. On 4 May 2011, the US House Agriculture Committee passed a bill to increase the statutory deadline by 18 months to give regulators the time and data they need to develop thoughtful guidelines without making substantive changes to the intent of the Dodd-Frank Act.

Myron S. Scholes, professor of finance, emeritus, in the Graduate School of Business at Stanford University (California, USA), indicates that infrastructure to support financial innovations, as suggested by economic theory, will, by and large, increase the chances that controls will be insufficient at times to prevent breakdowns in governance mechanisms.[2] It would be too expensive to build all of the information links, legal rules, risk management controls and so forth in advance of new product introductions.

The relevant questions that need to be asked are: How does the Dodd-Frank Act impact IT auditors? How does the Dodd-Frank Act impact global organizations?

PROVISIONS OF THE DODD-FRANK ACT THAT MAY IMPACT IT AUDITORS

A review of a brief summary of the Dodd-Frank Act (hereafter referred to as the Act) prepared by the US Senate[3] and the results of a recent research study prepared by more than 40 professors from New York University Stern School of Business (USA) found that the Act appears to impact IT auditors in the following areas:[4]

1. **Corporate governance**—The Act provides shareholders with a voice on corporate affairs with a nonbinding vote on executive compensation and golden parachutes.[5]
2. **Funeral plans**—The Act requires large, complex financial companies to periodically submit plans for their rapid and orderly shutdown should they go under. Companies will be hit with higher capital requirements and restrictions on growth and activity, as well as divestment, if they fail to submit acceptable plans. These plans will help regulators understand the structure of the companies they oversee and will serve as a road map for shutting down a company if it fails. Significant costs for failing to produce a credible plan create incentives for firms to rationalize structures or operations that cannot be unwound easily.[6] Auditors review the adequacy and completeness of disaster recovery and contingency plans prepared and executed by IT management. These plans are also evaluated by external regulatory authorities. The need for funeral plans will require IT auditors to review the company's shutdown procedures.
3. **Confusion as to governmental authorities**—The Act does not identify a central agency or authority that will be accountable for ensuring compliance. Instead, the responsibility is shared. As a result, the potential for conflicting and inconsistent requirements between agencies exists, which then complicates the evaluation of internal controls, processes and technologies. It becomes difficult because coordination with other agencies regarding their requirements and standards is a necessity.
4. **Financial stability oversight council**—The Act establishes an oversight group, called the Financial Stability Oversight Council. The council will be chaired by the Treasury secretary and will include the Federal Reserve Board, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Housing Finance Agency (FHFA), the National Credit Union Administration (NCUA), the new Consumer

Financial Protection Bureau, and an independent appointee with insurance expertise. The council is responsible for identifying and responding to emerging risks throughout the financial system. Also, the Office of Financial Research and member agencies of the council will collect and analyze data to identify and monitor emerging risks to the economy and make this information public in periodic reports and testimony to the US Congress each year.[7] A reasonable question to ask is whether the emerging risks to the economy will and should include risks to the IT infrastructure of enterprises, such as vulnerabilities and threats to their cybersecurity networks, social engineering, data leakage, lack of patch management procedures, and lack of ITIL Service Management processes. One can guess that the response to this query is negative, and that the risks included in the scope of the council's purview will be primarily financial.

5. **Fills regulatory gaps**—The Act requires hedge funds and private equity advisors to register with the SEC as investment advisers and provide information about their trades and portfolios necessary to assess systemic risk. These data will be shared with the systemic risk regulator, and the SEC will report to Congress annually on how it uses these data to protect investors and market integrity.[8] The question is whether the hedge funds will:
   - Update their procedures to ensure the accuracy and completeness of regulatory reporting of portfolio positions
   - Track and monitor the financial risk of their trading and principal positions, where appropriate
   - Reduce their IT risk, e.g., disaster recovery, to their infrastructure based on a tighter definition and latitude of system risk that they can incur
6. **Disclosure**—Requires nationally recognized statistical ratings organizations to disclose their methodologies, their use of third parties for due-diligence efforts and their ratings track records.[9] The question is whether and how this affects the status of the Statement on Auditing Standards (SAS) No. 70 standard issued by the American Institute of Certified Public Accountants (AICPA) and used by firms to ensure the quality of services offered by their clients and service bureaus.

   In April 2010, the AICPA published Statement on Standards for Attestation Engagements (SSAE) No. 16, to supersede the existing guidance (SAS 70) for performing an examination of a service organization's controls and processes, with an effective date of 15 June 2011. SSAE 16, *Reporting on Controls at a Service Organization*, updates the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard, International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*.

   A service auditor's report with an unqualified opinion offers several benefits, including:
   - It differentiates the service organization from its peers by demonstrating the establishment of control objectives and effectively designed control activities.
   - It can help a service organization build trust with its user organizations (i.e., customers).
   - Without a current service auditor's report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A service auditor's report ensures that all user organizations and their auditors have access to the same information; in many cases, this will satisfy the user auditor's requirements.[10]

   The differences noted by SSAE 16 are as follows:[11]
   - The assertions in SSAE 16 are similar in nature to SAS 70 audit management representation letters. A separate management representation letter is also still required.
   - For Type II reports, the service auditor's opinion on fair presentation of the system and suitability of design will be for the period covered by the report; under SAS 70, this is currently as of a point in time.
7. **Better disclosure**—Requires issuers to disclose more information about the underlying assets and to analyze their quality.[12] This requirement does not impact the degree and quality of information being released to the SEC at this time.

HOW THE DODD-FRANK ACT MAY IMPACT GLOBAL ORGANIZATIONS

Given the global nature of financial markets and competition among major banks, how organizations will be impacted internationally by the Dodd-Frank Act is not yet known. For example, the Dodd-Frank Act requires all firms to disclose the permissibility of hedging their stock and option positions. Further, some believe that international cooperation in regulation is needed to prevent financial firms from arbitraging the market for human capital through choice of jurisdiction. The international Group of Twenty (G-20) Finance Ministers and Central Bank Governors put in place a set of agreed-upon principles on compensation that address three layers of governance at significant financial institutions: managerial performance and risk incentives, corporate governance, and regulatory oversight. The international Financial Stability Board proposed to operate in tandem the:

- Creation of a board remuneration committee
- Endorsement of a limit on total variable compensation
- Review by regulatory supervisors of compensation policies to guard against institutional and systemic risk

The international impact of the Dodd-Frank Act is intertwined with efforts by the G-20 to control system and institutional risk.

CONCLUSIONS

At this time, the Dodd-Frank Act, along with other reforms issued by the US Congress and other regulatory agencies, attempts to address the systemic risk that impacted the US economy several years ago. The impact of this act on regulatory reporting infrastructure by firms will not be seen for at least several years. One chief information officer at a global fund manager told *Wall Street & Technology* that there is not enough information about Dodd-Frank for his firm to comment. "The legislation is long and complex at 2,307 pages, 16 titles and 540 sections. To back the provisions of the act, dozens of new boards, bureaus and offices must be created."[13] One can expect the following: raising budgets or financial companies trying to work around this regulation via spinoffs and the like.

ENDNOTES

1 Acharya, Viral V.; Thomas F. Cooley; Matthew P. Richardson; Ingo Walter; *Regulating Wall Street, The Dodd-Frank Act and the New Architecture of Global Finance*, New York University Leonard N. Stern School of Business, Wiley Finance, USA, 2011

2 Acharya, Viral V.; Thomas F. Cooley; Matthew P. Richardson; Ingo Walter; *Regulating Wall Street: The Dodd-Frank Act and the New Architecture of Global Finance*, Wiley, USA, 2010

3 US Senate, *Brief Summary of the Dodd-Frank Wall Street Reform and Consumer Protection Act*, USA, 2010, *http://banking.senate.gov/public/_files/070110_Dodd_Frank_Wall_Street_Reform_comprehensive_summary_Final.pdf*

4 *Op cit*, Acharya, Viral V.; Thomas F. Cooley; Matthew P. Richardson; Ingo Walter

5 *Ibid*., page 2

6 *Ibid*.

7 *Ibid*., page 4

8 *Ibid*., page 9

9 *Ibid*., page 10

10 *SSAE 16.com*, "Benefits to Service Organizations," *http://ssae16.com/SSAE16_service.html*

11 Brenner, Bill, "SAS 70 Replacement: SSAE 16," *CSO*, 6 October 2010, *www.csoonline.com/article/622277/sas-70-replacement-ssae-16-*

12 *Op cit*, US Senate, page 14

13 MacSweeney, Greg; "Dodd-Frank's Impact on IT," *Wall Street & Technology*, 8 February 2011, *www.wallstreetandtech.com/regulatory-compliance/229200184*

Prepare for the **2011** CISM Exam

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 December 2011 exam, 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*

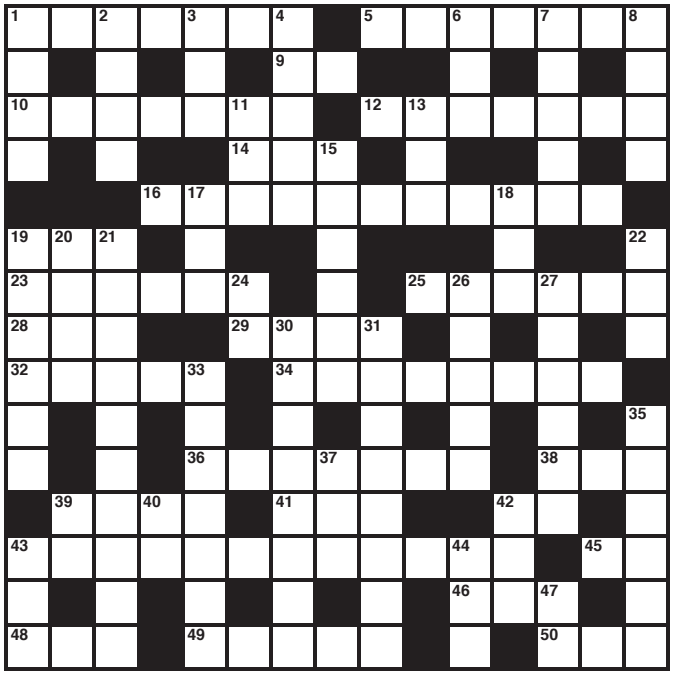
The comprehensive CISM Practice Question Database v11 combines the *CISM Review Questions, Answers & Explanations Manual 2011* with the *CISM Review Questions, Answers & Explanations Manual 2011 Supplement* into a single 750-question study guide. Exam candidates can take sample exams with randomly selected 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 Worm aimed at Iran's nuclear program
5 Smallest discrete amount of some physical property that a system can possess
9 __ track....
10 Pinpoints the problem (two words)
12 Web-based
14 Experimental area
16 One of the major advantages of cloud computing
19 Abampere, for short
23 COBIT process associated with AppDev risk (goes with 25 across)
25 See 23 across
28 Comes before carte
29 Judge
32 Nada
34 Absolutely necessary
36 Performance standards
38 Government organization that recently experienced a security breach
39 Constructed
41 Third-quarter month, abbr.
42 Giant conglomerate that started in electricity
43 Internet disruptions that are predicted to become part of wars
45 Indicates authorship
46 Erode, with away
48 Expert
49 Special market position
50 CD's partner

DOWN
1 Electronics and gaming company
2 Windows alternative
3 Negative utterances
4 Complete
6 Voice
7 "Access, Control, Security and ___" by Shu-Kai Chin and Susan Older
8 Think (over)
11 International legal group, for short
13 Roman 3
15 Financial supporter
17 Part of a machine
18 "This ___ surprise!" (two words)
19 Creators of EC2
20 Java neighbor
21 Capable of being partitioned
22 Put money on it
24 Article checker, for short
26 Gets a cab
27 Subtlety
30 Delighted
31 Lessen the seriousness of a situation
33 Something that is exactly what was needed to achieve a goal (two words)
35 Indian company that collapsed following accounting fraud
37 Ho-hum routine
39 Not yours!
40 ___bug
42 US department that acts as a property manager
43 Organization that is leading the way in relation to cloud security, abbr.
44 Pivotal
47 Train, 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 It is very common for many organisations to have policies on acceptable use of systems, applications and other resources. Often such policies have a tenet stating that limited personal use is allowed. How do you define 'limited personal use'? How do you determine that someone has exceeded the permitted limit? Can any metrics be used to determine whether someone exceeds acceptable limits?

Do you have suggestions in terms of how to make the 'acceptable-use policy' slightly more prescriptive, with a set of controls rather than cryptic statements stating that limited personal usage is allowed?

A Brilliant question, although it does not have an easy answer.

Let us start with a few real-life examples. A CEO of a well-known Irish bank was sacked for exceeding the limit of acceptable personal use of his bank-funded Internet facilities. Whilst on a business trip, sitting in his hotel and using his bank-provided laptop, he browsed some escort-related web sites. Once this became known to the bank, he lost his job. What if the same person had used his employer-provided mobile phone to make calls to an escorting agency? Would it have meant violation of the bank's policy on acceptable use of bank-provided devices and equipment? Or, did it become an issue because the trail left on the laptop was more obvious than some obscure telephone numbers?

In another case, a mayor of a large US city landed in a controversy when more than 14,000 text messages exchanged with one of his colleagues, with whom he had had an illicit affair, became public. At least, in this case, it can be said that the mayor committed an unacceptable act of moral turpitude and landed himself in trouble. Of course, in the process, he used his employer-provided equipment to send 14,000-plus text messages.

Gambling is deemed illegal in some countries, whereas it is perfectly legal in others. So, if an employee chooses to enter a gambling web site, he may be violating the law of the land, in the first place. No employer will tolerate an employee indulging in something illegal. The same act might be considered acceptable in countries in which the law does not expressly forbid gambling. It can be an act of immorality, depending on the value system, but it may not be illegal in the eyes of the law.

Any act of browsing that crosses the acceptable law of the land can fall under 'limited personal use'.

The following parameters can be used to define the limits of acceptability:

- Personal use of business-owned or business-provided resources must not involve something illegal. Once someone crosses the boundaries set by law, even a small amount of personal use cannot be justified.
- The usage must not result in loss of productivity. Employees are paid to do a job, and expectations are set clearly on the quantum and quality of their deliverables. If employers see a downtrend in both the quantity and quality of an employee's deliverables, browsing the Internet during normal business hours, setting aside or according low priority to assigned work can be a possible reason for such decreases.
- Any act of personal use of company equipment must not result in excessive consumption of other resources, again leading to potential business impact, e.g., causing the systems to be slow or less responsive. Bandwidth consumption due to excessive browsing of videos on the Internet might be an issue, for example. This is particularly valid in some countries in which Internet bandwidth is both costly and a scarce resource.
- Company resources must not be put to use to do something that can be deemed unethical. For example, using employer-provided e-mail systems to aid insider trading. Such scenarios do not fall under limited-personal-use criteria.
- Any act of moral turpitude using company resources is unacceptable. See the previous example.

- Imagine a scenario in which an employee uses his company-provided e-mail ID to post some material or content on the Internet that could be deemed offensive, e.g., committing an act of racial or sexual discrimination. In such a case, the act of the employee can potentially defame the company as well, and have detrimental impact on its brand.

The point is that it is not always about excessive use of company resources. Even a personal act of an employee using company resources can land its employer in trouble. Let us take an actual incident that occurred in the UK: When an employee quit a law firm, her previous boss wrote an e-mail to his colleague stating that she could be replaced with a 'busty blonde'. The person who left the organisation somehow got hold of this e-mail, and, as a result, the company paid thousands of UK pounds in damages.

Each organization may have its own definition of 'limited personal use', but it is safe to say that, generally, limited personal use is about doing some occasional online shopping or travel booking or paying some bills. The act must be done infrequently, must not consume excessive resources, and must not violate any legal or ethical requirements.

Q&A

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 Smita Totade, Ph.D.,
CISA, CISM, CGEIT, CRISC

QUIZ #138

Based on Volume 3, 2011—Data Miners

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

TRUE OR FALSE

CADREGARI AND CUTAIA ARTICLE

1. Generally, most laws and regulations require an enterprise to prove that its cloud provider (or application service provider [ASP], Software as a Service [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 them.
2. The recent study done by the Ponemon Institute regarding the cost and frequency of cybercrimes shows that the companies surveyed had at least two successful cybercrimes perpetuated against them per week and that the annual cost of managing those attacks exceeds US $5.8 million.

BROWN AND PIKE ARTICLE

3. A recent 2010 survey by Financial Executives International (FEI) and KPMG found that responders could attain an implementation deadline of 2014, if the International Financial Reporting Standards (IFRS) decision is made in 2011.
4. The most difficult IFRS standards are those that require fair values, external data or key assumptions to be made to implement the standards.
5. 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.
6. 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 low or medium impact on IT systems, whereas only 27 percent of private companies expected a low or medium impact.

WENIG AND KIM-REINARTZ ARTICLE

7. Having to deal with large data sets and a growing variety of audit questions makes time the most essential resource for auditors.
8. Audit routines cannot be predefined and are then generally not applicable—worldwide, cross company or, at least within the core processes, independently of the business areas of an enterprise.
9. 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.
10. Subject matters that are fairly definable and measurable facilitate automated audit testing.

GOLDBERG ARTICLE

11. As the audit 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.
12. In terms of financial auditing, the key financial system's reliability directly, with an inverse relationship, affects the amount of testing necessary.
13. Internal audit does not opine on the company's financial results, but performs compliance tests on financial balances to verify Relevance, Accuracy, Completion and Fairness (RACF).
14. IT plays a key role in the assessment of risk in the planning stage of the audit year, but not in each audit.

VAN DER MOLEN ARTICLE

15. The Internet is vulnerable if nodes are attacked in ascending order of their number of links to other nodes.
16. Percolation theory is not appropriate for malware because a computer can be simultaneously infected by multiple exploits and yet remain operational.
17. Because a computer can be infected more than once by the same malware or simultaneously infected by different malware, the Susceptible, Infected, Recovered (SIR) model is more suitable to describe the spread of malware.
18. Because all antivirus (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.

ISACA Journal
CPE Quiz
Based on Volume 3, 2011—Data Miners

Quiz #138 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC# _____

Quiz #138

True or False

CADREGARI AND CUTAIA ARTICLE

1. _____
2. _____

BROWN AND PIKE ARTICLE

3. _____
4. _____
5. _____
6. _____

WENIG AND KIM-REINARTZ ARTICLE

7. _____
8. _____
9. _____
10. _____

GOLDBERG ARTICLE

11. _____
12. _____
13. _____
14. _____

VAN DER MOLEN ARTICLE

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

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

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

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

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

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

Answers—Crossword by Myles Mellor

See page 49 for the puzzle.

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

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

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 December 2011 CISA exam.

CISA REVIEW MANUAL 2011

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

QAE-11	English Edition	(900 Questions)
QAE-11C	Chinese Simplified 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

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

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 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

MDB-11	CD-ROM – English Edition	(750 Questions)
MDB-11W	Download – English Edition (no shipping charges apply to download)	(750 Questions)

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 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 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.

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.

ACCESS CONTROL, SECURITY, AND TRUST: A LOGICAL APPROACH
Shiu-Kai Chin, Susan Beth Older

Access Control, Security, and Trust: A Logical Approach equips readers with an access control logic that they can use to specify and verify their security designs. Throughout the text, the authors use a single access control logic based on a simple propositional modal logic. The first part of the book presents the syntax and semantics of access control logic, basic access control concepts, and an introduction to confidentiality and integrity policies. The second section covers access control in networks, delegation, protocols and the use of cryptography. In the third section, the authors focus on hardware and virtual machines. The final part discusses confidentiality, integrity and role-based access control. Taking a logical, rigorous approach to access control, this book shows how logic is a useful tool for analyzing security designs and spelling out the conditions upon which access control decisions depend. 2010, 351 pages. **48-CRC**

INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE FOR GLOBAL EXECUTIVES, LAWYERS AND TECHNOLOGISTS
NEW
Thomas J. Shaw Esq. (Editor)

Today more than ever, legal practitioners need to fully understand the obligations, liabilities, risks and treatments involving information security and privacy. Top executives must have a firm grasp of the information security and privacy statutes and regulations in each country where they do business, including any industry sector-specific rules. This book provides a practical and comprehensive approach to information security and privacy law for both international and domestic statutes. It provides all the tools you need to handle the business, legal and technical risk of protecting information on a global scale. For anyone responsible for or advising a corporation involved in domestic or international business, who must comply with a dizzying array of statutes, regulations, technologies, methodologies and standards, this book is the invaluable resource you've been looking for. 2011, 424 pages. **2-ABA**

IT AUDIT, CONTROL, AND SECURITY
NEW
Robert Moeller

When it comes to computer security, the role of auditors today has never been more crucial. Auditors must ensure that all computers, in particular those dealing with e-business, are secure. The only source for information on the combined areas of computer audit, control, and security, the book describes the types of internal controls, security, and integrity procedures that management must build into its automated systems. This very timely book provides auditors with the guidance they need to ensure that their systems are secure from both internal and external threats. 2010, 667 pages. **90-WACS**

IT CONTROL OBJECTIVES FOR CLOUD COMPUTING: CONTROLS AND ASSURANCE IN THE CLOUD
NEW
ISACA

Cloud computing has become an important emergent issue in business today. As a follow-up to the whitepaper issued in October 2009, ISACA has produced this book to examine assurance in the cloud. The focus is on controls and countermeasures that can be used in the cloud, but it also closely examines how to use the cloud to create value in systems. The book details the issue, why it is important to business, risks, why assurance is critical and how COBIT can help.

The book contains an audit program in the appendix, which is also available as a Word document. 2011, 190 pages. **ITCOC**

IT STRATEGIC AND OPERATIONAL CONTROLS
NEW
John Kyriazoglou

Nowadays, integrated information systems can significantly magnify the accrued benefits of a given project and greatly strengthen an organization, but such benefits are balanced by a serious risk. If IT systems are not used in a disciplined manner, they can create havoc and frequently bring about unexpected results and catastrophe, as shown by the rise in security incidents and computer-based crimes. Written with practicality and convenience in mind, this book is an ideal tool for those without specialized technical expertise who are seeking to understand IT controls and their design, implementation, monitoring, review and audit issues. This book provides a comprehensive guide to implementing an integrated and flexible set of IT controls in a systematic way. It can help organizations to formulate a complete culture for all areas that must be supervised and controlled—allowing them to simultaneously ensure a secure, high standard whilst striving to obtain the strategic and operational goals of the company. 2010, 686 pages. **6-ITSOC**

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**

SAP SECURITY AND RISK MANAGEMENT, 2ND EDITION
NEW
Mario Linkies, Horst Karin

The revised and expanded second edition of this best-selling book describes all requirements, basic principles and best practices of security for an SAP system. Readers will learn how to protect each SAP component internally and externally while also complying with legal requirements. Furthermore, the book describes how to master the interaction of these requirements to provide a holistic security and risk management solution. Using numerous examples and step-by-step instructions, this book teaches the reader the technical details of implementing security in SAP NetWeaver. 2010, 726 pages. **2-SAPP**

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
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**

IDENTITY MANAGEMENT: CONCEPTS, TECHNOLOGIES, AND SYSTEMS
NEW
Elisa Bertino, Kenji Takahashi

Digital identity can be defined as the digital representation of the information known about a specific individual or organization. Digital identity management technology is an essential function in customizing and enhancing the network user experience, protecting privacy, underpinning accountability in transactions and interactions, and complying with regulatory controls. This practical resource offers readers an in-depth understanding of how to design, deploy and assess identity management solutions. It provides a comprehensive overview of current trends and future directions in identity management, including best practices, the standardization landscape and the latest research finding. Additionally, readers are given a clear explanation of fundamental notions and techniques that cover the entire identity life cycle. 2011, 194 pages. **10-ART**

PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS
Joe Weiss

Aimed at both the novice and expert in IT security and industrial control systems (ICS), this book will help readers gain a better understanding of protecting ICSs from electronic threats. Cybersecurity is getting much more attention and SCADA security (supervisory control and data acquisition) is a particularly

important part of this field, as are distributed control systems (DCS), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs), and all other field controllers, sensors, drives and emission controls that make up the "intelligence" of modern industrial buildings and facilities. 2010, 327 pages. **1-MPPI**

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

Deloitte Touche Tohmatsu Research Team and 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**

CISA EXAMINATION REFERENCE MATERIAL

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

CISM EXAMINATION REFERENCE MATERIAL

Study aids available in Japanese and Spanish for the 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.

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**

CYBERCRIMES: A MULTIDISCIPLINARY ANALYSIS

NEW

Sumit Ghosh, Elliot Turrini (Editors)

Designed to serve as a reference work for practitioners, academics and scholars worldwide, this book is the first of its kind to explain complex cybercrimes from the perspectives of multiple disciplines and to scientifically analyze their impact on individuals, society and nations, holistically and comprehensively. In particular, the books shows how multiple disciplines concurrently bring out the complex, subtle, and elusive nature of cybercrimes; how conventional laws and traditional thinking fall short in protecting organizations from cybercrimes; and how to transform the destructive potential of cybercrimes into amazing innovations in cyberspace that can lead to explosive technological growth and prosperity. 2011, 414 pages. **2-SCC**

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

HONEYPOTS: A NEW PARADIGM TO INFORMATION SECURITY

NEW

R. C. Joshi, Anjali Sardana

A well-rounded, accessible exposition of honeypots in wired and wireless networks, this book addresses honeypots from a variety of perspectives. Case studies enhance the practical understanding of the subject along with strong theoretical foundation. The book covers the latest technology in information security and honeypots, including honeytokens, honeynets and honeyfarms. Topics include denial of service, virus, worms, phishing, and elaborates on virtual honeypots and forensics. Practical implementations as well as current state of research are discussed. 2011, 340 pages. **49-CRC**

MOBILE APPLICATION SECURITY

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

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**

CREATING A CULTURE OF SECURITY (E-BOOK)

NEW

Steven J. Ross, Risk Masters and ISACA

No security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted. Therefore, if stakeholders are not grounded in a culture of security, there is potential for improper actions. The culture determines what an enterprise actually does about security (or any other objective) and not what it intends to do. An effective security culture supports the protection of information while also supporting the broader aims of the enterprise. To sustain a security culture, it is critical to understand whether it was created in a purposeful manner or by accident. A culture of security is not an end in itself, but a pathway to achieve and maintain other objectives, such as proper use of information. The greatest benefit to a culture of security is the effect it has on other dynamic interconnections within an enterprise. It leads to greater internal and external trust, consistency of results, easier compliance with laws and regulations and greater value in the enterprise as whole.

Creating a Culture of Security by Steven J. Ross, Risk Masters discusses how to achieve a meaningful, intentional security culture. It provides information on the benefits of, and inhibitors to, a culture of security. It discusses positive and negative reinforcement strategies and the steps to take to achieve the right balance in a security culture program. 2011, 140 pages. **WCCS**

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

GREEN IT IN PRACTICE, 2ND EDITION

NEW

Gary Hird

This best-selling practical book helps managers to navigate the confusing mass of information surrounding Green IT with greater ease. Focusing on the experience of implementing the John Lewis Partnership's Green IT program, it contains a host of valuable ideas for establishing and formalizing a green IT initiative. Benefits of the book include:

- Understand the link between general corporate social responsibility and green IT
- Finding out how best to construct appropriate policies and metrics
- Practical tried and tested tips on how to engage with employees and suppliers
- An insight into other people's experiences through in-depth case studies
- A deeper appreciation of just how IT can begin to enable carbon footprint reduction in an organization as a whole.

2010, 128 pages. **7-ITGR**

IMPLEMENTING THE PROJECT MANAGEMENT BALANCED SCORECARD

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**

IT GOVERNANCE: A POCKET GUIDE

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: 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 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**

IT SERVICE MANAGEMENT: IMPLEMENTATION AND OPERATION

NEW

Ahmad K. Shuja

IT Service Management: Implementation and Operation focuses on how to achieve the best return from an IT service management implementation investment, in the least possible time. It discusses the key challenges organizations experience as they leverage ITIL Version 3 to achieve desired transformations and includes the approaches adopted to address those challenges. It includes templates, checklists, implementation patterns and detailed plans for each pattern to kick start implementation efforts.

Detailing the components needed to implement, operate and optimize ITIL service management, the text explains the organizational architecture required to achieve business-IT integration within ITIL. Complete with case studies, examples, problems and access to additional resources on the author's web site, the book illustrates how to achieve service management excellence with ITIL in a way that is seamless to customers and enables the delivery of business value effectively, visibly and efficiently. 2010, 554 pages. **47-CRC**

KEY PERFORMANCE INDICATORS (KPI): DEVELOPING, IMPLEMENTING, AND USING WINNING KPIS, 2ND EDITION

NEW

David Parmenter

By exploring measures that have transformed businesses, the author has developed a methodology that is breathtaking in its simplicity and yet profound in its impact. Now in an updated and expanded Second Edition, *Key Performance Indicators* is a proactive guide representing a significant shift in the way KPIs are developed and used, with an abundance of implementation tools.

Now including a discussion of critical success factors, as well as new chapters that focus on implementations issues and 'how to sections' on finding your CSFs and brainstorming the performance measures that report progress within the CSFs, *Key Performance Indicators*, Second Edition will help you identify and track your organization's KPIs to ensure continued and increased success. 2010, 320 pages. **91-WKPI**

MONITORING INTERNAL CONTROL SYSTEMS AND IT

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**

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

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

Peter A. High

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

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

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

ISACA Bookstore Price List

2011 CISA® EXAM REFERENCE MATERIALS

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

Code	Title		Nonmember	Member
CISA Review Manual 2011*				
CRM-11	English Edition		$135.00	$105.00
CRM-11C	Chinese Simplified 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-11C	Chinese Simplified 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-11ES	English Edition	(100 Questions)	60.00	40.00
QAE-11CS	Chinese Simplified 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 **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 **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 (No charge to paid CGEIT exam registrants)	15.00	5.00

2011 CRISC EXAM REFERENCE MATERIALS

◆ *To prepare for the **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

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
48-CRC	Access Control, Security, and Trust: A Logical Approach	100.00	90.00
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
2-ABA	Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists	106.00	96.00
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
90-WACS	IT Audit, Control, and Security	95.00	85.00
	IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud		
WITCOC*	E-book – PDF Format (purchase online only)	50.00	FREE
ITCOC*	Print Format	60.00	35.00
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
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
6-ITSOC	IT Strategic and Operational Controls	70.00	60.00
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
1-RIA	Practical IT Auditing with current Supplement	420.00	410.00
2-SAPP	SAP Security and Risk Management, 2nd Edition	80.00	70.00
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
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
10-ART	Identity Management: Concepts, Technologies, and Systems	110.00	100.00
	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

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

CISM Examination Reference Material
Study aids available in Japanese and Spanish for the 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
2-SCC	Cybercrimes: A Multidisciplinary Analysis	199.00	189.00
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

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

ISACA Bookstore Price List

Code	Title	Nonmember	Member
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
49-CRC	Honeypots: A New Paradigm to Information Security	150.00	140.00
29ST-3	The Little Black Book of Computer Security, 2nd Edition	35.00	25.00
21-MMS	Mobile Application Security	60.00	50.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00
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	100.00	90 .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
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
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
WCCS*	Creating a Culture of Security (e-book)	50.00	FREE
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
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
7-ITGR	Green IT in Practice, 2nd Edition	60.00	50.00
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
47-CRC	IT Service Management: Implementation and Operation	80.00	70.00
91-WKPI	Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs, 2nd 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
15-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
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. 5 -11

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

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

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

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

Customer Information

Name _____
FIRST MIDDLE LAST/FAMILY

ISACA Member: ☐ No ☐ Yes Member Number _____

Company Name _____

Address: ☐ Home ☐ Company

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

Fax Number ( ) _____

E-mail Address _____

Shipping Information (If different from customer information)

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

Name _____
FIRST MIDDLE LAST/FAMILY

Company Name _____
(IF PART OF SHIPPING ADDRESS)

Address: _____

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

E-mail Address _____

Code	Title/Item	Quantity	Unit Price	Total

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

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

Payment Information—Prepayment Required

☐ Payment enclosed. Check payable to "ISACA" in US dollars, drawn on US bank.

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

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

Credit Card # _____

Exp. Date _____

Print Cardholder Name _____

Signature of Cardholder _____

Shipping & Handling Rates for Orders

All orders outside the US are shipped Federal Express Priority.

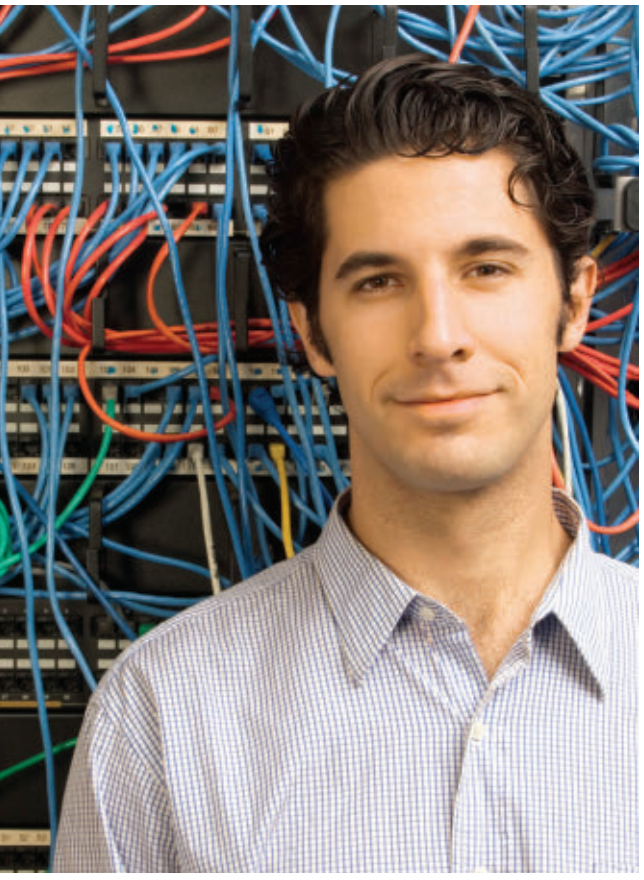
For Orders Totaling	Outside US	Within US
Up to US $30.00	US $10.00	US $5.00
US $30.01 to US $50.00	US $15.00	US $7.00
US $50.01 to US $80.00	US $20.00	US $8.00
US $80.01 to US $150.00	US $26.00	US $10.00
Over US $150.00	17% of Total	10% of Total

No shipping charges apply to *Meycor COBIT*.
No shipping charges apply to CISA Practice Question Database v11—download.
No shipping charges apply to CISM Practice Question Database v11—download.

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

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

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