VOLUME 6, 2010

ISACA® Journal

Challenges of a Changing Landscape

Featured articles:

Criteria for Evaluating and Selecting Continuous Controls Monitoring Solutions

Show Me the Money! Three Ways to Better Partner With Finance

Building a Business Case for Records Management

And more...

ISACA®
Trust in, and value from, information systems

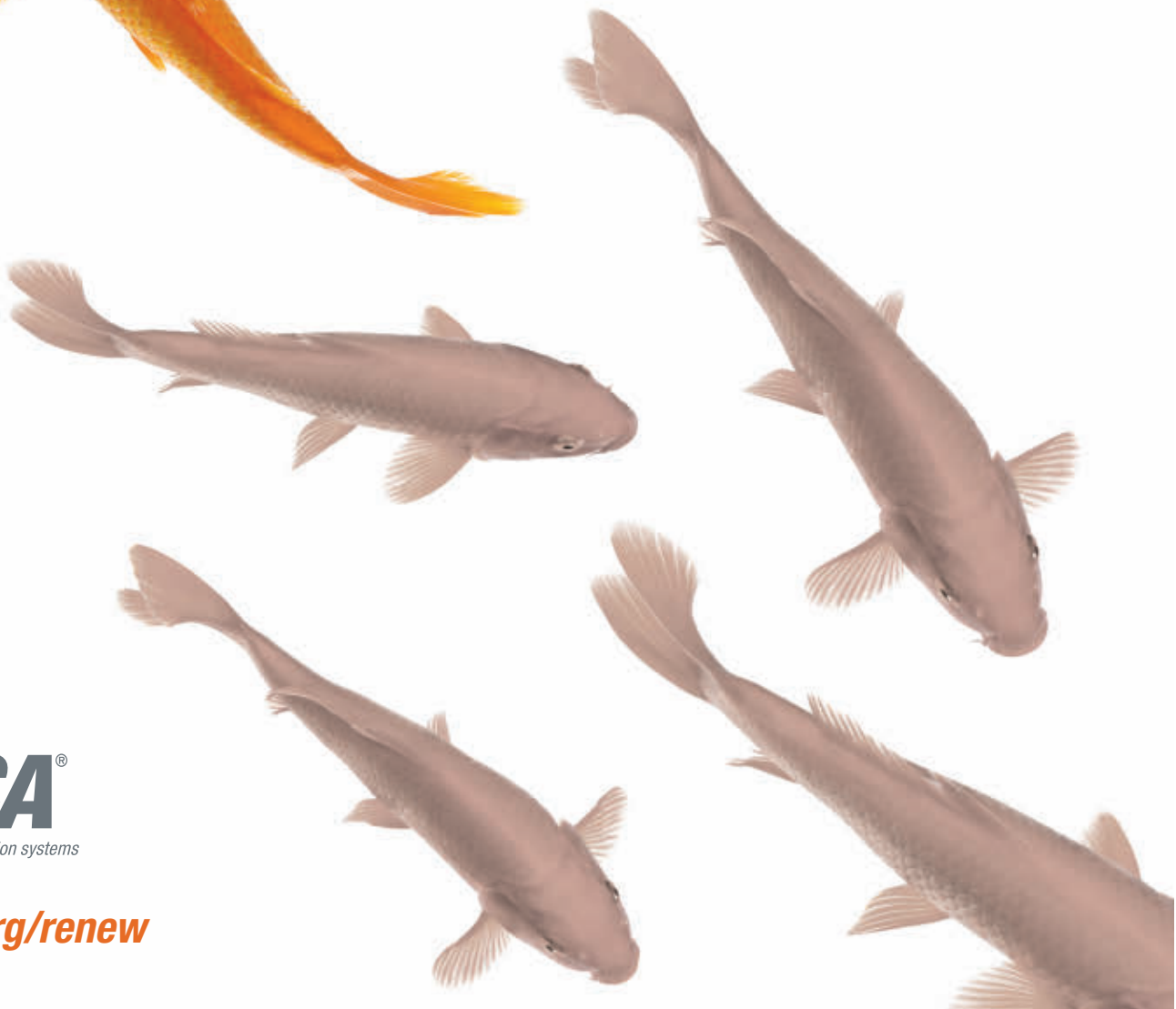
WWW.ISACA.ORG

ISACA members get recognized

In a sea of IT professionals, ISACA members get noticed.

Many IT and information systems professionals worldwide consider membership in ISACA® essential to their career advancement. ISACA connects exceptional people with exceptional knowledge to provide members with a robust offering of professional resources.

Don't miss any benefits in 2011. Renew your ISACA membership today!



ISACA®

Trust in, and value from, information systems

www.isaca.org/renew

MODULO Risk Manager

Comprehensive solutions from the experienced global leader in GRC management

Benefits of Modulo Risk Manager™:

- Complete visibility into risk, compliance and security posture

- Comprehensive integrated platform that automates the entire GRC management lifecycle

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

Contact us

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

MODULO Solutions for GRC
Governance, Risk and Compliance
25 Years

Volume 6, 2010

ISACA® Journal

Columns

Features

Plus

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

Read more from these *Journal* authors...

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

Journal Online

Want more of the practical, peer-reviewed articles you have come to expect from the *Journal*? Additional online-only articles will be available on the first business day of each month in which no *Journal* is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA® members during their first year of release. Use your unique member login credentials to access them at *www.isaca.org/journalonline*.

Online Features
The following articles will be available to ISACA members online on 1 December 2010.

Book Review: Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions
Reviewed by Carlos Villamizar Rodriguez, CISA, CGEIT, ISO 27001 LA, BS 25999 LA

Emergency Access Controls in SAP Environments
Jose Espin, CISA, CISSP, MCP, SAP Certified Security Consultant

Information Security Automation: The Second Wave
David Ramirez, CISA, CISM, CISSP, BS 7799 LA, MCSE, QSA

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

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

Flexibility . . . Knowledge . . . Growth

ISACA®

Trust in, and value from, information systems

Service Availability and Disaster Recovery

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

Bad things happen to good information systems. That is how life is; everything is moving along swimmingly and then, KA-POW, nothing is moving at all. It is impossible to prevent all bad things from happening; all that can be done is to devise ways to rebound when they do occur. Some organizations are content to wait until something goes wrong before figuring out what to do. This may be fine for small businesses with little information, long lead times for their transactions and extensive insurance policies. Any organization with a lot of data in use all of the time and that must be available shortly following a disruption must plan for recovery in advance of the aforementioned bad things.

PLANS AND PLANNING

If it were only clear which bad things were going to happen, this would all be much easier. But it is in the nature of bad things not to let on; that is one of the things that make them bad. This necessitates planning for many more bad things than actually will occur and probably in a greater degree of detail than will be necessary at the time. But to quote former US president Dwight D. Eisenhower, "The plan is nothing. Planning is everything."[1] In information systems terms, Eisenhower's dictum means that consideration of needs and acquisition of necessary resources are more important by far than a neatly printed emergency manual.

Organizations must devise *emergency response plans* for the immediate period following an incident, with the emphasis on preserving human life and safety and only secondarily on information resources. A *crisis management plan* guides management in making and executing decisions to minimize the effect on an organization until operations return to normal. A *business continuity plan* prepares organizations to carry on vital (and ultimately all) operations under adverse circumstances.

DATA LOSS AND DOWNTIME

The speed and volatility of modern business create some confusion regarding disruptions to and recovery of information systems, as well as the recovery of the organizations that depend on them. For what exactly are plans needed? Total destruction? Inaccessibility? Application mishaps? Only long interruptions or short ones, too? Will one plan adequately address all exigencies?

A *disaster recovery plan*, as applied to information systems, is intended for response to a catastrophic event that destroys all or most of a data center, renders it inoperable or impossible to reach. This is the so-called "smoking hole" scenario. Of course it is a plan for extreme circumstances, but there have been too many floods, hurricanes, toxic spills, terrorist attacks, fires and airplanes crashing into data centers to discount such events on the basis of rarity. They are credible threats and must be addressed. Briefly stated, organizations need an alternate data center with the right equipment, current data and a network to reach them. They need a set of processes for transitioning and carrying on operations in the alternate data center. Oh, yes, and they need all these things at a price that management considers prudent and affordable.

Questions arise in trying to make the "smoking hole" plan apply to lesser disruptions, such as failures of equipment, software or network services. Is an organization that is prepared for disasters *ipso facto* ready to deal with interruptions of service? Or, put another way, are service availability and disaster recovery the same or different concerns and can one plan suffice to deal with both? Is a *service availability plan* the same as a plan for recovering from disasters?

If there is anything positive to be said for a disaster, it is that, as with the sight of the gallows, it wonderfully concentrates the mind. There are no wherefores and maybes; a smoking hole is a powerful inducement to action. The same cannot be said of system failures. A virus, for example,

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.

may cause a service interruption, but it is not disastrous in a physical sense. System failures may go on for some time before anyone realizes which failure caused a disruption. It may be necessary to diagnose what has caused an outage in order to fix it; the same cannot be said of a physical disaster.

More central to the discussion is that the responses necessarily differ, or at least they do most of the time. The operative principal of disaster recovery is to go where the disaster is not. For service interruptions, it generally makes more sense to stay in one place and fix the problem. But one critical element unites them: in both cases, it is essential to have current data. This leads to the determination of how timely the data must be or, viewed differently, how much data can an organization acceptably do without?

This question leads backward to requirements and forward to solutions. There are some business activities that require that not a bit of data be lost. In financial services, millions may be made or lost in seconds, so loss of the data generated in those seconds is unacceptable. Lives are at stake in hospitals and the military, so these industries have similar needs. But, for most organizations, and all organizations some of the time, a little loss—minutes to hours or even days—is tolerable. Similar considerations apply to the determination of acceptable downtime.[2]

RISK AND AFFORDABILITY

> "The more downtime and data loss approach zero, the higher the cost will be."

It may be fairly stated that the more downtime and data loss approach zero, the higher the cost will be. The cost is based on having alternate locations with backup equipment and on capturing the data in multiple locations. It also stems from the disk and tape storage required to hold all the data, the network to transport them and the repository in which to store them.

Who, then, is to make the decision regarding risk tolerance and affordability? Business managers are supposed to set the limits of acceptability, but they are often so swayed by the cost of reducing data loss that they understate their needs. Business continuity and disaster recovery managers should respond to business drivers; they are often in no position to contradict the stated needs of business leaders, even if they fear that their organizations are underprepared.

What is needed is a programmatic approach to managing all outages, whether they are caused by disasters or lesser events. At issue are not the causes but the effects, such that disaster recovery and service availability merge, albeit incompletely. No disaster will cause seconds of downtime and no operational problem would be allowed to continue for weeks. In the middle, though, it is possible to evaluate the ramifications—in financial, operational and reputational terms—of outages of various durations with data losses of various magnitudes. Business managers should not be asked how much loss their functions can tolerate, but rather how much money will be lost in seconds, minutes, hours and days of downtime. How badly will operations be disrupted? How much effect will there be on customer and public confidence? If the impact falls within certain ranges, the decision on funding continuity of service, regardless of the cause, should be made impartially and systematically for the business.

In short, bad things can be made better by careful and skillful analysis beforehand. There need to be plans for both disasters and service outages. Very short-term and very long-term disruptions should be seen as extremes that must be planned for separately. If these are called disaster recovery and service availability plans and are kept in two different drawers of the same desk, no harm done. Outages that fall in between—for more than minutes but less than weeks—are the ones most likely to be faced. In this case, the disaster recovery and service availability plans had better say the same things.

ENDNOTES

[1] Dwight David "Ike" Eisenhower was the leader of Allied forces in Europe in World War II and served as President of the United States (1953-61). I have seen this quote in various forms, but the gist of it is always the same, putting the emphasis on planning over the product of the process.

[2] Astute readers of this column will recall, from previous columns in this space, the terms "recovery point objective" and "recovery time objective" and consider them in this paragraph.

YOUR

SUPPORT

TEAM'S

SILVER BULLET.

QUICK ON THE DRAW

AND

QUICK TO SOLVE!

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

GoToAssist® EXPRESS™

by CITRIX®

Try It FREE for 30 Days

www.gotoassist.com/isaca

Data Extraction, A Hindrance to Using CAATs

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CMA, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998-1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the *ISACA Journal*.

Almost all auditors agree that a key tool in conducting audits, especially fraud and IT audits, is the use of a computer-assisted audit tool (CAAT). There are many factors that go into the effective and efficient use of CAATs in IT audits, including technology issues, social/personnel issues, choosing the right CAAT, defining the data to extract and making sure audit objectives drive the use (or fit) of a CAAT.

Anecdotal evidence suggests that one of the primary hindrances, if not *the* prime one, of using CAATs is in getting the data from the operational system into the IT auditor's CAAT. This article will center on data extraction, focusing on the most efficient methods given the current state of features among the leading CAATs vendors.

IDEAL IMPORT FORMAT

The ideal format of data being imported into a CAAT is generally a flat file in which the first row contains the column headings and the second row begins the data set and in which the data set (rows) is contiguous until the end of the data (see **figure 1**). That is, subtotals, breaks and subheadings create situations where data have to be "cleaned" or manually manipulated into the ideal format. This format is the goal of data extraction, regardless of the specific methodology.

DATA EXTRACTION DATA FORMATS

The IT auditor will need to consider the different formats of data available for data extraction and find the best fit for the tool and operational data format. Factors that affect this decision are platform, database/database management system (DBMS) and application software (i.e., the accounting software system).

The data extraction file could be one of several formats, such as dBase, PDF, Excel, Extensible Markup Language (XML), delimited text and open database connectivity (ODBC), to the operational data files. Some of these are easier or more efficient for extraction purposes. Generally speaking, the order of ease with which to work follows the order in **figure 2**.

Caution should be used in converting operational data into some of these formats. For example, when converting data into a PDF file, it is important to make sure that the file is not a scanned image (which will not work). Usually, printing to a PDF file is easier to work with than saving the data as a PDF. Most "heavy duty" CAATs today can read data from a PDF file, even if it is a report filled with breaks, subtotals and extraneous data—in other words, a report in which the data get messy. The CAAT features allow the IT auditor to pick and choose the data with relative ease from the PDF soft-copy document.

When exporting to a text file (ASCII format), systems often add breaks, subtotals or subheadings. The text file should follow the "ideal" format demonstrated in **figure 1**. Also, the fields (columns) should be delimited with a comma (CSV) or tab; for the data to read correctly, a delimiter is usually necessary.

Figure 1—Ideal Data Format for Data Extraction

ID	NAME	ADDRESS	CITY	STATE	ZIP	PHONE	CONTACT	CREDIT LIMIT	BALANCE
1	ABC Co.	101 Main St.	Anywhere	FL	33333	123-4567	Joe	$50,000.00	$24,000.00
2	Cranky Repairs	211 Elm St.	Anywhere	FL	33333	234-5678	Sally	$10,000.00	$1,200.00
3	Mild Soap Inc	314 Oak Ave.	Anywhere	FL	33333	345-6789	Tim	$30,000.00	$5,000.00
4	Sunny Side Home	411 Pine St.	Anywhere	Fl	33333	456-7890	Sue	$25,000.00	$26,000.00

Figure 2—Data File Formats by Order of Efficiency to Import	
File Format	**Type/Use**
dBase	.dbf
Adobe PDF file (not a scanned image)	Export data or print data to a PDF file.
Microsoft Excel file	Export data as an .xls file.
Delimited text file (e.g., CSV)	Export or save as an ASCII/text file, with delimited fields (comma or tab).
XML (XBRL is similar to XML.)	.xml
Others (e.g., bring data file over directly into CAAT)	The others are fairly time-consuming to use.

OPTIONS TO EXTRACT DATA FROM OPERATIONAL SYSTEMS

There are usually one or more ways that a platform/system will allow the IT auditor to pull data from the operational system to extract the data needed. These options will be discussed beginning with the one that is generally considered the most efficient method.

First, one should investigate the export functionality options of the accounting application. Some usual options are "save as" options that include Excel, PDF or text delimited files. If the IT auditor can load a report or data file that contains some or all of the data needed, a save-as option may be available, especially in Microsoft-type systems. It could also be a menu option that allows data to be extracted (e.g., MENU -> FILE -> EXPORT). This option is usually the easiest one to perform, and it can usually export data into the easiest-to-use formats (see **figure 2**). The save-as function can serve as an export function as well.

Sometimes the best approach is to extract the data in one format and then convert it to a PDF file. For instance, a "messy" Excel spreadsheet can be efficiently cleaned up by converting it to PDF (i.e., print to PDF), and then using the CAAT to identify and extract the data from the report.

Second, if necessary, one should investigate the print and report functionalities. For example, many systems allow reports to be printed as a soft-copy file, rather than a hard-copy printout. In the print dialog box, this option would be available if the system allows for "print to file." Print to file creates a text file output of the report. It is important to note that there may be a need to convert the text file into the ideal format (see **figure 1**). A better option is to print to PDF. Many systems have that option, even if Adobe Acrobat is not installed. If the system allows the data file or report to be printed to a PDF soft-copy file, it is important to note that this method is the second-easiest file format (see **figure 2**). Of course, the IT auditor could simply print the data needed to a hard copy and manually key it in to the CAAT, but this option should be used as a last resort as it is time-consuming.

Last, if needed, one should pull the data directly from the operational database into the CAAT. This can be done with ODBC, a dynamic connection from the CAAT to the operational database. It is usually possible to extract the data using Structure Query Language (SQL), because SQL is used by almost all databases. Additionally, XML is becoming a common data extraction and communication tool. Microsoft products and many accounting applications are compatible with XML. But this option requires a few things the others may not require. The IT auditor will probably need a data dictionary to extract data using ODBC, SQL or XML, and the data dictionary may not be readily available.

DATA INTEGRITY

Before using the extracted data in the CAAT, the IT auditor will need some assurance that the data set in the CAAT is identical to the data on the operational system. There are various ways of performing a "crosswalk" or reconciliation, but the IT auditor must make sure to select some reasonable method to ascertain integrity of the CAAT data. Often, this involves something similar to the old batch transmittal sheet methodology. In that methodology, one created metrics about the data set, e.g., number of records, total dollar amount column, total numeric column and other similarly identifiable summary facts.

CONCLUSION

CAATs provide a method for IT auditors that is efficient and effective in meeting audit objectives. In fact, IT audit pioneers stated that the invention of CAATs was the most significant event in the history of IT audit. But that does not necessarily mean that it is always easy to use a CAAT. Perhaps the most difficult step in using a CAAT is getting the data in a usable format in a reasonable amount of time. The information in this article is intended to make that process as efficient as possible with any given platform, database and accounting application.

CPTRAX

Providing Compliance and Control for your Windows® Enterprise.

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

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

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

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

Use CPTRAX to:

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

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

CPTRAX does not use or require Windows® Event Logs.

Download your FREE EVALUATION today!

www.visualclick.com

Visual Click

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

Five Questions With...

Jose Luis Carrera Jr., CFE, CIA

Jose Luis Carrera Jr. has been responsible for directing the internal audit department of Agility Defense & Government Services (DGS), Kuwait City, Kuwait, since 2008. He has more than 19 years of international auditing and internal auditing experience, which he gained from his positions at RSM McGladrey & Pullen LLP; Singer Lewak Greenbaum & Goldstein, a regional certified public accountant (CPA) firm in the Los Angeles, California, USA area; PricewaterhouseCoopers LLP (PwC); and Saudi Arabian Oil Company.

As senior manager of PwC's Global Risk Management Services (GRMS) group, Carrera was responsible for assisting high-tech clients (Microsoft and Nintendo) and international energy clients (Chevron, Saudi Arabian Oil Company and PEDVSA). He also served as senior manager for two SAP and PeopleSoft implementations for three multinational oil and gas conglomerates (Venezuela, Saudi Arabia and UAE) and one federal energy company located in the northwestern US. In addition, Carrera was one of the founding members of the PwC Tiger Teams for SAP System Security and was the exclusive PwC senior manager for the annual cosourced internal audit engagements for Raytheon and Washington Group International.

At RSM McGladrey, Carrera was responsible for directing the Risk Management Consulting Service group of the Desert Southwest Region (USA), and he spent six years in Saudi Arabia as the special audit internal audit manager and information systems internal audit manager of the Saudi Arabian Oil Company.

Carrera has extensive experience in strategic financial performance; organizational behavior; business process improvement and operational efficiency; internal audit outsourcing; risk management; assistance and implementation of sections 302, 404 and 906 of the US Sarbanes-Oxley Act of 2002; and large-scale application and system implementation (budgets in excess of US $200 million). He also has strategic and senior-level management experience,which he gained in the financial, manufacturing, high-tech, government and energy industry sectors.

Carrera is fluent in English and Spanish and is proficient in conversational Arabic. He is a "weekend warrior" on his 2000 Special Edition Harley Davidson Road King motorcycle and has more than 5,000 Cuban cigars in storage. He is also a long-time season ticket holder for the Arizona Cardinals football team. He can be reached at *jlcarrerajr@aol.com*.

Q How has continuous auditing/monitoring changed in recent years? What makes it unique?

A During my tenure in internal auditing and in working for a Big Four international accounting firm, continuous auditing/monitoring (CM) has changed dramatically.When I was introduced to CM, it got its impetus from the academic environment—the type of applications created in Fortran and then punched into cards to be read by the big academic mainframe: an IBM 3081! I can still remember having to run SAS routines that I created to extract and "monitor" complex financial application algorithms in order for me to perform my electronic data processing (EDP) application audits. Fast forward to the last three years, ACL, Structured Query Language (SQL) and other built-in enterprise resource planning (ERP) applets are performing the same function—created in "English speak" and providing "executive business reports" to executive management and the independent business consultative internal audit department for review, evaluation and possible risk mitigation. CM, in my professional career, has provided me a "full-time cyborg" to assist in enterprise risk management planning by updating the planned internal audit engagement. However, the value comes into play when asked by the audit committee to perform that "special project" under their guidance and preview. CM is like the US Navy Seals: Get in and get out.

Q In regard to enterprise risk management, what do you believe is the single largest IT-related risk for businesses today?

A I am a firm believer that enterprise risk management—if performed correctly, combined with CM, and coupled with well-disciplined operational employees who understand their internal control environment

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.

and perform annual control self-assessments, is utopia! The reality in my inner sanctum is that enterprise risk management is performed on an annual basis, and in my position, I spend the entire year, after planning the current year's internal audit plan, convincing the audit committee of what should be performed and requesting additional budget to cover all the low-hanging fruit for the upcoming year.

However, persistence and open communication with the audit committee chair and other executive management is probably the initial step in maintaining a consultative internal audit department that moves into enterprise risk management on a full-time scale. Additionally, creating and maintaining computer-assisted audit technique (CAAT) applications that are embedded and set to provide real-time data to executive management are also evidence that moving risk management into the daily vocabulary of operational management and staff is where we need to be.

Q How would you describe the impact of the increasingly strict regulatory environment on the IT auditor?

A The increasingly strict regulatory environments, from an internal audit profession perspective, definitely keep us on our toes. Increased regulatory oversight, to some extent, is in highly regulatory environments. In other environments, it is the *soup du jour*. You see, when the US Sarbanes-Oxley Act inundated the accounting profession, it was a necessity based on a specific situation that rocked the accounting profession—the demise of Enron and Arthur Andersen. How was that different in the health care field? Are we seeing more regulatory oversight and mandates from the airline industry? I am sure we are going to see an increase in regulatory oversight in the energy industry as a result of the recent BP disaster in the US Gulf Coast, but how would increased IT auditing and ACL applets or denial-of-service (DOS) prevention have assisted in mitigating the events that occurred? It is my personal belief that the more we push regulatory mandates, the more we get away from what "should be" done and, instead, concentrate on what "needs to be done." Internal auditing, including IT, financial, operational and compliance auditing, should work off of sound principles of internal control, checks and balances, and programmed processes.

Q Having lived and worked in numerous cities in the US and Middle East, how would you advise someone considering such a move? What are the biggest challenges and differences that you have encountered in your work in different countries?

A Living and working in numerous cities in this beautiful world has been an adventure, not only for my professional career, but also for my family. It took some convincing for my wife to leave Arizona, USA, and travel to the Kingdom of Saudi Arabia, especially during the Gulf War. Then we returned to the US to work in the beautiful northwestern part of the country, only to be transferred by my employer back to the Grand Canyon state (Arizona). Then we were off to Los Angeles for several years, to again return to Arizona…which then led me to my present employment location, Kuwait City.

The biggest challenges that I have uncovered during my internal audit tenure, away from the US, are twofold:

- First, answering this as a husband and father, I'd say you have to have faith. Do not get me wrong; I am not trying to proselytize, but to state a fact: If you have faith—be it in a higher power or whatever suits you—you must have a strong conviction and be faithful to guide and care for your spouse; children; family network; and, more important, your skill set because there is only one of you, and when the going gets tough, and it will, you need to rely on your convictions.
- Second, if you maintain any recognized international certification, you need to remember your ethics and common sense. The farther away you are from the nest, the birds play at a different level! I have been challenged repeatedly to overlook my ethics and integrity, and fortunately, I do not bend when faced with those critical decisions.

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

A As a chief audit executive, the workplace challenges I have been faced with and continually deal with include:

- Maintaining career satisfaction among IT auditors
- Cultural sensitivity

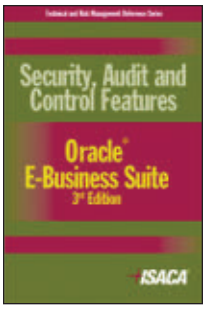
Let's face it, keeping IT auditors engaged as valued members of an integrated internal audit team as well as letting them fulfill highly complex IT internal auditing, for some, takes its toll on the cohesiveness of the internal audit department. This is the fundamental yin-yang internal

audit department theory. An IT auditor who is technically knowledgeable and current with existing technology and platform operating systems requires a challenging and dynamic career path and constant daily interaction. It is challenging for someone in my capacity to keep the revolving door from turning. On the other hand, the talent pool that I have had fill these types of IT audit positions has been very gratifying, with gifted individuals with higher-education credentials and many IT-related certifications.

A more sensitive issue in this part of the world is the religious "overtone" in the work place. Kuwait is a very open country and the Emir has given individuals the opportunity to openly practice several religions in this country. However, for some, this entails more "political correctness" that must be engrained in the workplace, and for others, it is an added bonus. Personally, I live by the golden rule: "If you can't say something nice about someone, don't say it at all." Always engage the synapses before the mouth.

As an American working abroad, I continually remind myself that I am an ambassador for the US, and that I am an ambassador for the internal audit profession as a whole. Never look in the rearview mirror of life. Focus on the oncoming traffic.

Security, Audit and Control Features Oracle E-Business Suite, 3rd Edition



Reviewed by Mustapha Benmahbous, Ph.D., CISA, CISM, chief executive officer of Xpertics Solutions. Benmahbous has more than 20 years of IT experience and more than 10 years of experience actively working with Oracle EBS releases 11*i* and 12. He adopted and used the *Security, Audit and Control Features Oracle® E-Business Suite, 2nd Edition,* within major customer organizations.

Oracle's enterprise resource planning (ERP) software is among the biggest business packages ever released. Designed to automate multiple enterprise and corporate operations and processes, Oracle® E-Business Suite (EBS) is a very large system of more than 130 integrated business applications and IT infrastructure modules. Many organizations looking for robust and integrated solutions adopt this suite. *Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition*, as well as its previous editions, is the major published reference covering the security, audit and control points of view and requirements. Business regulatory compliance and the complexity of EBS technology make this publication a practical tool and source of reference for many audiences, including business executives and managers, IT auditors, and security officers. This publication is also a unique reference that covers specific Oracle EBS Release (R) 12 auditing aspects with a formal methodology, an IT audit framework and a risk-control approach.

Two aspects of the book are of particular note. First, there is a balance between techniques and technology on one side and audit framework and methodology on the other. Second, the "popularization" of ERP auditing concepts with a risk-based audit framework is discussed and working tools and adapted templates are provided. These are based on best practices and models (including Committee of Sponsoring Organizations of the Treadway Commission [COSO], COBIT and the Information Technology Assurance Framework™ [ITAF™]) and are provided to assist in conducting practical audit and assurance activities on EBS built-in processes.

The publication aims to adapt existing auditing techniques into an Oracle EBS context to facilitate the audit "contextualization" with an audit framework and practical information on risks, key controls, testing procedures, etc.

The book is a practical introduction to the management of ERP-based operations and risks within Oracle EBS R12, financial accounting and expenditure business cycles.

The publication discusses newer topics than the second edition. It includes about 150 pages of audit work templates as part of an audit/assurance program. Useful templates are provided for EBS business processes including:

- Audit plans for:
  - The Financial Accounting Business Cycle
  - The Expenditure Business Cycle
  - Oracle Security Administration
- A maturity assessment template to help maturity management of related COBIT control practices
- Internal control questionnaire (ICQ) to build on Oracle EBS processes with references to COBIT practices

These appendices extend the practical aspect and usability of this publication.

Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition, provides a very good audit framework, templates, known risks and common key controls for each EBS process (financial scope). In specific operational circumstances and contexts, there may be additional risks not included in this book and others may not apply. Adaptation to specific situations is the auditor's challenge and still requires appropriate judgment.

EDITOR'S NOTE

Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition, is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650. The audit programs and ICQs appendices from this publication are posted in Word for ISACA members at *www.isaca.org/auditprograms*.

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.

Feature

Criteria for Evaluating and Selecting Continuous Controls Monitoring Solutions

Angsuman Dutta is unit leader of the Customer Acquisition Support Team at Infogix. Since 2001, he has assisted numerous industry-leading enterprises in their implementation of automated information controls by providing assessment, advisory, implementation and support services for Infogix clients.

Bobby Koritala leads the Product Development Group at Infogix. He previously served as the director of risk technology solutions at Protiviti, director of applied technology at Blue Cross Blue Shield, director of product development at Lexis Nexis and senior manager of software development at SPSS.

In the post-US-Sarbanes-Oxley-Act era, many organizations consolidated and integrated corporate governance, risk management and compliance (GRC) activities into a single domain to ensure alignment of all activities. A robust internal control system is used as the primary vehicle for achieving the objectives of GRC. While designed to manage risks, detect and prevent errors, and ensure compliance, existing internal control systems are costly due to reliance on manual controls[1] and nonstandard automated controls.

Recent trends, including an expanding array of compliance requirements, enhanced focus on operational excellence and increased awareness of continuous controls monitoring (CCM), are forcing organizations to take a fresh look at their internal control environments. Many organizations have, or are now in the process of developing, strategies to replace their manual and costly internal controls with automated, reliable and cost-effective controls and controls solutions to effectively mitigate risk.[2] In addition to creating sustainable financial returns, automated controls enable organizations to continuously monitor and audit control activities.

> "The concept of CCM… has been adopted by a few organizations to monitor their critical business information and controls."

The concept of CCM and continuous auditing has been around for the last several years,[3] but has been adopted by few organizations to monitor their critical business information and controls. While these organizations have demonstrated progressive thought leadership in managing financial data, the adoption of CCM solutions in broader market sectors has been somewhat limited due to reliance on manual controls and to lack of awareness, spending and leadership support.

Recent releases concerning monitoring internal controls by ISACA®[4] and the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[5] and the advances made in automated controls have renewed interest in CCM solutions in a large number of organizations, the media and the analyst community.[6, 7] Many organizations are now seeking to further optimize their GRC efforts through the effective use of automated controls and CCM solutions. As organizations review various features and functionalities of CCM solutions, they need to evaluate the short-term goals and long-term objectives. For example, a Fortune 500 organization procured and implemented niche CCM solutions for its payroll application to increase visibility and governance activities following the recommendations of its external auditors. However, this solution was not usable the following year when the external auditor recommended the need for additional oversight of the organization's billing process and credit card settlement process. As a result, the organization had to go through the CCM solution evaluation process again. To achieve alignment with their GRC objectives, organizations need to utilize structured evaluation criteria that meet their GRC automation and optimization objectives.

This article outlines a 10-factor model that may be considered during the CCM solution evaluation process.

1. **Scope of the solution**—The scope of CCM solutions should, at minimum, be aligned with the scope of internal controls systems. Internal controls span financial operations, business operations and technology operations of organizations. Many current market offerings narrowly focus on five to six expense-related financial processes, such as procure to pay, payroll or order management. Others focus on providing monitoring capabilities for the key enterprise resource planning (ERP) system controls. An inability to add new controls as a supplement to ERP controls severely limits the value of a CCM solution. In addition, a narrow focus on ERP controls misses a large portion of the enterprise that uses third-party systems and homegrown applications. The scope of the

selected solution must align with the organization's short-term goals (i.e., controls that the organization wants to monitor in the next four to six months) and long-term strategies.

2. **Capability of the solution**—The best-in-class CCM solution goes beyond controls monitoring by providing robust automated control, controls monitoring and exception management capability. Control capabilities should include the ability to automate transaction, segregation-of-duties and security controls. Controls monitoring capabilities should enable organizations to monitor and manage key controls in real time. In addition, control monitoring capabilities should focus on discovering trends and patterns to gain insight about the underlying process that is being controlled. For example, a transaction processing company not only controls its automated clearinghouse (ACH) payment process to prevent errors, it also trends the total volume of ACH payments and different types of exceptions to understand underlying changes in the business. Controls exception management capabilities should provide workflow to research, resolve the issues identified by the controls, and capture the complete audit trail of the issue resolution process for audit and compliance.
3. **Technical support**—Despite increased adoption of the distributed platform across industries, many critical business applications are still on the mainframe environment. Organizations should assess their critical business processes and opt for solutions that closely align with their technology environment. Controls solutions that focus on only one environment ignore a true enterprise reach, failing to deliver the comprehensive solution to mitigate end-to-end risk. Organizations that have real-time applications should evaluate the ability of the CCM solution to capture and control real-time transactions.
4. **Data processing solution**—Organizations are information-driven, and as organizations continue to experience growth, the data volume will grow in proportion. A best-in-class CCM solution must support processing of high data volume. The technology of the solution should be robust enough to handle current and future transaction loads. Multicompany, multidivision and multicurrency environments should be supported without restrictions, but with historical trends of reliability.
5. **Support for multiple systems**—Finance, operations and technology departments will continue to use myriad applications to support business needs. An enterprise-class CCM solution should provide support for all applications and systems.
6. **Nonintrusiveness**—An ideal CCM solution will seamlessly support enterprise processes and data without requiring any significant changes. Solutions that require changes in data format usually result in longer implementation times and are often costlier to maintain.
7. **Usability of the solution**—Organizations should evaluate the ease-of-use factors of proposed CCM solutions. The following factors must be considered in determining usability:
   - Is the product too complex or sophisticated for the average user?
   - Is a context-based help menu available? Is the menu structure simple to use?
   - Are the results easily accessible for reporting, researching and analyzing?
   - Does the product provide template controls that can be used throughout the organization without any significant changes?
8. **Technology and architecture**—Organizations should also consider aligning the technology architecture and scalability of the solution with their internal standards for ongoing support and maintenance of the solution. In addition, organizations should consider integration of the solution with their security infrastructure and disaster recovery framework.
9. **Product innovation**—With increased adoption and use of CCM solutions, the need for additional features and functions of CCM solutions will continue to evolve. Organizations should continuously evaluate a vendor's ability and willingness to support the product in the long term. In evaluating the organization's commitment to enhanced products, the following factors need to be considered:
   - Percentage of revenue invested in product development
   - Number of major and minor product releases each year, including enhancements and fixes
10. **Return on investment**—Return on investment is vital in any major investment, and a good CCM solution can offer quick payback. The total cost of ownership for a CCM solution includes the cost of implementation and the cost of maintenance. Balance needs to be established between license costs and the functionality offered. A true "implementation services to software" ratio for comparably sized organizations should be established to determine the best value.

CONCLUSION

While CCM solutions open up new possibilities and opportunities to improve GRC processes through control automation, monitoring and exception management, organizations must evaluate their options through the lens of both short-term goals and long-term objectives.

Short-term goals normally revolve around solving a problem that has recently surfaced and cannot be easily mitigated. While it is tempting to achieve a short-term goal through the use of a niche solution specifically designed to solve a particular problem, such an approach is neither scalable nor sustainable. Without a long-term vision, short-term goals may address only immediate needs and may not be cost-effective as the scope of CCM increases.

> "Organizations… must take a strategic approach to evaluating CCM solutions in the context of their needs and goals."

As the CCM space continues to be defined with respect to features and functionalities, appropriate consideration must be given to assessing the needs of organizations. Because of the immense risk and business pressure facing them, organizations can no longer assume that just any market solution can be customized to meet their specific needs, but must instead take a strategic approach to evaluating CCM solutions in the context of their needs and goals. The most effective CCM solutions for a GRC approach should optimize an organization's business and regulatory environments and mitigate risk.

ENDNOTES

[1] Aguilar, Melissa Klein; "404 Study Shows Little Automation Yet," *Compliance Week*, 3 November 2009, *www.complianceweek.com/article/5654/404-study-shows-little-automation-yet*

[2] Tucci, Linda; "Is Continuous Controls Monitoring at the Top of Your GRC Agenda?," IT Knowledge Exchange, 19 February 2010, *http://itknowledgeexchange.techtarget.com/it-compliance/is-continuous-controls-monitoring-at-the-top-of-your-grc-agenda*

[3] ISACA Standards Board; "Continuous Auditing: Is It Fantasy or Reality?," *Information Systems Control Journal*, ISACA, vol. 5, 2002

[4] ISACA, *Monitoring Internal Control Systems and IT*, USA, 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Monitoring-of-Internal-Controls-and-IT-(Exposure-Draft).aspx*

[5] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Guidance on Monitoring Internal Control Systems*, USA, January 2009

[6] Caldwell, French; Paul E. Proctor; "Magic Quadrant for Continuous Controls Monitoring," Gartner, March 2010

[7] Caldwell, French; Paul E. Proctor; "Continuous Controls Monitoring for Transactions: The Next Frontier for GRC Automation," Gartner, January 2009

Data Governance for Privacy, Confidentiality and Compliance:
A Holistic Approach

Javier Salido, CIPP, has 12 years' field experience working with large enterprise and government customers, first as a consultant and later as director of services for Microsoft Consulting in Mexico, Argentina, Chile and Uruguay. A former researcher at the Network Security Laboratory at the University of Washington (USA), Salido has published multiple works at IEEE conferences, in *IEEE/ACM Transactions on Networking* and in the "A Guide to Data Governance for Privacy, Confidentiality, and Compliance" series published by Microsoft Corp. He currently works with the Microsoft Trustworthy Computing Group on privacy-related topics.

The digital era has created unprecedented opportunities to conduct business and deliver services over the Internet. Nevertheless, as organizations collect, store, process and exchange large volumes of information in the course of addressing these opportunities, they face increasing challenges in the areas of data security, maintaining data privacy and meeting related compliance obligations.

Forward-looking organizations are recognizing the need for a holistic approach to meet these challenges. In this context, "holistic" means an approach that enables the organization to address the following three objectives in a unified, cross-disciplinary way, rather than as three separate problems to be addressed by different groups within the organization:

- Traditional IT security approaches that focus on protecting the organization's IT infrastructure by securing the network edge and end points need to be augmented with protective measures that focus specifically on protecting the data that are stored and moved through that infrastructure.
- Privacy-related protective measures must extend beyond those aspects of privacy that overlap with security, to include protective measures that focus on capturing, preserving and enforcing the choices customers have made with respect to how and when their personal information may be collected, processed, used and potentially shared with third parties.
- Data security and data privacy compliance obligations need to be rationalized and addressed through a unified set of control objectives and control activities that meet the requirements.

Such an approach requires cooperation among the IT, human resources, legal and finance departments as well as business groups and the marketing department—in short, any group with a stake in collecting, processing, using and managing personally identifiable information (PII), intellectual property, trade secrets and other types of confidential information.

It is important to point out that the proposed approach to data governance for security, privacy, confidentiality and compliance does not call for modifying or replacing the organization's existing information security management systems or IT governance processes. Rather, it augments them by specifying additional roles, tasks and technical tools that can help organizations better protect data privacy and security and satisfy compliance obligations.

This article presents an overview of the Data Governance for Privacy, Confidentiality and Compliance (DGPC) framework developed by Microsoft to assist organizations in creating a data governance program that addresses all three objectives in a holistic manner.[1] In particular, this discussion focuses on the risk management portion of the DGPC framework.

BUSINESS CASE FOR DATA GOVERNANCE

IT professionals may ask why they would want to employ yet another framework if they already have a successful IT governance process, a well-established control framework and an effective information security management system to meet their security needs and compliance obligations. There are two reasons for this:

- Security standards and control frameworks tend to focus primarily on protecting the overall IT infrastructure and on aligning investments in that infrastructure with the organization's business goals. In other words, they provide a view of the data security "forest." The DGPC framework complements these elements in crucial ways by focusing on the "trees" of data security—on identifying and managing security and privacy risks related to specific flows of data that need to be protected, including personal information, intellectual property, trade secrets and market data. Such focus is necessary to identify additional, data-flow-specific protective measures

and controls that need to be implemented to cover gaps—that is, residual risks that are specific to the data flow and that are not addressed by broader protective measures.
- The DGPC framework creates a context that enables identification of threats against privacy, including privacy threats that do not overlap security threats such as violations of customer choice and consent with respect to what types of personal information are collected and how they are used, processed and shared.

The DGPC framework works in concert with the organization's existing IT management and control frameworks, such as COBIT, and with security standards such as ISO/IEC 27001/27002 and the Payment Card Industry Data Security Standard (PCI DSS). To the author's knowledge, no other existing industry framework provides this combination of benefits and integration.

DGPC FRAMEWORK COMPONENTS

The DGPC framework is organized around three core capability areas: people, process and technology. This section briefly summarizes the first two areas and offers a more detailed look at the technology-related considerations that are integral to threat identification and risk management.

People

Data governance processes and tools are only as effective as the people who use and manage them. An important first step is to establish a DGPC team that consists of individuals from within the organization and give them clearly defined roles and responsibilities, adequate resources to perform their required duties, and clear guidance on the overall data governance objectives. Essentially, this is a virtual organization whose members are collectively responsible for defining principles, policies and procedures that govern key aspects of data classification, protection, use and management. These individuals—commonly known as "data stewards"—also typically develop the organization's access control profiles, determine what constitutes a policy-compliant use of data, establish data breach notification procedures and escalation paths, and oversee other related data management areas.

> "Data governance processes and tools are only as effective as the people who use and manage them."

Process

With the right people involved in the DGPC effort, the organization can focus on defining the processes involved. This begins with examining various authority documents (statutes, regulations, standards, and company policies and strategy documents) that spell out requirements that must be met. Understanding how these legal mandates, organizational policies and strategic objectives intersect will help the organization consolidate its business and compliance data requirements (including data quality metrics and business rules) into a harmonized set.

The next step is to define guiding principles and policies that generate the appropriate context in which to meet these requirements. Last, the organization should identify threats against data security, privacy and compliance in the context of specific data flows; analyze the related risks; and determine appropriate control objectives and control activities.

Technology

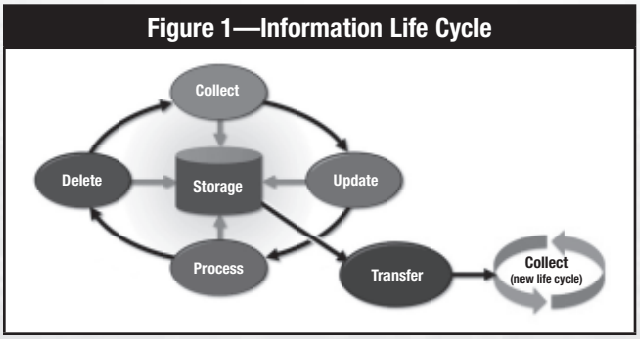
Microsoft has developed an approach to analyze specific data flows and identify residual, flow-specific risks that may not be addressed by the information security management system's and/or the control framework's broader protective measures. This approach involves filling out a form called the Risk/Gap Analysis Matrix, which is built around three elements: the information life cycle, four technology domains, and the organization's data privacy and confidentiality principles. The following sections explain these concepts and discuss how they come together in the Risk/Gap Analysis Matrix.

Information Life Cycle

To identify residual risks and select appropriate technical measures and activities to protect confidential data, an organization must first understand how information flows throughout its systems over time and how the information is accessed and processed at different stages—by multiple applications and people and for various purposes. **Figure 1** illustrates this concept of the information life cycle. Understanding the risks within each life-cycle stage helps clarify what safeguards are needed to mitigate those risks.

Most IT professionals are well acquainted with these life-cycle stages, so discussing them in detail here is not necessary, except for one important facet: the need to include a transfer stage.

Figure 1—Information Life Cycle



As data are copied or removed from storage as part of a transfer, a new information life cycle begins. Organizations should place as much emphasis on security and privacy for data that are being transferred as they do for the original data set. This requires understanding transfer vehicles—such as private networks, the Internet and storage media sent by courier—and their inherent risks. For example, media sent by courier or postal mail can be lost or stolen, so measures such as encryption should be taken to protect the data on those media. Data security also requires understanding how the recipient organization's policies, systems and practices differ from those of the current keepers of the data. If the recipient does not have the same security capabilities and processes as the current keepers of the data, protections may need to be placed on the data or the process before transfer.

Other transfer challenges can arise when individuals and departments run reports or extract subsets of data from centralized databases for processing—particularly if they are using desktop data-mining and analysis tools that generate reports and data sets in the form of document files and spreadsheets. These files can also be easily transferred as e-mail attachments or saved to laptops, handheld smart devices or USB drives. Given that more than 60 percent of US data breaches in 2009 were attributed to lost or stolen laptops or media, organizations should closely monitor and protect such data transfers.[2]

Technology Domains

Organizations also need to systematically evaluate whether the technologies that protect their data confidentiality, integrity and availability are sufficient to reduce risk to acceptable levels. The following technology domains provide a frame of reference for this task:

- **Secure infrastructure**—Safeguarding confidential information requires a technology infrastructure that can protect computers, storage devices, operating systems, applications and the network against malicious software, hacker intrusions and rogue insiders.
- **Identity and access control**—Identity and access management (IAM or IdM) technologies help protect personal information from unauthorized access while facilitating its availability to legitimate users. These technologies include authentication mechanisms, data and resource access controls, provisioning systems, and user account management. From a compliance perspective, IAM capabilities enable an organization to accurately track and enforce user permissions across the enterprise.
- **Information protection**—Confidential data require persistent protection because they are shared within and across organizations. Organizations must ensure that their databases, document management systems, file servers and practices correctly classify and safeguard confidential data throughout the life cycle.
- **Auditing and reporting**—Technologies for systems management, monitoring and automation of compliance controls are useful for verifying that system and data access controls are operating effectively, and they are useful for identifying suspicious or noncompliant activity.

Data Privacy and Confidentiality Principles

The following four principles are meant to help organizations select technologies and activities that will protect their confidential data assets. They are high-level statements that can be followed by more detailed guidance—clear, concise statements or questions that inform the risk management and decision-making process.

- **Principle 1: Honor policies throughout the confidential data life span.**[3] This includes a commitment to process all data in accordance with applicable statutes and regulations, preserve privacy and respect customer choice and consent, and allow individuals to review and correct their information if necessary.
- **Principle 2: Minimize risk of unauthorized access or misuse of confidential data**. The information management system should provide reasonable administrative, technical and physical safeguards to ensure confidentiality, integrity and availability of data.
- **Principle 3: Minimize the impact of confidential data loss**. Information protection systems should provide reasonable safeguards, such as encryption, to ensure the confidentiality of data that are lost or stolen. Appropriate

data breach response plans and escalation paths should be in place, and all employees who are likely to be involved in breach response should receive training.

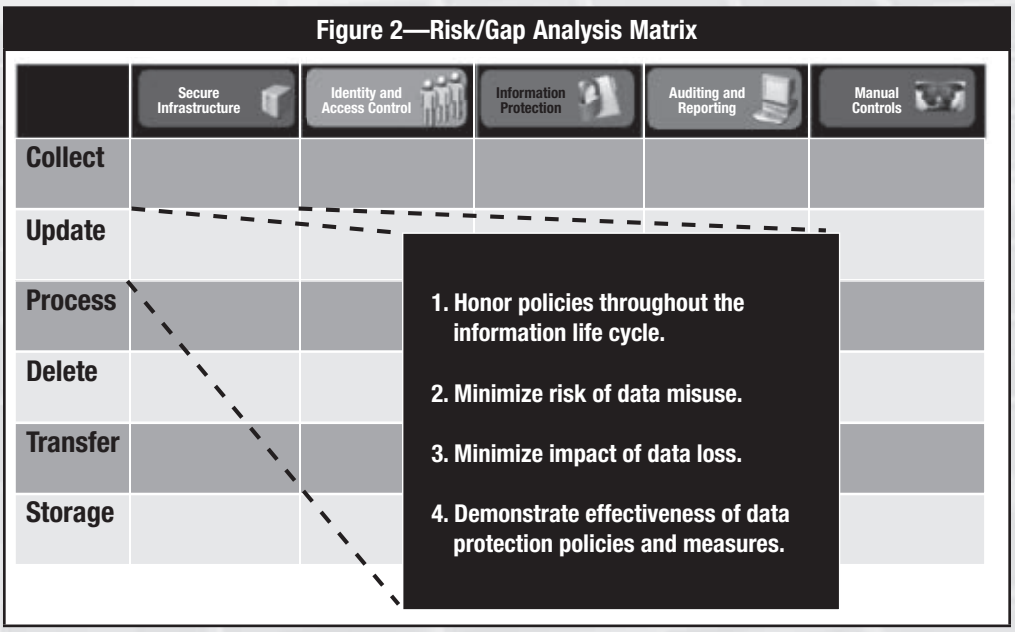
- **Principle 4: Document applicable controls and demonstrate their effectiveness**. To help ensure accountability, the organization's adherence to data privacy and confidentiality principles should be verified through appropriate monitoring, auditing and use of controls. Also, the organization should have a process for reporting noncompliance and a clearly defined escalation path.

The Risk/Gap Analysis Matrix

The Risk/Gap Analysis Matrix, shown in **figure 2**, brings together the information life cycle, technology domains, and data privacy and confidentiality principles in a tool that helps organizations identify and address gaps in their existing efforts to protect data against privacy, confidentiality and compliance threats within a specific data flow. The matrix provides a unified view of the flow's existing and proposed protection technologies, measures and activities.

Each row depicts a stage in the information life cycle. The first four columns in the matrix represent a technology domain, while the far-right column represents manual control activities that must take place to meet the requirements of the four data privacy and confidentiality principles at each stage of the information life cycle. The four principles form the basis of questions that will be asked for every cell of the matrix.

Figure 2—Risk/Gap Analysis Matrix

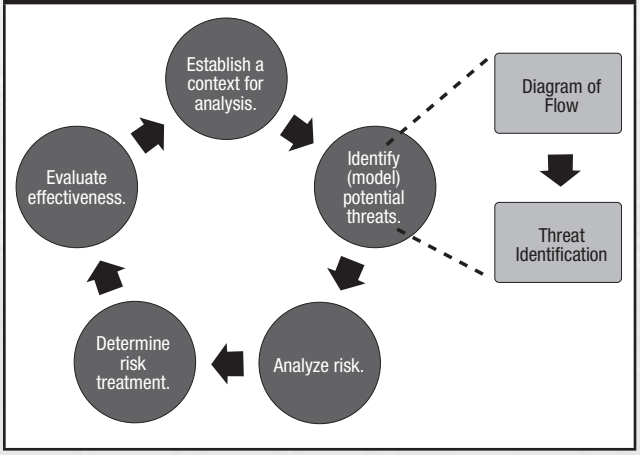


Assessing Risks With the Risk/Gap Analysis Matrix

The matrix gives organizations a powerful tool for risk assessment and mitigation. The analysis process shown in **figure 3** and the following steps can help organizations identify gaps in existing protective measures and select corrective actions:

- **Step 1: Establish the risk analysis context**—This involves defining the business purpose of the data flow; understanding how the data will be used and what systems are involved (defining the use cases); and identifying the privacy, security and compliance objectives for the flow.
- **Step 2: Perform threat modeling**—Most threat-modeling techniques focus on security threats only, so they must be modified to detect nonsecurity-related threats involving privacy and noncompliance. Threat modeling involves two phases:
  - Diagramming involves creating a graphical representation of the data flow. Multiple techniques can be used for diagramming. Microsoft's product teams and consulting services organization typically use data flow diagrams (DFDs) with the addition of "trust boundaries." As shown in **figure 3**, a trust boundary is a border that separates business entities and/or IT infrastructure realms, such as networks or administrative domains. In this scenario, a customer provides PII to the application servers, which store it in servers administered by a cloud provider. Every transaction is logged in a log server that is administered by the same entity that administers the application servers. Every time confidential data cross a trust boundary, basic assumptions about security, policies, processes or practices—or all of these combined—may change, and, with them, the threats that will be identified in step 3. Note that in the diagramming step, the modeled entities typically represent systems and data stores rather than individual processes depicted in "traditional" application security threat modeling. A detailed description of

Figure 3—Risk/Gap Analysis Process



DFDs and trust boundaries can be found in the "Microsoft IT Infrastructure Threat Modeling Guide."[4]

– Threat enumeration is a systematic analysis of the threat diagram, an example of which follows. In this context, a threat is not limited to attackers or technical threats, but can refer to anything that may violate any of the four data privacy and confidentiality principles. Organizations should use these principles to define categories of threats, as shown in **figure 4**, which is an example of the output that results from applying threat enumeration to the data flow shown in **figure 5**. The exact definition of the categories will depend on the organization's unique policies and the applicable industry, geography and legal compliance framework.

Figure 4—Collection and Update Stages in the Risk/Gap Analysis Process

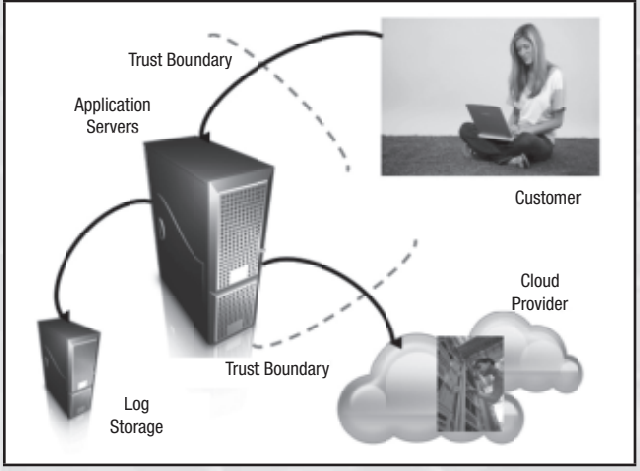


Figure 5—Threat Identification

Threat Type	Specific Threat
Choice and consent	Options have to be displayed clearly in order to obtain appropriate consent.
Access and correction	Customer is not able to view/modify personal information.
Accountability	Customer PII is not properly classified.
Compliance	Compliance reports are not defined; escalation path to business owners is not specified.
Information protection	Customer information is sent in the clear, over an unauthenticated channel.
Data quality	Quality depends on customer; no threat is identified.

The following is a threat enumeration example of what the definition of the threat categories described in step 2 may look like:[5]

– Principle 1: Honor policies throughout the confidential data life span.
  • Choice and consent (collection, use and disclosure)
    - Inadequate notice of data collection, use, disclosure and redress policies
    - Unclear or misleading language or processes for the user to follow in choosing and providing consent for the collection and use of personal information
  • Individual access and correction
    - Limited or nonexistent means for users to verify the accuracy of their personal information
  • Accountability
    - Lack of controls to enforce customer choice and consent as well as other relevant policies, laws and regulations

– Principle 2: Minimize risk of unauthorized access or misuse of confidential data.
  • Information protection
    - Lack of reasonable administrative, technical and physical safeguards to ensure confidentiality, integrity and availability of data
    - Unauthorized or inappropriate access to data
  • Data quality
    - Inability to verify accuracy, timeliness and relevance of data
    - Inability of users to make corrections as appropriate

– Principle 3: Minimize the impact of confidential data loss.
  • Information protection
    - Insufficient safeguards to ensure the confidentiality of data if they are lost or stolen
  • Accountability
    - Lack of a data breach response plan and an escalation path
    - Lack of system encryption of all confidential data
    - Inability to verify adherence to data protection principles through appropriate monitoring, auditing and use of controls
– Principle 4: Document applicable controls and demonstrate their effectiveness.
  • Accountability
    - Improper documentation of plans, controls, processes or system configurations
  • Compliance
    - Inability to verify or demonstrate compliance through existing logs, reports and controls
    - Lack of a clear noncompliance escalation path and process
    - Lack of a breach notification plan and other response plans that are required by law

Identifying these threat types offers a starting point for organizations to assess their data flows and consider how assumptions about privacy, confidentiality and compliance may change when a flow crosses a trust boundary, such as during transitions between life-cycle phases.

- **Step 3: Analyzing risk**—Most organizations have already taken some steps to ensure data security and privacy, as specified by their existing control framework and/or information security management system. To complete this step, the organization should first gather information about its existing protective controls, technologies and activities. Then, for each cell in the Risk/Gap Analysis Matrix, it should determine which controls, technologies and activities support compliance with each of the four privacy and confidentiality principles. This step concludes when the threats that are not addressed by existing protective measures are identified in the appropriate cells of the matrix and when the related risks have been evaluated.
- **Step 4: Identifying mitigation measures**—In the appropriate cells of the matrix, organizations should list additional controls, technologies and activities that are necessary to bring each risk to an acceptable level, and then evaluate the cost/benefit of each. This step concludes when the organization decides whether and how each identified risk will be mitigated, transferred or assumed.
- **Step 5: Evaluating the effectiveness of mitigation measures**—Organizations should review the results of the preceding steps and reinitiate the cycle if unacceptable risks remain (**figure 6**).

Figure 6—Identified Mitigation Measures

	Secure Infrastructure	Identity and Access Control	Information Protection	Auditing and Reporting	Manual Controls
Collect/ Update	*Servers are on regular OS and App. Patch cycle, and up to date in malware signatures.* *Incoming data are correctly classified and tagged as per customer choice and consent.*	**All transactions to take place on authenticated communications.**	*Choices are displayed and consent is obtained as per MPSD guide.* *Transaction log data are encrypted in transit and at rest.* **All material customer transactions arrive over encrypted communication channel.**	*All material transactions are to be logged as per logging framework.* *Communications channel and log servers are monitored. Failover process to local log servers in processor facilities is up and running.* **Alerts and alert recipients are defined and operational.** **Access and use reports, along with recipients and delivery schedules, are defined.**	**The escalation path for issues is defined.**

CONCLUSION

As organizations manage growing volumes of confidential data, they face increasingly complex challenges in protecting the data against theft, misuse or unauthorized disclosure. In addition, organizations need to take steps to prevent accidental collection or use of customer and employee personal information, in violation of each individual's preferences, and also to meet related compliance obligations.

A program based on the Data Governance for Privacy, Confidentiality and Compliance framework complements existing security standards and control frameworks by providing a holistic approach to identifying data-flow-specific threats against data privacy, security and compliance and by addressing residual risks in effective and efficient ways.[6]

This article provides a high-level overview of the three components of the DGPC framework—people, process and technology—and a more detailed summary of key aspects of the technology component:

- The use of data-centric threat modeling for security, privacy and compliance that complements but does not substitute for "traditional" security threat modeling, which is application-/process-centric.
- The selection of appropriate controls, technologies and activities that address flow-specific residual risks through the use of the Risk/Gap Analysis Matrix. This is a simple tool that can help organizations understand how different technologies and protective measures come together in the context of an application's information life cycle to treat the aforementioned risks.

ENDNOTES

[1] For more information about the DGPC framework, see the white papers and webcasts of the series "A Guide to Data Governance for Privacy, Confidentiality, and Compliance," available at *www.microsoft.com/datagovernance*.

[2] Open Security Foundation DataLossDB, *http://datalossdb.org*

[3] These policies may consist of requirements derived from laws, standards, promises, individual customer or employee choices, commercial obligations, and other sources.

[4] For a detailed description of "traditional" threat modeling and how to build data flow diagrams, see "Microsoft IT Infrastructure Threat Modeling Guide," available from *http://technet.microsoft.com/en-us/library/dd941826.aspx.*

[5] For a more detailed list of technical and nontechnical questions that illustrate the types of threats against each principle, see the Application Privacy Assessment questionnaire available at *www.microsoft.com/privacy/datagovernance.*

[6] To learn more about Microsoft's DGPC framework and how Microsoft tools can be used to identify and mitigate gaps in existing protective measures, visit *www.microsoft.com/datagovernance.*

Show Me the Money! Three Ways to Better Partner With Finance

Brian G. Barnier, CGEIT, with ValueBridge Advisors, has a practical and action-oriented perspective as a result of his experience in business lines, IT and risk management. He serves on multiple best practice committees. He conducts professional education courses, was an adjunct professor of finance, is one of the select Open Compliance and Ethics Group (OCEG) Fellows, is widely published, and contributed to *Risk Management in Finance* (Wiley, 2009). In prior roles, he was with IBM, Lucent and AT&T. For ISACA, he chairs the IT Governance, Risk and Compliance Conference Program Committee. He can be reached at *brian@valuebridgeadvisors.com.*

In the movies, there are simple formulas. In an action film, it is good vs. evil fighting each other through action scenes, and (hopefully) good triumphs. Corporations also have simple formulas. These are "business models"—how they grow profit. Finance is the language of that movie script. Business depends on IT. IT assets include hardware, software and people. Through financial processes, funds get allocated to assets. Financial people measure whether IT did a good job of managing the assets. This is not new. What is new is that the finance-IT interaction has changed during these troubling economic times in at least three ways:

- Dramatic budget cuts and a "new normal" with more scrutiny of business benefit
- Increased focus on cash management (*when* and *how* money is spent, not just what is spent)
- More concern about the risk of the wrong decision and less patience for implementation problems

This suggests three growing needs for IT:

- Learning to think in more financial terms in requests for funds and demonstration of results
- Partnering deeply (not just casually) with finance in jointly going to "the business" to demonstrate how IT can build capabilities needed to seize more opportunity
- Partnering with finance in evaluating business-IT projects in terms of both risk and return, to avoid wasting precious resources

To help chief information officers (CIOs) and IT managers better position and relate to finance and other business leaders, an article published in *COBIT Focus* last year provided guidance on how to use finance-related content in COBIT[1] and Val IT: Based on COBIT[2] to build a more productive relationship between the CIO and the chief financial officer (CFO) and their organizations.[3] It looked first at the basics—the CFO as budget-controller for and internal customer of the CIO. Then, it turned to value creation—the CIO and CFO teaming to help business-line leaders transform through business-IT projects to better grow profitable revenue in troubled economic times. As the economic woes have dragged on and IT leaders have asked more questions—such as "What do I need to do with finance to better prioritize and manage business-IT spending?" and "How do I do this more easily and effectively?"—another article is needed.

To set the stage, this article first looks at two frequently asked questions: "How does IT better relate to the teams within finance?" and "How do IT and finance improve communications?" Then, it moves to the pivotal question: "How can business-IT models be used to drive better benefit?" It closes by reflecting on additional frequently asked questions and suggests three ways to enhance implementation of COBIT, Val IT and/or Risk IT: Based on COBIT.[4] The goal is to empower readers with tips to improve funding allocation and to better demonstrate benefit.

SETTING THE STAGE

Who Stands Where? (Roles and Responsibilities)

IT practitioners frequently ask: "Who in finance do I ask about xyz?" "Why didn't the person I talked to in finance tell me to…?" Or, "Doesn't anybody in finance really care about…?" The simple fact is that finance, just like IT, is composed of several areas. If a business-line person asked IT a question about a new customer relationship management system, would the architect, service delivery management, disaster recovery and security manager answer the question in exactly the same way? No. Just the same, in finance, one needs to talk to the right person to find the right answer for the situation.

The finance organization is led by the CFO. Organization structures vary by broader organization design (centralized, decentralized, etc.), industry, country (including number and location of countries covered) and business model. Typically, it has these main functions:

- **Planning and budgeting**—Conducts analysis of past spending and projections of future

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.

spending. This manages the budget cycle for people, expenses and capital. Some organizations have a separate team for capital budgeting or investment portfolio management for activities needing more focus than routine budgeting. IT works closely with these groups in the budget cycle.

- **Accounting**—Usually in six areas: financial accounting (external reporting for investors and others), managerial/cost accounting (more detail for internal analysis, often handles internal cross-charges and a principal contact for IT), accounts payable (A/P), accounts receivable (A/R), billing (collecting from external customers) and payroll. IT spending is tracked by the managerial accounting team. A/P is engaged by IT to pay service and product providers. This is also the area to ask about how accounting principles apply to IT spending categories.
- **Treasury and tax**—Manages cash availability, return and risk on cash and investments, equity (stock) and debt (loan instruments), and many taxes. IT touches this group when acquiring new hardware and software.
- **Procurement (might also be in operations)**—IT touches for supplier selection, contract management and ongoing vendor risk management.
- **Risk management (might also be in operations)**—Manages financial market risks (e.g., interest rate or foreign exchange rate risks), credit risks or buying insurance. Today, it is broadening into enterprisewide risk management. ISACA's Risk IT would be of most interest to this group.
- **Internal audit**—Usually reports to the CFO for administrative purposes, reporting formally to the audit committee of the board of directors for independence purposes. IT audit reports here in many organizations.

Additionally, some organizations have dedicated teams for financial policy or program management.

The following steps can be helpful when beginning to navigate finance:

- Get a copy of the finance organization chart.
- When creating permanent or temporary teams in IT, be sure to invite the appropriate person(s). Do not expect a single finance contact to know everything in finance.
- Be aware of the different roles in finance. For example, if one is looking to find a better way to finance the acquisition of new hardware or software, ask treasury, rather than accounting or budgeting.

What Language Is That? (Clear Communications)

"Why can't IT just speak regular business language instead of techie-talk?" is a common complaint from business leaders, including finance leaders. Yet, finance, like IT, has its own language. Weighted average cost of capital (Is that how heavy my new server rack is?), debenture covenants (Is that a place where witches live?), IRR (IT risk response?), NPV (no pay-per view television?). Yes, finance-speak can be as challenging to IT as IT-speak is to finance and other parts of the business. In the May 2010 "A Link, A Laugh and a Look," a video link was included that illustrates what happens when people of different backgrounds try to play the game Pictionary.[5]

Clear communication takes effort. Here are some steps to get started:

- Remove abbreviations or IT shorthand from documents. Try to get materials to pass the "spouse test" (i.e., ensure that your non-IT spouse understands what you are saying).
- Express benefits in business terms. "Business terms" means market share, sales, costs, expenses, quality, customer satisfaction measures and terms that business leaders understand.
- Use presentation formats that are widely used in the enterprise. Familiar tables and graphs make it easier for others to understand the point.

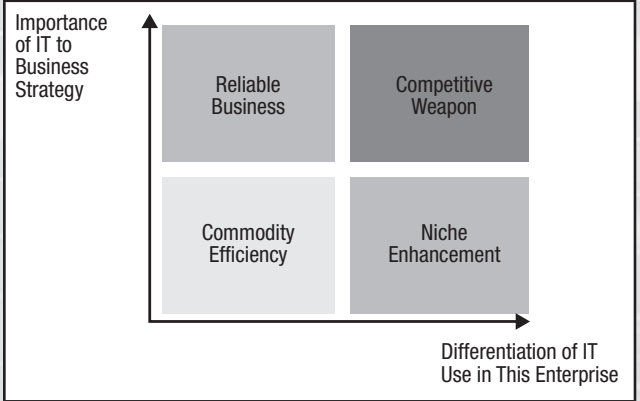
With these set-the-stage questions covered, the story can turn to what will be played out on the stage—the story that needs to be enabled by IT.

THE STORY

In creating a movie or a play, the nature of the story drives the production equipment needed to tell that story. A blockbuster action movie has much different equipment needs from a weekly situation comedy. In the business-IT world, the distinctive way(s) the business makes money (e.g., variety of offerings, speed and flexibility, low cost, personal service, creative design, broad distribution, marketing demand) drives the business-IT model. It turns out that alignment in models is a crucial piece of overall alignment, as this drives many business-IT governance and management decisions. Several authorities have proposed ways to view such models. **Figure 1** illustrates a simple, powerful and practical way to identify the needed model and take the right actions. An enterprise with multiple business lines might use multiple models such as:

- **Commodity efficiency**—An undifferentiated utility with low impact to the business. Generic software and hardware are used. Temporary outages can be worked around. It can be easily outsourced on a cost basis.
- **Reliability business**—Sometimes also termed "business of IT." Reliability is far more important than in the commodity model, but services have low differentiation. It can be provided as an insourced or outsourced model. A "service catalog" of standardized offerings and service levels is a typical feature.
- **Competitive weapon**—Adds high differentiation as a driver in the business-IT model. The CIO and IT team are deeply involved in the business. IT improvements are tightly coupled to business process improvements. Speed and flexibility are key. It is very difficult to outsource without significant damage to the business.
- **Niche enhancement**—When differentiation is key to only certain business lines or as product enhancements, the niche model is appropriate. This is seen when a special team is used to enable a growth business area while the rest of the business operates on a commodity efficiency or reliable business model.

Figure 1—Business-IT Models



Source: ValueBridge Advisors LCC, used by permission.

With this view of four types of story line, the story turns to the three areas of frequently asked questions regarding IT finance—the action.

LIGHTS, CAMERA, ACTION

Investment Portfolio Management

In investment portfolio management, most of the questions are about what goes into the portfolio, relating portfolio to business-IT alignment/engagement, accommodating business models, categories to use and managing risk.

In short, the following are some suggestions:

- The portfolio contains everything—programs, projects, services (business and IT), operations and other assets. For convenience, some organizations further distribute portfolios into subportfolios or super-/meta-portfolios. T his is acceptable, as long as there is a complete view to balance resource allocation across the entire portfolio based on risk and return.
- Portfolio categories depend on business-IT alignment/ engagement working because business-IT investment portfolio categories should flow from business investment portfolio categories. If the chief executive officer (CEO) and CFO talk to investors in categories such as acquisition, expansion into new countries and cost efficiencies in mature businesses, then those business categories should flow to IT portfolio categories such as building flexibility for new expansion or building efficient scale in mature businesses. If the business is investing in cross-selling products to customers, then the business-IT portfolio might include a data integration category. Spending can be tagged with other labels such as "maintenance" or "compliance," but the leading thought should be about the business.
- The business model used by an enterprise is a prime driver of investment portfolio design, categories and management. Guidance from ISACA and other organizations is often written in view of a single business model. Yet, there are many models, such as the four mentioned previously. The selection of one of the four models drives investment, project management and the operations approach to ensure that the business meets its objectives.
- Managing risk in the investment portfolio and programs is important (rather than just seeking return no matter how risky). Some industry analysts suggest that far more IT value is lost in the "what to do" decision than in the "how to do it" implementation. The guidance from Risk IT related to this area can help to address this.

Investment Program Management

In investment program management, most questions are related to managing risk, accommodating changing requirements, monitoring investments over time and retiring programs cleanly.

In short, the following are some suggestions:

- Managing risk in the investment programs and projects is extended by pointing to the guidance from Risk IT. Through mappings, COBIT users can also embrace the guidance of PRINCE and PMBOK.[6]
- In monitoring, many organizations state that they use a "fire and forget" approach to investment monitoring. Thus, the "what to do" is to improve life-cycle monitoring of an investment—from development progress reviews to retirement (as advocated in COBIT and Val IT).
- Changing requirements is a significant concern in implementation. Some organizations respond by "locking" requirements in an excessive way, which damages business flexibility to pursue revenue. Others try to accommodate too many changes, delaying deliverables and leaving users willing to take anything that exists. While beyond the scope of COBIT, there are approaches that can be adapted from project management, architecture, system development and product management to manage requirements in layers and components that promote a balance of stability and timely delivery and enable profitable revenue.

Financial Policies, Implementation, Analysis and Reporting

In the financial policies, implementation, analysis and reporting area, questions arise due to the difficulty in getting enterprise financial policy and reporting designed for functional areas (such as human resources, marketing or finance as a function) to support the more complex nature of IT (with many fixed assets and transformational projects spanning budget cycles). In short, many enterprises make life difficult for the CIO and the CIO's customers by accounting for IT on a period-expense basis, rather than the way they would for their own manufacturing or asset-intense operational areas. The following are some suggestions:

- In planning and budgeting policy, the earlier points on business models also apply. For example, applying policies appropriate for the commodity efficiency model when the business needs the competitive weapon model defeats the good work of business alignment/engagement/relationship teams that are forging a tightly coupled business-IT to drive product growth.
- In cost accounting policy, a key is to monitor IT costs at the appropriate unit of analysis to make better business decisions. This way, that unit can be rolled up to provide the insight needed for the business model used. For example, some organizations measure server utilization in units and charge it back; other organizations need to roll that up to a business view of IT cost structure to illustrate how IT costs vary if an acquisition is made, new products are launched or business is expanded into a new country. Cost structure and strategy are crucial to clear communication, alignment and architecture.
- In acquisition policy, organizations can benefit by: 1) placing more emphasis on financing IT assets (cash purchase, lease [operating or capital] or loan), 2) engaging treasury to preplan the year's activity, and 3) evaluating risk in third-party suppliers (such as applying the content of Risk IT to the supply chain).
- To help reporting, provide more actionable insight, provide explicit coverage of each policy area, organizations should use measures tied to the individual objectives of members of the enterprise IT governance committee and link to project postimplementation reviews. Finally, they should use this information to improve both management and the governance process.

CONCLUSION

COBIT, Val IT and Risk IT provide strong guidance and have active user communities.[7] A benefit of using open industry frameworks is gaining access to a body of experience-based guidance to extend the core frameworks. This article has provided tips on how to address them. To more easily advance organizations, it is important not to reinvent the wheel, but to draw on and tailor this body of knowledge to drive progress more quickly and easily.

ENDNOTES

[1] 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. For more information, visit *www.isaca.org/cobit*.

[2] Val IT: Based on COBIT is a framework that enhances COBIT with additional management guidance on enterprise governance of IT, managing a portfolio of business-IT investments and managing the life cycle of programs created by the investments. For more information, visit *www.isaca.org/valit*.

[3] Barnier, Brian; "COBIT for Troubled Times—Unlocking COBIT to Strengthen the CIO-CFO Partnership," *COBIT Focus*, vol. 3, 2009

[4] Risk IT: Based on COBIT is a framework that enhances COBIT with additional management guidance on risk governance, risk evaluation and risk response. For more information, see *www.isaca.org/riskIT*.

[5] Pictionary is a board game and trademark of Milton Bradley. If you have not seen "A Link, a Laugh and a Look" and/or the video, it is available at *www.youtube.com/watch?v=fyO5Kwc3NK8*.

[6] For more information on COBIT Mappings, visit *www.isaca.org/cobitmapping*.

[7] In addition to local chapter meetings, it is now easier to learn from peers around the world through the new user groups at *www.isaca.org*.

[8] The COBIT 5 concept paper is available at *www.isaca.org/cobit5*.

AUTHOR'S NOTE

This article responds to the questions and concerns of many people with whom the author has spoken in the past year. What is missing? What are your questions? ISACA frameworks are developed with much public comment, drawing on the questions and needs of practitioners like you. Please send your questions and comments to *brian@valuebridgeadvisors.com*.

The author thanks Bob Frelinger, a colleague on the COBIT 5 team,[8] for his review, comments and improvements.

EDITOR'S NOTE

With the growing importance of business value and finance to ISACA members, this year's ISACA IT Governance, Risk and Compliance Conference will include a new session on finance. The conference will focus on delivering business value, beginning with the opening keynote in which the audience will hear from the top of "the business" with an address by a member of the board of directors of a large financial institution. For more information on the ISACA IT Governance, Risk and Compliance Conference, visit *www.isaca.org/itgrc*.

An Introduction to Digital Records Management

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

To support the continuing flow of business, comply with the regulatory environment and provide necessary accountability, organizations should create and maintain authentic, reliable and usable records, and protect the integrity of those records for as long as required.[1]

Organizations are increasingly reliant on information communications technology (ICT) as a crucial component of business operations. As a result, information is often partially or fully in electronic form.

The main objective of this article is to introduce the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records in an electronic environment, based on international standards ISO 15489, part 1 and part 2.

REGULATORY ENVIRONMENT

All organizations need to identify the regulatory environment that affects their activities and the requirements to document their activities. The policies and procedures should reflect the application of the regulatory environment to the organization's business processes. An organization should provide adequate evidence of its compliance with regulations in the records of its activities.[2]

The regulatory environment might consist of:

- Statutes, case laws and regulations governing the sector-specific and the general business environment, including laws and regulations relating specifically to records, archives, access, privacy, evidence, electronic commerce, data protection and information
- Mandatory standards of practice
- Voluntary codes of best practice
- Voluntary codes of conduct and ethics
- Identifiable expectations of the community about what constitutes acceptable behavior for the specific sector or organization

For example, in Bosnia and Herzegovina:

- The taxation retention period for the original application for entry into a unified system is five years from the date of submission of the application, while the data entered into the database in electronic form have to be kept permanently
- Records maintained by the bodies responsible for issuing permits for the movement of weapons and military equipment must be kept permanently
- Records obtained pursuant to an act against money laundering and financing of terrorist activities must be kept at least 10 years after identification, the conduct of transactions, closing the account or termination of the business relationship, etc.

The nature of the organization and the sector to which it belongs determine which regulatory elements (individually or in combination) are most applicable to the organization's records management requirements.

RESPONSIBILITIES

ISO 15489 defines "records management" as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.[3] The term "records" is defined as information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Records management responsibilities and authorities should be defined, assigned and promulgated throughout the organization so that, where a specific need to create and capture records is identified, it is clear who is responsible for taking the necessary action.

POLICY

Organizations should define and document a policy for records management. The objective of the policy should be the creation and management of authentic, reliable and usable records that are capable of supporting business functions and activities for as long as they are required. Organizations should ensure that the policy is communicated and implemented at all levels in the organization.[4]

However, a policy statement on its own will not guarantee good records management. Critical to its success are endorsement and active and visible support by senior management as well as allocation of the resources necessary for implementation.[5]

A records management policy statement sets out what the organization intends to do and sometimes includes an outline of the program and procedures that will achieve those intentions. The policy statement should refer to other policies relating to information (e.g., those on information systems policy, information security or asset management), but should not seek to duplicate them. It should be supported by procedures and guidelines, planning and strategy statements, disposition authorities, and other documents that together make up the records management regime.[6]

CHARACTERISTICS OF RECORDS

A record should correctly reflect what was communicated or decided or what action was taken. Records management policies, procedures and practices should lead to authoritative records that have the following characteristics:[7]

- **Authenticity**—An authentic record is one that can be proven to:
  - Be what it purports to be
  - Have been created or sent by the person purported to have created or sent it
  - Have been created or sent at the time purported
- **Reliability**—A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.
- **Integrity**—The integrity of a record refers to it being complete and unaltered. It is necessary that a record be protected against unauthorized alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

  If the information is going to be used in a criminal proceeding, organizations must be able to identify who has had access to a particular record at any given time from collection, to creation of the evidence copy, to presentation as evidence. The evidentiary weighting of records will be substantially reduced if the chain of custody cannot be adequately established or is discredited.[8]
- **Usability**—A useable record is one that can be located, retrieved, presented and interpreted. It should be directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

ELECTRONIC RECORDS

Traditionally, corporations have considered the evidentiary implications of electronic documents only when they are required for litigation, or when forensic practitioners have focused on collecting IT evidence as artifacts of an investigation. However, successful management of IT evidence is much broader than a mere postmortem activity, and the IT evidence must be managed continuously throughout the records life cycle.[9]

In an electronic business environment, adequate records will not be captured and retained unless the system is properly designed.[10] It is important to note that media for storing digital data, and also formatting the data, are subject to change. For example, a significant number of documents archived by an organization over the past decade may now be largely illegible and incomprehensible because of damage to storage media or because the older file formats are incompatible with newer, currently used formats.

Sometimes digital records need to be archived for a certain period of time, so that, if necessary, they can be presented during the court process. With the current pace of technological development, it is very likely that problems with outdated storage media or formats of data can make the process of returning data very expensive. This can be because of the need to complete the conversion of all data to new media as technology develops or because of the need to keep the old equipment and software.

Digital evidence as a form of physical evidence creates several other challenges:[11]

- It is a messy, slippery form of evidence that can be difficult to handle.
- Digital evidence is generally an abstraction of some event or digital object.
- The fact that digital evidence can be manipulated easily raises additional challenges for digital investigators.
- Digital evidence is usually circumstantial, making it difficult to attribute computer activity to an individual.

Therefore, digital evidence can be only one component of a solid investigation.

SECURITY

A formal instrument that identifies the rights of access and the regime of restrictions applicable to records is a necessary tool to manage records in organizations of all sizes and jurisdictions. Reasonable security and access depend on both the nature and the size of the organization, as well as the content and the value of the information requiring security.[12]

Access to records may be restricted to protect:

- Personal information and privacy
- Intellectual property rights and commercial confidentiality
- Security of property (physical, financial)
- State security
- Legal and other professional privileges

Information security is key when discussing legal admissibility issues. The main discussion on this topic is likely to be the authenticity of stored information. When the electronic information was captured by the storage system, was the process secure? Was the correct information captured, and was it complete and accurate? During storage, was the information changed in any way, either accidentally or maliciously? When responding to these questions, information security implementation and monitoring are key to demonstrating authenticity.[13]

Proof of compliance with the recommendation of ISO/IEC 27001:2005[14] may provide helpful supporting evidence in court. It indicates that the organization has exercised its duty of care, and will assist the court in assessing the authenticity and integrity of information.[15]

RECORD STORAGE DECISIONS

The decision to capture a record implies an intention to store it. Appropriate storage conditions ensure that records are protected, accessible and managed in a cost-effective manner. The purpose served by the record, its physical form, and its use and value dictate the nature of the storage facility and services required to manage the record for as long as it is needed.[16]

It is important to determine efficient and effective means of maintaining, handling and storing records before the records are created and, then, to reassess storage arrangements as the records' requirements change. It is also important that storage choices be integrated with the overall records management program.

Backup copies of essential business records should be taken regularly. Adequate backup facilities should be provided to ensure that all essential business information can be recovered following a disaster or media failure.

Backup information should be given an appropriate level of physical and environmental protection consistent with standards applied at the main site.[17]

Technologies used for the initiation and control of the secure transfer of information between the organization and an archive, whether the archive is operated in-house or by a third-party service provider, should be documented. Using cryptographic techniques can be one way to ensure authentication of the sender and the electronic document.

The method of ensuring that received and subsequently stored information is identical to that originally sent should be documented.[18] Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance, when sending record media to another location, e.g., the off-site backup facility.

The following controls should be applied to safeguard computer media being transported between sites:[19]

- Reliable transport or couriers should be used. A list of authorized couriers should be agreed upon with management, and a procedure to check the identification of couriers should be implemented.

- Packaging should be in accordance with manufacturers' specifications and should be sufficient to protect the contents from any physical damage likely to arise during transit.
- Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. Examples include:
  - Use of locked containers
  - Delivery by hand
  - Tamper-evident packaging
  - In exceptional cases, splitting of the consignment into more than one delivery and dispatching contents by different routes
  - Use of digital signatures and confidentiality encryption

Organizations should conduct a risk analysis to choose the physical storage and handling options that are appropriate and feasible for their records. It is important to specify the relationship between the risks and the selected options for treating them. The selection of storage options should take into account access and security requirements and limitations in addition to physical storage conditions. Records that are particularly critical for business continuity may require additional methods of protection and duplication to ensure accessibility in the event of a disaster.

Risk management also involves development of a disaster recovery plan that defines an organized and prioritized response to the disaster, planning for the continuance of regular business operations during the disaster and making appropriate plans for recovery after the disaster.

All activity is susceptible to disruption from internal and external events, such as technology failure, fire, flood, utility failure, illness and malicious attack. ICT continuity management provides resilience to prevent ICT disruptions and to recover when disruptions occur.

Disruption to ICT can be a huge risk; it can damage an organization's ability to operate and undermine an organization's reputation. The consequences of a disruptive incident vary and can be far-reaching, and might not be immediately obvious at the time. BS 25777 may help organizations plan and implement an ICT continuity strategy.[20]

DIGITAL STORAGE

The storage of records in electronic form necessitates the use of additional storage plans and strategies to prevent loss:[21]

- Backup systems are a method of copying electronic records to prevent loss of records through system failures. Such systems ought to include a regular backup schedule, multiple copies on a variety of media, dispersed storage locations for the backup copies, and provision for both routine access and urgent access to backup copies.
- Maintenance processes may be needed to prevent physical damage to the media. Records may need to be copied to newer versions of the same media (or other new media) to prevent data erosion.
- Hardware and software obsolescence may affect the readability of stored electronic records.

USE AND TRACKING

The tracking of records usage within records systems is a security measure for organizations. It ensures that only those users with appropriate permissions are performing authorized records tasks. The degree of control of access and recording of use depends on the nature of the business and the records it generates. For example, mandatory privacy protection measures in many jurisdictions require that the use of records holding personal information be recorded.[22]

CONTINUING RETENTION

Records identified for continuing retention need to be stored in environments conducive to their long-term preservation. Preservation strategies for records, especially electronic records, may be selected on the basis of their ability to maintain the accessibility, integrity and authenticity of the record over time, as well as for their cost-effectiveness.

Preservation strategies can include copying, conversion and migration of records:[23]

- Copying is the production of an identical copy within the same type of medium (paper/microfilm/electronic), e.g., from paper to paper, microfilm to microfilm, or the production of backup copies of electronic records (which can also be made on a different kind of electronic medium).
- Conversion involves a change of the record's format but ensures that the record retains the identical primary information (content). Examples include microfilming of paper records, imaging and change of character sets.
- Migration involves a set of organized tasks designed to periodically transfer digital material from one hardware/software configuration to another, or from one generation

of technology to another. The purpose of migration is to preserve the integrity of the records and to retain the ability for clients to retrieve, display and otherwise use them. Migration may occur when hardware and/or software becomes obsolete, or it may be used to move electronic records from one file format to another.

Information may be stored for a considerable length of time and for longer than the lifetime of the current technology. Thus, to ensure the integrity of stored information, it is important to plan from the outset that the information may be subject to a migration process. Such a process may involve a change of media, computer hardware or software.

As a rule of thumb, a storage media migration process will occur approximately every five years. A reliable methodology for dealing with this potential problem is to ensure that data files are stored in an industry standard format, or that viewers for each stored format are maintained. It is also recommended that a restricted number of formats is used for long-term storage, to reduce future storage migration issues.

When making provisions for migrating data files, it is important to include all relevant metadata, including index data and audit trails. These additional data should also be migrated to the new technology without loss of integrity. Records, including audit trails, should be kept of any migration process to which stored data have been subjected, to allow the integrity of the data to be demonstrated beyond any reasonable doubt at any time in the future.[24]

As new technologies become available, other methods may be used to retain electronic records for long periods.

Where records are transferred to an external storage provider or an external archives authority, documentation that outlines continuing obligations to maintain the records and manage them appropriately should be formally established by agreement between the custodian(s) and the transferring party.

PHYSICAL DESTRUCTION

Physical destruction of records is carried out by methods appropriate to their level of confidentiality.

Records in electronic form can also be destroyed by reformatting or rewriting, if it can be guaranteed that the reformatting cannot be reversed. Deleting instructions is not sufficient to ensure that all system pointers to the data incorporated in the system software have also been destroyed. Backups containing generations of system data also need to be reformatted or rewritten before effective destruction of electronic information is complete. Physical destruction of storage media is an appropriate alternative, especially if deletion, reformatting or rewriting are either not applicable or are unsafe methods for destroying digital information (for instance, information stored on WORM [Write Once Read Many] media).[25]

It may be necessary to amend, dispose or expunge (i.e., remove without any trace of it ever existing) specific records from information management systems, perhaps to comply with a court order and/or to meet requirements of data protection legislation. The process should be auditable, such that the disposal of a particular document, for example, can be proven. It is also important to obtain any necessary authorization for such processes before implementation.

When positive removal of information from the system is required, identification and deletion of all copies of the information (including backup media) ensure that necessary action has been taken.[26]

The principles of good practice in record keeping are of value even if the need to produce electronic records in court never arises. The effort and resources required to comply bring business benefits, whether the organization is in court or not, in increasing organizational efficiency and improving control over information assets.

EVIDENTIAL WEIGHT

Records managers need to be aware of the potential for legal challenge when documents are presented in evidence to a court of law. If the integrity or authenticity of a record is called into doubt in court by suggestions of tampering, incompetence, improper system functionality or malfunction, the evidential weight or value put on the document by the court may be lost or, at least, reduced, creating a detriment to the case.

Records managers need to have readily available evidence to demonstrate and prove the organization's compliance with legislation, policies and procedures throughout the life of the system. It should also be possible to show that the system was operating as intended in accordance with the organization's normal business practices. This evidence would be available from records of the monitoring and auditing of system processes.

Because electronic records can be altered easily, opposing parties often allege that computer records lack authenticity because they have been tampered with or perhaps changed

after they were created. Courts have rejected arguments that electronic evidence is inherently unreliable because of its potential for manipulation. As with paper documents, the mere possibility of alteration is not sufficient to exclude electronic evidence. When specific evidence of alteration is absent, such possibilities go only to the evidence's weight, not its admissibility.[27]

The existence of an airtight security system (to prevent tampering) is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible.

CONCLUSION

Records contain information that is a valuable resource and an important business asset. A systematic approach to the management of records is essential for organizations and society to protect and preserve records. A records management system results in a source of information about business activities that can support subsequent activities and business decisions, as well as ensure accountability to present and future stakeholders.

ICT brings potentially increased, or at least different, risks in terms of civil or criminal wrongdoing and organizations need to be able to protect themselves against those risks. Failure to do so raises governance and accountability issues for which the management of the organization could be held responsible. The fact that the electronic environment is unfamiliar territory does not excuse directors from liability based on lack of knowledge.

One way of proactively addressing electronic records management is to follow a standardized records management process, such as the one recommended in international standard ISO 15489.

ENDNOTES

[1] International Organization for Standardization, ISO 15489-1:2001, *Information and documentation—Records management—Part 1: General*, 2001

[2] *Ibid*.

[3] *Ibid*.

[4] *Ibid*.

[5] International Organization for Standardization, ISO 15489-2:2001, *Information and documentation—Records management—Part 2: Guidelines*, 2001

[6] *Ibid*.

[7] *Op cit*, ISO 15489-1:2001

[8] Standards Australia International, HB 171-2003, *Guidelines for the management of IT evidence*, 2003

[9] *Ibid*.

[10] *Op cit*, ISO 15489-1:2001

[11] Casey, Eoghan; *Digital Evidence and Computer Crime, 2nd Edition*, 2004, Academic Press

[12] *Op cit*, ISO 15489-2:2001

[13] Shipman, Alan; BIP 0008-1:2004, *Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically*, The British Standards Institution, 2003

[14] International Organization for Standardization, ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*, 2005

[15] *Op cit*, Shipman

[16] *Op cit*, ISO 15489-2:2001

[17] International Organization for Standardization, ISO/IEC 17799:2005, *Information technology—Security techniques—Code of practice for information security management*, 2005

[18] *Op cit*, Shipman

[19] *Op cit*, ISO/IEC 17799:2005

[20] British Standards Institution, BS 25777:2008, *Information and communications technology continuity management*, 2008

[21] *Op cit*, ISO 15489-2:2001

[22] *Ibid*.

[23] *Ibid*.

[24] *Op cit*, Shipman

[25] *Op cit*, ISO 15489-2:2001

[26] *Op cit*, Shipman

[27] Computer Crime and Intellectual Property Section, Criminal Division, US Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," USA, 2001

Building a Business Case for Records Management

Cheryl Strait is a principal at Ernst & Young, where she provides strategic records management services to companies in all industries. She focuses her practice on helping organizations address and mitigate regulatory, legal and compliance risks through the development and use of a strong records management program. Strait has more than 20 years' experience in utilizing and delivering services focused on facilitating and reengineering processes; identifying, designing, implementing and deploying technology solutions; applying program management methodologies; and implementing global records management programs.

Managing large volumes of data is an ever-growing challenge in business and one that has an impact on the IT industry. This issue is further complicated by the constant need to update software and infrastructure for managing e-mail for numerous employees.

There is a way to filter this information overload. While these challenges cannot be avoided, they can be controlled by adopting an effective records management program. This article outlines step-by-step details to help enterprises build a business case for a robust records management program. It includes helpful insights on how an IT leader can:

- Assemble an essential cross-disciplinary team to help gain senior management's support
- Identify legal, compliance, operational and other records management risks
- Quantify and prioritize the myriad of records management risks
- Adopt case studies to demonstrate the real-life consequences of poor records management
- Develop a robust records management plan and a proposed implementation budget

HOW TO BUILD A BUSINESS CASE

Building a business case for a records management initiative begins with providing the background of the challenge being addressed. Start by identifying and listing the challenges the company faces. Are there difficulties managing large volumes of data already stored in electronic systems? Is dealing with outdated or obsolete software or hardware creating a problem? Has managing e-mail become overwhelming?

Next, include a description of the scope of the records management initiative, along with details of the future state to be achieved at the end of the initiative. It is imperative to demonstrate solid reasoning for performing the initiative by describing the risks associated with not doing it. For example, a company could incur millions in additional costs from poorly managing electronically stored information, not following its own retention policy or being unable to produce proper documents at a critical time. But remember—it is equally important to describe any risks associated with doing the initiative.

Finally, the business case will need to establish an estimated plan and timeline, and then provide an estimated budget to carry out the initiative.

The following five steps offer detailed suggestions for creating a business case for records management.

Step 1: Assemble a Cross-disciplinary Team

A cross-disciplinary team will aid in collecting the information needed to create a business case for investing in records management. First, establish a structure and the associated roles for a cross-disciplinary team, defining responsibilities for each team member. Determine from which areas team members should come, e.g., legal, IT, records management, business areas (such as purchasing, human resources, accounting, engineering and manufacturing) and audit. Select business areas in which records and information pose the greatest risk and impact to the business.

Document the roles, responsibilities, communication plan and meeting architecture, and share them with each team member. Provide individuals with an understanding of their purpose on the team. Address such questions as: How will team members interact? How often will they meet? What is the expected level of involvement for each team member? Gain support from senior executives for the proposed cross-functional team. Senior-level support is essential to securing the individuals who will act as team members—and who are necessary to sustain the initiative within the organization.

Identify who should fill the defined roles as representatives for each area. Seek out people who are well connected in their area. They should be at a level that provides them with access to both the user community and executives within

their designated areas. And they should have the knowledge to identify risks and the motivation to make things happen.

Step 2: Identify Records Management Risks

Identifying, understanding and prioritizing the risks a company faces are important steps in building a convincing business case for the program. Here are some leading practices:

- Hold working group sessions to identify risks associated with records and the management of records.
- Review business processes, identifying where records are input and output within the process.
- Examine where records enter into the process, are accessed during the process and are generated by the process.
- Consider how records are created, stored, used, maintained, distributed, accessed, preserved and disposed of.

Next, determine if there are any issues or risks associated with any aspect of the process or records life cycle. Are any records likely to be required during a litigation discovery event or a regulatory investigation? Find out if records pose any operational risk during any part of their life cycle. Operational risks may include mishandling, inappropriate access, accessing the incorrect version and inappropriate retention duration. Hold working sessions within the cross-disciplinary team and also within high-risk business areas.

Step 3: Quantify and Prioritize Records Management Risks

While risks are being identified, it is important to capture the impact (or consequence) and probability (or likelihood) of a risk.

The *impact* of the risk, should it occur, should be quantified based on a numerical scale (1 = low, 2 = moderate, 3 = high, 4 = significant). The numerical impact scale should contain definitions for each level that clearly articulate the criteria for a specific number. Include a monetary amount that might result from a loss and a description of what the loss would entail. For example, "significant" could mean irreversible issues that may lead to costly mitigation or brand risk.

The probability of a risk occurring should also be quantified numerically, based on the likelihood of occurrence (1 = rare, 2 = unlikely, 3 = possible, 4 = likely, 5 = certain). Document risks along with a description containing "if… then" statements that describe the risk, along with the numerical impact and probability associated with each risk. Prioritize risks based on a ranking associated with the quantified probability and the impact of the event occurring.[1]

Step 4: Use Case Studies to Show Consequences and Gain Support

A natural reaction to records management programs is to raise the question: Why are we focusing resources on an administrative task? Organizational change management practices show that using specific examples to convey the importance of a program helps gain awareness about why a specific initiative is important and the roles individuals play in making it happen.

Cross-disciplinary team members should collect examples of the impact of poor records management practices from within their own business areas. The team should review the collected examples and select the most relevant and distressing stories to share across the organization. This is an effective way to demonstrate the real-life consequences of improper records management.

For example, the tax department may have examples of expenses that had to be reversed because required documentation could not be found during a tax audit. Legal departments may have examples demonstrating the significantly high cost of searching for and producing information from terabytes or even petabytes of electronically stored information in response to a litigation discovery request. Purchasing departments may have examples of multiple purchase orders for a single vendor that were not properly filed, thus causing the company to miss volume discounts. Collectively, these examples could cost a company millions in losses. Remember, individuals react more favorably to stories that resonate with them and are relevant to the work they perform.

Step 5: Propose a Plan and Estimate a Budget

After completing the previous steps, develop a high-level plan focused on addressing records management challenges. Describe the intended scope of the initiative. Identify milestone activities, prioritize them into a logical sequence and create tentative timelines based on perceived durations. Determine the resource requirements to perform the initiative. These resources should include internal team members, external team members (vendors or consultants), process enhancements and technology requirements. Examine the plan with the cross-disciplinary team and then with executive leadership. It is important to gain support by socializing the plan prior to publishing it in a business case.

Create a budget to correspond with the milestone activities of the plan. This is required to gain approval for a business case. Developing a budget estimation can include:

- Estimating resource requirements
- Determining if outside consultants will be needed
- Determining what technology may be required
- Determining if any other records management vendors may be needed (e.g., offsite storage vendors, imaging vendors)

Work with consultants and vendors to secure realistic budgetary estimates. Finally, vet the proposed budget with executives to gain their support by socializing the numbers prior to publishing the business case.

CONCLUSION

Cost reduction continues to be top priority for most business executives in today's turbulent environment. As many organizations look to drive costs out of the enterprise, expanding how and where records management is applied is being recognized as an enabler for reducing storage costs and improving the efficiency of routine operations. Realizing efficiencies by increasing an organization's records management capabilities will require the investment of valuable resources, including people, time and money. Acquiring commitment to expend resources on records management will involve gaining the attention and support of executives with the authority to grant approval and provide access to the necessary assets. Creating a thoughtful and socialized business case lays the foundation for communicating the need, generating awareness of the benefits and providing executive leadership with an estimated return on investment required to gain their approval for the consumption of the scarce resources that will be utilized to improve the organization's records management program.

AUTHOR'S NOTE

The views expressed herein are those of the author and do not necessarily reflect the views of Ernst & Young LLP.

ENDNOTES

[1] Pritchard, C. L..; *Risk Management Concepts and Guidance*, ESI International, USA, 1997

IT Governance and Business-IT Alignment in SMEs

Steven De Haes, Ph.D., is professor of information systems management at the Antwerp Management School and the University of Antwerp (Belgium) and a managing director of the Information Technology and Alignment (ITAG) Research Institute. He can be contacted at *steven.dehaes@ua.ac.be.*

Rogier Haest is IT auditor at 2-Control B.V. Over the past years, he has been involved in various IT audit and consultancy assignments at small and medium enterprises. He can be contacted at *rogier.haest@2-control.nl.*

Wim Van Grembergen, Ph.D., is professor at the Information Systems Management Department of the University of Antwerp and the Antwerp Management School and is academic director of the ITAG Research Institute. He can be contacted at *wim.vangrembergen@ua.ac.be.*

For several years the concept of IT governance has been high on the agenda of organisations. Many projects regarding IT governance have been initiated in various companies and government institutions, to achieve better alignment between IT and the organisation and to obtain the necessary involvement of senior business management in the value creation from IT-enabled investments. Prior research has demonstrated a relationship between IT governance and business-IT alignment. Companies in the financial sector with a high degree of business-IT alignment typically manage mature IT governance practices.[1, 2] IT governance has been underlined as one of the necessary conditions for a better business-IT alignment.[3, 4]

Whether these findings also apply to the small and medium enterprise (SME) market is not known. This article focuses on companies in the SME segment in the Netherlands and discusses findings on business-IT alignment and IT governance practices in organisations in this field.[5]

It starts with a high-level description of the existing literature on business-IT alignment and IT governance. Subsequently, results are discussed on how business-IT alignment was perceived and how IT governance was implemented in a sample of SMEs from the Netherlands.

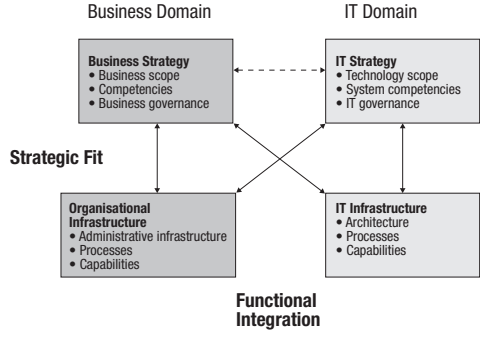
The main conclusion of this study is that SMEs in the Netherlands score relatively low in the field of business-IT alignment compared to other international benchmarks. Furthermore, it was found that a select organisation with a relative high business-IT alignment score clearly applied better IT governance practices and *vice versa*. Although the sample is small, this result lines up with earlier results[6] for large organisations, where this positive relationship between IT governance and business-IT alignment was also found.

CONCEPTS OF BUSINESS-IT ALIGNMENT AND IT GOVERNANCE

Business-IT Alignment

One of the first (and one of the best known) theories with regards to business-IT alignment is the Strategic Alignment Model (SAM), developed by Henderson and Venkatraman.[7] SAM identifies four areas: business strategy, IT strategy, organisational infrastructure and IT infrastructure. The central issue in SAM is that organisations should continuously seek alignment amongst these four domains, with particular attention to the strategic fit (connection of the strategy and infrastructure, for both business and IT) and functional integration (connection of business and IT strategy and the business and IT infrastructure). The Henderson and Venkatraman model is portrayed schematically in **figure 1**.

Figure 1—Strategic Alignment Model



Source: Henderson, J.; N. Venkatraman; "Strategic Alignment: Leveraging Information Technology for Transforming Organizations," *IBM Systems Journal*, vol. 32, no. 1, 1993

Business-IT alignment is a complex subject, which makes it difficult to measure in an unambiguous way. The Strategic Alignment Maturity Assessment Method was one of the first concrete models for measuring business and IT alignment.[8] This method provides a comprehensive tool for assessing business-IT alignment in terms of the current situation and what organisations can do to improve alignment.

This method was further validated in 2006,[9] resulting in a list of 22 questions, in which business and IT managers have to give their perception on the degree of alignment on a scale of zero to five. Based on this instrument, the earlier research presented a global business-IT alignment benchmark based on different sectors. An average maturity level of three (on a scale of zero to five) was discerned (see **figure 2**).[10]

This alignment maturity measurement instrument was used in this exploratory study as a basis for business-IT alignment measurement in Dutch SMEs.

IT Governance

As often happens with new management models and principles, many different definitions have been developed for IT governance in recent years. Some important definitions that describe IT governance are:

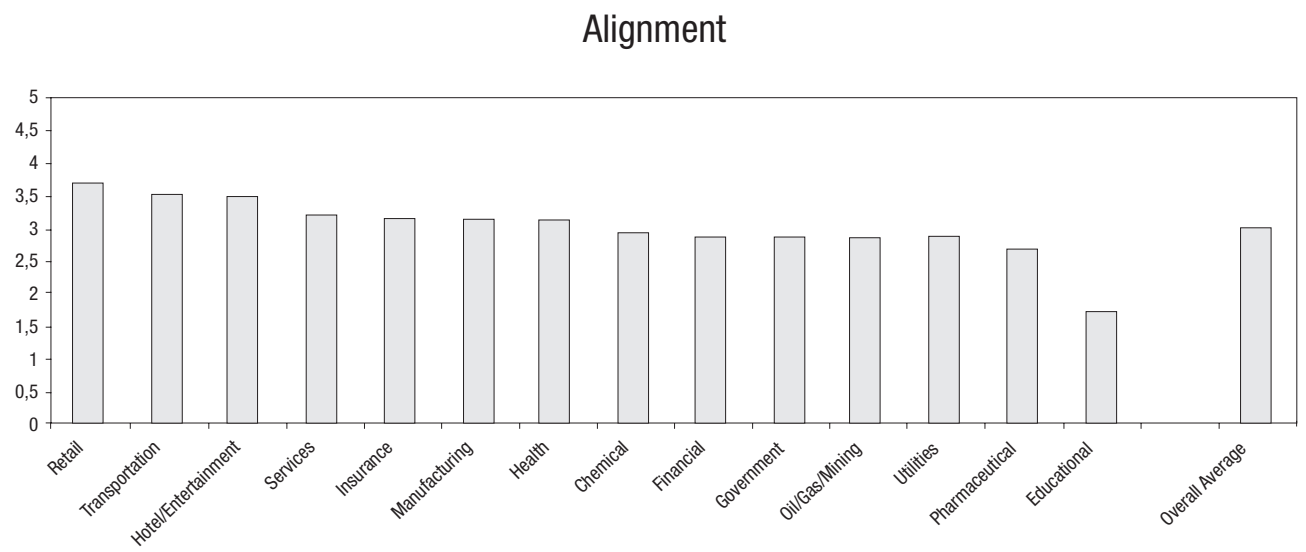
- IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.[11]
- IT governance is the organisational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT.[12]
- Enterprise governance of IT (EGIT) is an integral part of corporate governance and addresses the definition and implementation of processes, structures and relational mechanisms in the organisation that enable both business and IT professionals to execute their responsibilities in support of business-IT alignment and the creation of business value from IT-enabled business investments.[13]

The recent change to speaking about 'enterprise governance of IT' instead of 'IT governance' ensures that the primary responsibility of the business is stressed, thereby ensuring that IT governance does not remain a debate within IT.

In the field, COBIT[14] is more and more accepted as a framework for IT management and governance. This framework includes 34 IT governance processes divided into four domains (Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate) and a broad set of processes and control objectives (see **figure 3**).

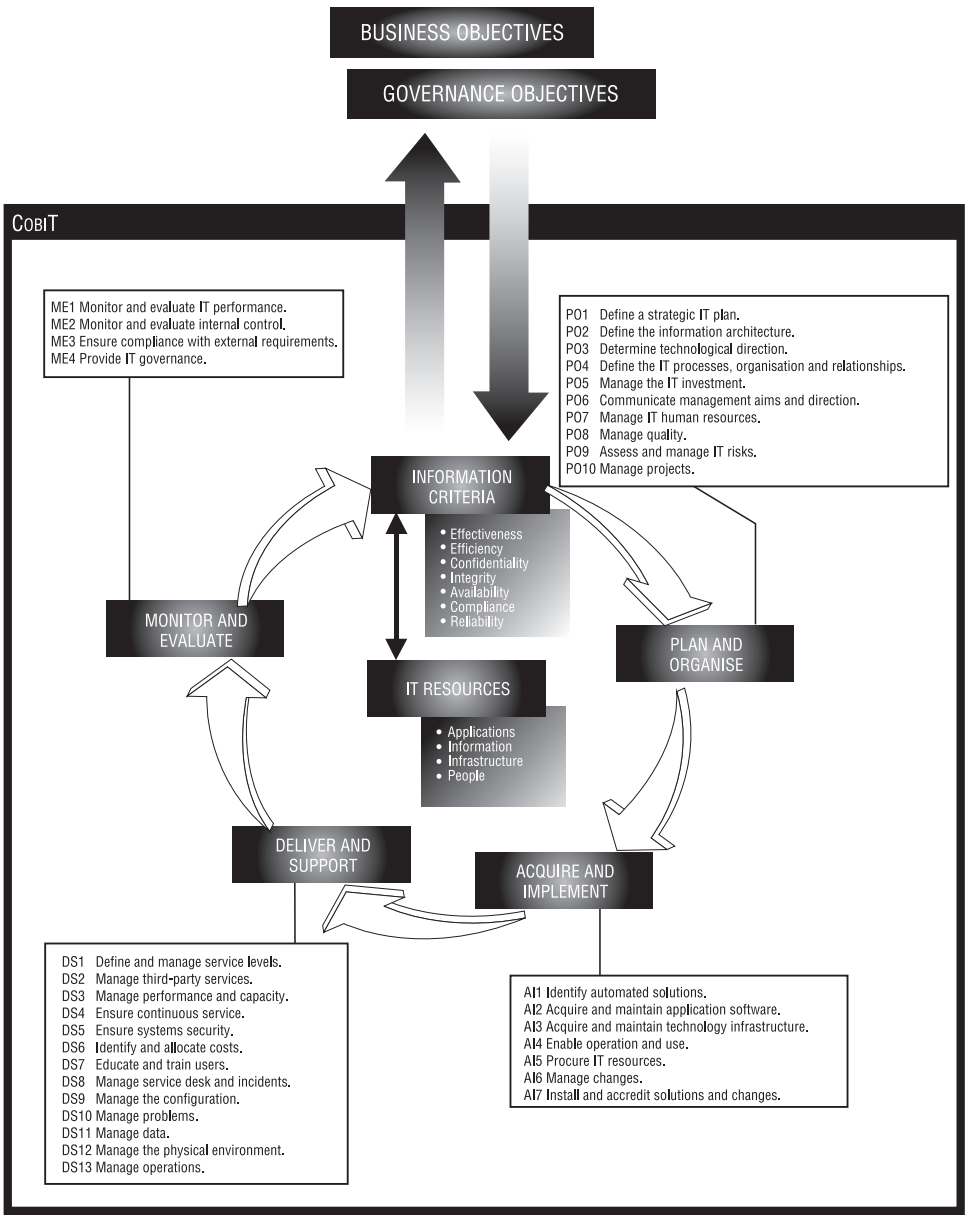
The broadness of COBIT may be perceived as overwhelming to small organisations.[15] ISACA and ITGI

Figure 2—Worldwide Business-IT Alignment Benchmark



Source: Luftman, J.; R. Kempaiah; "An Update on Business/IT Alignment: A Line Has Been Drawn," *MISQ Executive*, vol. 6, no. 3, 2007. Luftman, J.; "Assessing Business-IT Alignment Maturity," *Communications of the Association for Information Systems*, vol. 4, article 14, December 2000

Figure 3—COBIT 4.1



Source: IT Governance Institute, 2008, COBIT 4.1

have equally recognised this and, for these reasons, *COBIT Quickstart* was developed.[16] *COBIT Quickstart* is based on a selection of the processes and control objectives and is a 'light' version of the COBIT framework (see **figure 4**). It presents a simplified version with 32 processes (DS6 and DS7 are not included in *COBIT Quickstart*) and 59 control objectives, which typically apply to SMEs.

Figure 4—Comparison of COBIT and *COBIT Quickstart*

Part	COBIT	*COBIT* Quickstart
Domains	4	4
Processes	34	32
Audit objectives	210	59

Since *COBIT Quickstart* is designed for deployment and management of IT governance in SMEs, this downsized framework was used as a basis for measuring the IT governance implementation status in this exploratory study. The assumption here is that COBIT IT processes are a good proxy to measure IT governance practices.

BUSINESS-IT ALIGNMENT AND IT GOVERNANCE IN DUTCH SMES

Business-IT Alignment

For this study, a sample has been composed containing 20 randomly chosen SMEs in the Netherlands. Each company was asked directly by telephone for co-operation in this study. After confirmation, the companies received a digital questionnaire with which business-IT alignment was measured. The questionnaire was based on the alignment instrument developed by Luftman.[17] This instrument consisted of a questionnaire with 22 questions posed to business and IT managers, in which they scored business-IT alignment on a scale of zero to five. This questionnaire was supplemented with two questions on IT intensity. These IT intensity metrics measure, per company, the relative amount of budget spent on IT in general and on strategic investments specifically. The latter was asked to enable comparison of similar types of organisations, with a focus on comparing organisations with high IT intensity.

Ultimately, 13 workable data sets were collected. For both alignment (A) and IT intensity (I) a mean score was calculated (all scores on a scale of five) (see **figure 5**).

The results show a rather low score for IT intensity for this sample of SMEs. This might suggest that for many companies in this sample, IT may not be seen as a strategic asset. The main conclusion, however, is that SMEs in the Netherlands score rather low regarding business-IT alignment. Under alignment, no responding company reports achieving a maturity level of 3 (the global average as can be seen in **figure 2**). Out of the 13 analysed companies, 10 have reached level 2 and three companies have achieved only level 1.

Figure 5—Survey Results Per Company

#	Company	I	A
1	Company 1	0,8	1,5
2	Company 2	1,0	1,5
3	***Company 3***	***2,3***	***1,5***
4	Company 4	1,0	2,1
5	Company 5	2,5	2,1
6	Company 6	2,8	2,1
7	Company 7	0,8	2,4
8	Company 8	1,5	2,4
9	Company 9	3,0	2,4
10	***Company 10***	***3,0***	***2,5***
11	Company 11	1,0	2,5
12	Company 12	1,0	2,6
13	Company 13	1,3	2,8
	AVERAGE	**1,7**	**2,2**

To give a further explanation on the differences in business-IT alignment, two extreme cases were selected from this sample. The selection of the extreme cases was made based on:

- Outliers in the results of business-IT alignment (one low-scoring and one high-scoring company)
- Firms with high IT intensity

Based on these criteria, Company 3 and Company 10 were retained for further analysis.

IT Governance

As previously indicated, *COBIT Quickstart* forms a suitable framework to analyse the IT governance practices in SMEs. At each company, during an onsite visit, this framework was used as the basis for measuring IT governance implementation status. For each of the 32 COBIT processes described in *COBIT Quickstart*, an implementation status was measured

using the scores shown in **figure 6**. This estimation was made based on several interviews in the organisations, supplemented by documentation such as internal documents and presentations.

Figure 6—Possible Scores to Measure Implementation Status

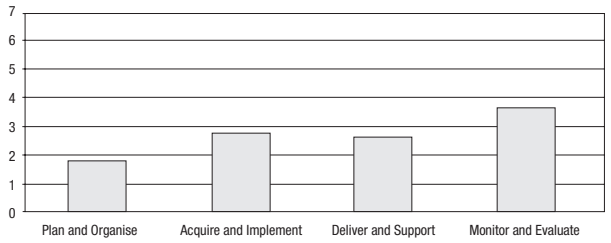
Score	Explanation
0	Management is not aware.
1	Management is aware.
2	The will to implement solutions exists.
3	Implementation is started.
4	Implementation is on track.
5	Solution is implemented.
6	Solution is well maintained.
7	Solution is optimised.

Extreme Case 1: Company 3

The first in-depth study was conducted in Company 3, a trading company with more than 250 employees. The information and communication technologies (ICT) department, part of the administration, consists of two people—the head of IT and the technical system administrator. The head of IT is mainly responsible for the functional/operational issues. The technical system administrator is responsible for the technical/hardware issues. **Figure 7** shows the average score per *COBIT Quickstart* domain. Three areas scored below 3; only Monitor and Evaluate nearly scored a 4. The overall average implementation score for all the processes together was 2.7, implying that the IT governance implementation is not yet started (see the scale in **figure 6**).

The rather low observed implementation status of the COBIT IT processes can be explained by the fact that within this case company, IT is primarily viewed as a supporting cost centre and not as a value-creating activity. As such, there was little attention to improving the IT governance approach. Also, the organisation has limited resources (people) to address these IT governance issues. Moreover, it appeared that most of the processes and knowledge were not documented, again explaining the relative low scores, certainly in the Plan and Organise domain. The relatively high score in the Monitor and Evaluate domain is explained by the fact that the company does have a documented internal control policy, which is evaluated and audited regularly by external experts (accountants).

Figure 7— Company 3 Summary Results

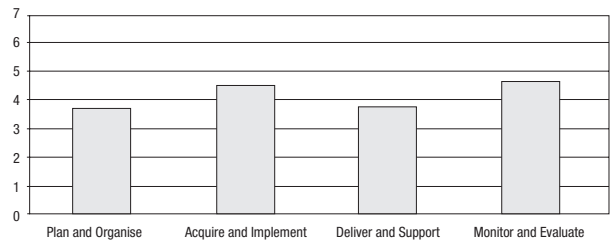


Despite all of this, the case company recently started a step-by-step implementation of the most relevant COBIT IT processes, with the objective to improve its IT maturity.

Extreme Case 2: Company 10

The second in-depth study was conducted in Company 10, a social labour supply entity with more than 1,300 employees. The IT department of Company 10 consists of seven individuals and is divided into network and application management. The IT department consists of a head of ICT, three network administrators and three application managers. **Figure 8** shows the average implementation score per *COBIT Quickstart* domain. All areas scored around 4 on average, showing that implementation is well underway. The overall average score of all the processes was 4.1.

Figure 8— Company 10 Summary Results



The overall conclusion is that part of the company's *COBIT Quickstart* processes have been implemented and that the implementation of the other (relevant) parts has

started or is already well underway. The relatively high score can be explained by the fact that the IT policies were being defined in the context of a large internal reorganisation. Also, a recent failed ERP project raised awareness for the need for better IT governance practices. This explains the high score in the domain of IT development (Acquire and Implement). The high score in the Plan and Organise domain is a result of well-organised *COBIT Quickstart* processes regarding technical infrastructure and organisational aspects of the IT department. Furthermore, the Deliver and Support domain is covered by detailed service level agreements and backup facilities. The scores in the Monitor and Evaluate domain are explained by the existing regular processes of reviews and audits of external experts. Furthermore, part of the developed IT policy includes defined key performance indicators, with which the company intends to measure the performance of IT more concretely in the future.

COMPARING IT GOVERNANCE AND BUSINESS-IT ALIGNMENT

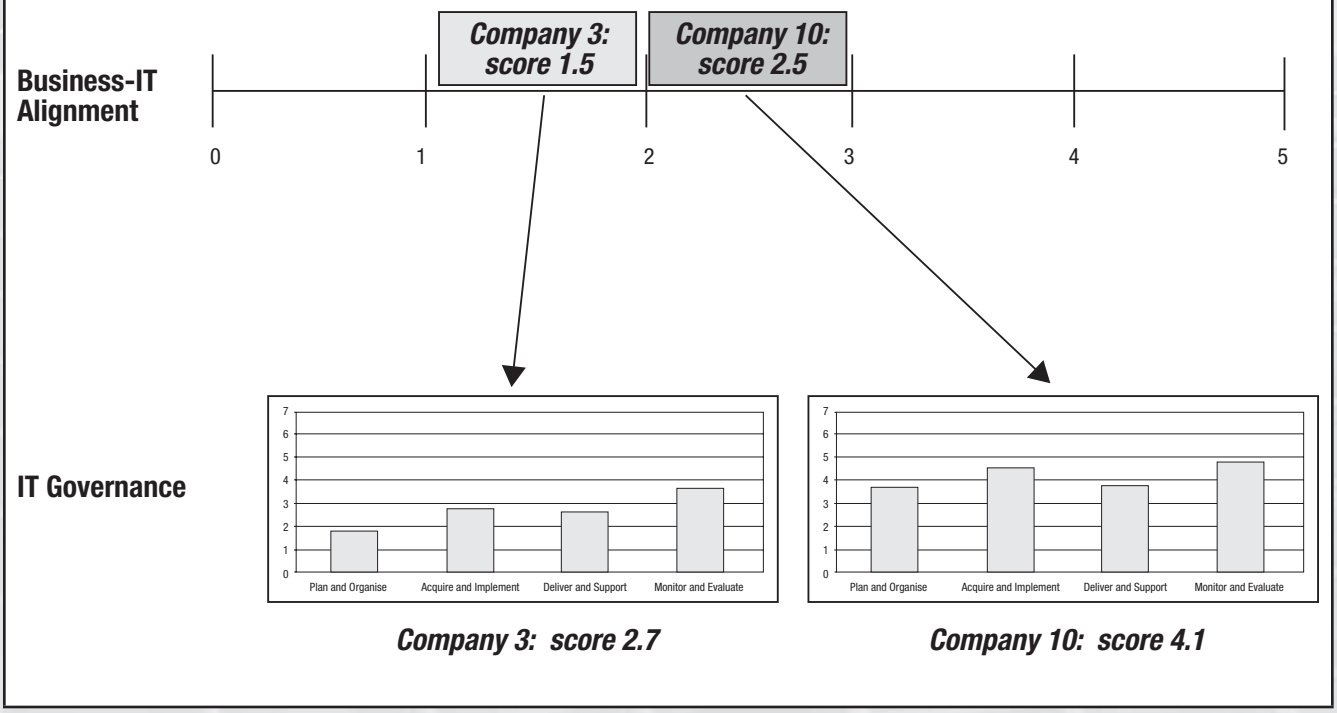
Figure 9 puts together the results of the business-IT alignment and IT governance measurements and illustrates that the company with high business-IT alignment maturity (top of the figure) clearly possesses better IT governance practices (bottom of the figure) as compared to the company with a lower business-IT alignment maturity.

This field study is based on a very limited sample and, therefore, should be interpreted carefully. Nevertheless it may be argued that this outcome illustrates and parallels earlier findings on the relationship between IT governance and business-IT alignment and that, for this sample, it can be extended to SMEs.

CONCLUSION

This article discusses the results of a limited field study on IT governance and business-IT alignment in SMEs in the Netherlands. The main conclusion of this analysis is that in the sample taken, SMEs in the Netherlands are on average not very IT-intensive and score low in the field of business and IT alignment. Further, it was shown for two extreme case companies, with relatively high IT intensity scores in this sample, that the organisation with the lower business-IT alignment results clearly had a lower IT governance

Figure 9—IT Governance and Business-IT Alignment



implementation status, compared to the organisation with the highest business-IT alignment maturity.

Of course, the extent and size of the study sample was limited, but notwithstanding this, it lines up with the results of prior research (in other sectors and environments). As with the prior research, the results indicate that organisations with a better set of IT governance practices are likely to score better in terms of business-IT alignment and *vice versa*. Further studies in the field of SMEs are required to better understand business-IT alignment in this environment and how IT governance can help in improving alignment.

ENDNOTES

[1] De Haes, S.; W. Van Grembergen; "Analysing the Relationship Between IT Governance and Business/IT Alignment Maturity," Proceedings of the 41st Hawaii International Conference on System Sciences (HICSS), 2008, *www.uams.be/itag*

[2] Van Grembergen, W.; S. De Haes; *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value*, Springer, USA, 2009

[3] Luftman, J.; R. Kempaiah; "An Update on Business/IT Alignment: A Line Has Been Drawn," *MISQ Executive*, vol. 6, no. 3, 2007. Luftman, J.; "Assessing Business-IT Alignment Maturity," *Communications of the Association for Information Systems*, vol. 4, article 14, December 2000

[4] Weill, P.; J. Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

[5] This exploratory study was conducted as part of a master thesis within the Executive Master in IT Governance & Assurance at the University of Antwerp Management School (UAMS) (*www.uams.be/ictmanagement*).

[6] *Op cit*, De Haes, 2008; Van Grembergen, 2009

[7] Henderson, J.; N. Venkatraman; "Strategic Alignment: Leveraging Information Technology for Transforming Organizations," *IBM Systems Journal*, vol. 32, no. 1, 1993

[8] *Op cit*, Luftman and Kempaiah

[9] Sledgianowski D.; J. Luftman; R.R. Reilly; "Development and Validation of an Instrument to Measure Maturity of IT Business Strategic Alignment Mechanisms," *Information Resources Management Journal*, vol. 19, no. 3, 2006, p. 18-33

[10] *Op cit*, Luftman and Kempaiah

[11] ISACA, Glossary, *www.isaca.org/glossary*

[12] Van Grembergen, W.; "Introduction to the Minitrack: IT Governance and Its Mechanisms," Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS), 2002

[13] *Op cit*, Van Grembergen, 2009

[14] IT Governance Institute, COBIT 4.1, 2008

[15] *Op cit*, Ridley. These authors argue, for example, that large enterprises will implement the COBIT framework more often and more rapidly than SMEs.

[16] IT Governance Institute, *COBIT Quickstart, 2nd Edition*, 2007

[17] *Op cit*, Luftman and Kempaiah

A Higher Level of Governance—Monitoring IT Internal Controls

Mike Garber, CGEIT, CIA, CITP, CPA, has many years' experience as both director for IT governance and as IT audit director for Motorola Inc. (USA), a Fortune 500 company. Since his retirement, Garber has become an independent consultant, focusing on audit practice optimization and risk assessments. Most recently, he was a member of the ISACA core team that wrote *Monitoring Internal Control Systems and IT.*

In the past few years, senior management's interest in good internal controls has increased. Surveys in recent financial magazines show that many chief financial officers (CFOs) would like to have internal control monitoring programs in their enterprises, but do not know where to start to develop a program.[1, 2]

WHAT HAS CHANGED

Many public and private agencies are requiring verification that internal controls are in place and operating effectively—at all times. In the US, the Sarbanes-Oxley Act of 2002 mandates effective controls for financial reporting. Many companies, particularly in Europe, require certifications that show compliance with various International Organization for Standardization (ISO) process standards. Credit card companies are requiring compliance with the Payment Card Industry Data Security Standard (PCI DSS). Internationally, privacy laws are gaining public attention. Companies need to ensure ongoing compliance in many business areas.

> "Controls tend to degrade over time and between audits."

Compliance with laws and regulations is generally the responsibility of business management. Business management should lead the identification and implementation of good internal controls. Traditionally, internal audit organizations, IT compliance functions and public accountants have performed audits and reviews to measure compliance with company internal control processes, laws and standards.

However, audits and separate reviews determine internal control effectiveness only at a single point in time. Controls tend to degrade over time and between audits. With the current growing focus on internal controls, it is no wonder that both senior IT and finance management are now more interested in control monitoring.

WHERE TO START? MONITORING PROGRAM SPONSORSHIP

Strong sponsorship and tone at the top are required for an effective monitoring program. Unlike audits and separate compliance reviews, monitoring requires ongoing testing and evaluation. Detailed sampling and testing for a monitoring program may need to be performed by IT staff or those in business operations, rather than by corporate audit and compliance organizations. Management of the areas in the scope of monitoring programs needs to understand the benefits of the monitoring program. Having the support of senior management will help facilitate cooperation of staff members who will need to perform the monitoring process.

An easy-to-understand project plan or project charter will facilitate communication with senior management and the business operations areas under consideration for monitoring and include the following steps.

Step 1—Prioritize Risks

One of the challenges IT professionals may face when being involved in a monitoring project is linking IT risks to business risk. This requires focusing on IT processes to determine how the business may be affected by internal and external IT risk factors.

This involves understanding:

- Each business process and the role IT plays in that process
- The business objectives, related risks and key controls associated with the business process

Asking and answering questions such as the following can facilitate the IT professional's understanding of the business process and the internal control environment:

- What is the objective of the business process?
- When and how does the process start? What are the triggers? Is there only one trigger or are there many? Have they all been identified?
- When and how does the process end?
- Which process steps or control activities are automated? Which are performed manually? Who performs the manual control activities?

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.

- How is success (achievement of the predicted outcome) measured? Do the metrics cover the essential parameters to determine whether the objective is being met? These parameters include:
- Effectiveness—Does it meet the output criteria (i.e., deliver what was ordered) with the promised quality and timeliness?
- Efficiency—Are resources managed well?
- Reliability—Does it meet specifications?
- Other key factors—Are security, timeliness, confidentiality, integrity, availability and compliance addressed?
- Who is accountable for the overall process performance?
- Can process participants and their related roles and responsibilities in the process be identified?
- What other information is utilized in the process?
- Are significant risks related to the business process identified and prioritized?
- Are control activities defined to address higher-priority risks?

Risks should be considered in the context of organizational/business objectives so they can be prioritized and appropriate resources can be allocated to manage them. A formal risk assessment can identify and evaluate the full range of risks against the stated business objectives and the enterprise's unique business environment. It also can highlight functional areas that are most likely to impact enterprise objectives so that management can make informed choices about where to focus their monitoring efforts. No enterprise has unlimited resources. Information, people, applications and infrastructure allocated to reduce risk in one area inherently deplete resources that could be employed in other, potentially higher-risk areas.

Step 2—Identify Key Controls and Information

Start by identifying key controls in the process area under consideration for monitoring. In many organizations, processes have already been documented through past audits or compliance reviews. Using existing available documentation will help maintain focus on key controls—monitoring should focus only on key controls. Key controls are those that, if they fail, could materially affect the business objectives of the process or the organization. Past audits or reviews may help to identify controls that frequently fail or are more susceptible to business changes.

It is also important that the baseline of effective internal controls be identified and defined. The characteristics of the effective operation of the key controls identified need to be known to understand under what circumstances variation to the baseline would result in control failures. Past audit or review work can help to provide necessary information. By selecting key controls that address risks, management can efficiently focus its limited resources on high-value control activities.

Figure 1 describes considerations relating to the complexity and maturity of business and IT process control types.

Figure 1—Business and IT Process Control Types and Considerations

Process Criteria	Considerations
More complex	Use existing process documentation methodologies, such as Six Sigma's Suppliers, Inputs, Process, Outputs, Customers (SIPOC), to identify controls that may benefit from monitoring.
Less complex (mature, routine or not complex)	Select monitoring activities that can be leveraged across multiple controls. Use existing technology or off-the-shelf tools for monitoring controls with minimal investment.
More mature (well defined and managed)	Integrate control monitoring into the daily business process operations (and the business process documentation) to add value.
Less mature	Once a control baseline is established, implement more frequent and stringent monitoring of the control until a control baseline is established.

Broad monitoring coverage for *all* key controls can be achieved by using a combination of direct and indirect information sources. Monitoring depth and frequency of *specific* key controls can be further determined by considering the following:

- How directly does the control support the relevant business objectives?
- What risks does the control address, and how important are they?
- Is the control considered a key control?
- What are the feasibility and costs of monitoring the control (using either direct or indirect information)?
- What is the nature of the control? Is it manual or automated, detective or preventive, etc.? If manual, is it dependent on IT information or an IT process for its effectiveness?
- If historical data are available, what is known about the maturity and past operating effectiveness of the control?

Once these factors are considered, the process of identifying the controls to be monitored and the information source for monitoring (direct or indirect) can begin. The following actions should be taken:

- **Identify controls that are in scope for monitoring**—Although key controls should be monitored, the degree of

monitoring may vary based on the relative risk and value of each control. For example, those controls that address risks related to the most important business objectives and those that support multiple objectives may be monitored more extensively.

- **Determine the information sources available for monitoring**—Direct information is more effective than indirect information in ongoing monitoring and it usually allows for fewer separate evaluations. Information that comes directly from the control process is preferable to indirect information. Direct information is generally highly persuasive because it provides an unobstructed view of control operation; direct information comes directly from the execution of the control. In addition to direct information, however, indirect information such as key performance indicators (KPIs) may be useful. KPIs, as found in ISACA's COBIT framework, can provide an excellent source for determining potential indirect monitoring measures.

In short, the management team expects that its most important processes will be both well defined and tightly controlled. The rigor of managing and measuring a process can vary, however, and depends greatly on how the enterprise interprets the relative importance of one process in comparison to others.

Step 3—Implement Monitoring

Implementing a monitoring program begins with the development of a project plan. Six Sigma and other project management methodologies provide excellent templates for planning and communication. **Figure 2** provides an example of a practical project charter template.

Once the project plan has been developed, the process of determining the frequency for monitoring, developing the monitoring procedures and setting thresholds for monitoring that utilize indirect information can begin. The following actions should be taken:

- **Determine monitoring frequency**—A determination must be made regarding the use of ongoing monitoring, separate evaluations or a combination of both techniques. When ongoing techniques utilize highly persuasive information (i.e., direct information), they can routinely provide evidence that a control is operating as intended. If they use less persuasive information (i.e., indirect information),

Figure 2—Attributes of a Monitoring Project Plan

Attribute	Description
Business case	Describes the benefits for undertaking a monitoring project. Why is this monitoring project important to the enterprise? What are the risk implications of the failure of key control(s) selected for monitoring? Why is it important to do it now? How does the monitoring project align with enterprise goals? What are the consequences of *not* doing this monitoring for the enterprise?
Problem/ opportunity statement	States what problems or needs the initiative will solve and clarifies the "why" of undertaking the project. For example, control failures within the software change management process can result in processing errors and other control failures affecting enterprise operations and can make excessive programming rework necessary within the IT department.
Goal statement	Defines the objective of the project in measurable terms. The goal statement should solve the potential problems identified in the problem/opportunity statement. The goal statement provides direction for detecting control failures, leading toward solutions. For example, monitoring of key controls within the change management process—specifically, the use of formal change request forms, approval of change requests by authorized personnel and testing of all changes in compliance with enterprise policy—will increase system reliability, help availability, decrease rework and help contain cost.
Scope	Defines the boundaries of the project and should answer the following questions: • What parts of the enterprise or business processes are included in the scope? • Where will the work be performed? • What parts of the enterprise or business processes are *not* included in the scope? • What is the role of IT and users in this project? • Can the project be subdivided so that a pilot area can be reviewed first to test the assumptions, data collection and testing processes?
Approach	Defines the information, methods and tools selected for monitoring projects. The type of sampling may also be documented.
Timeline and budget	Documents the major milestones, timing and estimated costs for the project. At a minimum, the plan should consider the time for the design, implementation, testing and periodic follow up on results. It should also identify any out-of-pocket costs that may be incurred, including any ongoing maintenance costs and, if appropriate, internal personnel costs.
Project team	Identifies the monitoring team. The team members should include people with a good knowledge of the business process. They should have IT skills that enable them to understand the IT processes and controls. If specialized IT automated audit tools are required to obtain sample transactions for review, someone on the team needs to have the skills and experience to develop the automated testing process.
People accountable and responsible	Identifies the senior management personnel who are accountable for the monitoring project, and identifies the leaders of the monitoring project and key members of the business process teams involved in the monitoring
Evaluation and feedback	Identifies how project success is going to be measured. It may consist of nothing more than reviewing the results of the monitoring activity and determining whether the goals of the project were realized. For example, using the goal statement example, evaluation may consist of review, on a periodic basis, for positive changes to the metrics around system reliability, help availability, rework and cost containment.

additional separate evaluations may be required more frequently. In both cases, separate evaluations may be required periodically.

Automation is another consideration in determining the frequency of monitoring. In general, based on the assessed level of risk (key control or not), automated controls require less frequent monitoring of their automated aspects because once the control is verified to be working properly, automated aspects are unlikely to change unless change management controls cannot be relied upon. Nonautomated aspects, such as follow-up on reported exceptions, may require more frequent monitoring, depending on the risks. An automated control may allow for even greater usage of indirect information, once the initial baseline for using direct information has been established, as system controls are less likely to degenerate than manual controls if—and *only if*—the underlying IT general controls are effective.

- **Develop monitoring procedures**—A monitoring procedure needs to be developed for both ongoing and separate evaluations. The project plan should specify the information source to be utilized for each approach. Enterprises using indirect information as a source for ongoing monitoring will still find it necessary to perform a separate evaluation using more persuasive or direct information. In addition, monitoring procedures that provide comfort over more than one control may be given preference over more targeted procedures (e.g., the review of a change control ticket may provide evidence of business sign-off, testing results and the existence of a back-out plan).
- **Determine thresholds for monitoring when utilizing indirect information**—Indirect information cannot provide positive assurance that a control is operating effectively; however, indirect information can be a good indicator of the effectiveness with which the process meets its overall performance objectives. If such indirect information suggests that the performance objectives are not being met, this may indicate that the related key controls are not functioning effectively. A tolerance window for the deterioration of a key metric or indirect monitoring should be established to trigger the need for direct monitoring or other follow-up action.

To be successful, accountable process owners need to be able to rely on the monitoring process itself for reliable results. Consequently, their involvement is essential during the development process and once the monitoring process is operational.

To ensure correct results and conclusions, the monitoring process must be repeatable and it must minimize the variations in how monitoring is performed. In cases in which a monitoring process is critical to an enterprise, it may be necessary to implement controls over the monitoring process itself to detect and manage variability in how the data are extracted, validated, analyzed and reported.[3]

Wherever possible, monitoring programs should leverage automation. Automation of testing can reduce the effort needed to perform internal control monitoring and reduce resistance to implementation of a monitoring program. Automated monitoring is less likely than manual monitoring to produce variations in the monitoring processes. As stated previously, effective IT general controls must be in place for development and subsequent operation of automated monitoring solutions. These include controls over software development, software maintenance, and system and user testing. Such controls are covered in detail in various ISACA publications, such as COBIT® 4.1, *Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0* and the *IT Assurance Guide: Using COBIT®*.

After monitoring program design and implementation are complete and the system is operational, processes need to be in place to monitor and assess the results. Although testing would have been performed to validate functionality during development, ongoing activities that need to be considered include:

- Reviewing the monitoring results to minimize false positives or negatives and to ensure valid, current and timely results. Control failures may be reported when, in fact, they are not failures because the business itself has changed. This would be more likely to be true with continuous controls monitoring solutions vs. manual monitoring processes.
- Determining the reason for the control failure
- Reporting results back to the project sponsors, along with any recommendations, so they can implement corrective actions

Once the monitoring process flags a potential control failure, identifying the root cause will aid in defining appropriate corrective actions. The goals of root-cause analysis are to identify and correct the primary reason for the failure of the controls. More information may need to be gathered, such as when, where and how the failure occurred. Did it occur because of a recurring condition that could be resolved by process improvements, or was it due to a less common or special circumstance that would have been difficult to predict or anticipate? Further testing or sampling may be required to determine whether the failure is repeated.

It is important to identify the appropriate levels of enterprise management that must be informed about the condition or event, the type of corrective action that is or will be taken, and the expected time frame for mitigation (assuming it is not postrecovery). Management should receive information that is clear and concise (preferably stated in nontechnical business terms) to enable efficient and effective understanding of the impact to the enterprise and clients.

As a minimum for reporting, the results of monitoring should include the items listed in **figure 3**.

Figure 3—Items to Include in a Report on Monitoring Results

Item	Related Action
Problem statement	Identify the problem, e.g., control failure.
Cause identification	Describe the root cause of the control failure.
Perspective on risk	Describe the risk to the business process created by the control failure. For example, the risk may be lack of compliance with a particular standard or regulatory requirement. Also, describe any adverse consequences that might have occurred.
Recommendations	Identify the corrective action, including what is to be done, by whom and by when (estimated completion date). Any follow-up actions should also be discussed.

Any warranted and cost-justifiable changes should be noted, and any changes resulting from corrective actions taken should be mapped back to any processes affected. Documentation should be updated and appropriate personnel notified. Also, the monitoring process should be regularly reviewed to help ensure that the monitoring process and the controls it monitors continue to operate effectively.

CONCLUSION

Senior management is interested in saving time, money and other resources in business processes. Finance and IT management want to know that internal controls under their responsibility are operating effectively at all times. Internal audit and IT governance personnel can meet the needs of their management through the development of efficient and cost-effective internal controls monitoring programs

To develop a good internal controls monitoring program, the following are needed:

- Management sponsorship and tone at the top
- An understanding of business processes, objectives and organizational structure
- An established baseline of effective internal controls from the past or from a current review
- Identification of key controls and prioritization of risks
- Identification of information for monitoring controls (direct information is best)
- A good project plan and implementation of monitoring
- A report on the findings of the monitoring processes
- A follow-up process for corrective actions

EDITOR'S NOTE

The new ISACA publication *Monitoring Internal Control Systems and IT* is available in the ISACA Bookstore and posted for complimentary download on the ISACA web site, *www.isaca.org.*

ENDNOTES

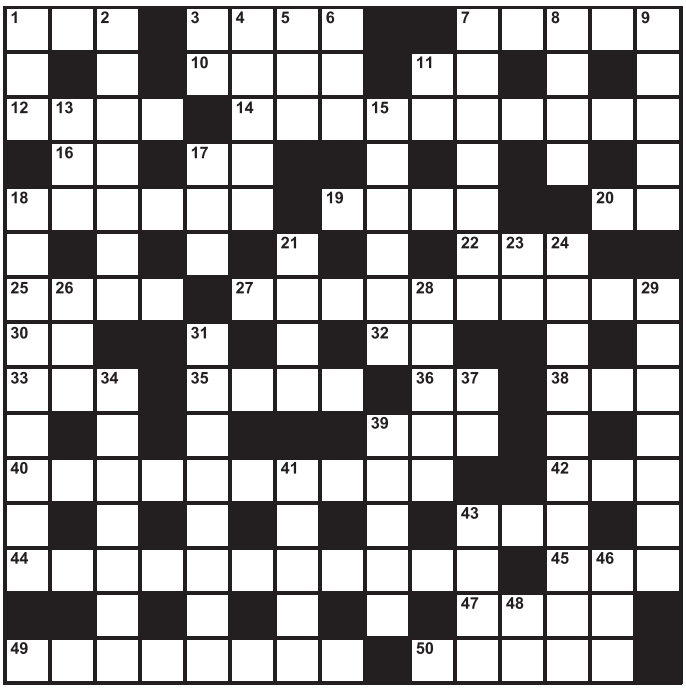
[1] *CFO Magazine*, 10 December 2009

[2] *CFO Magazine*, 12 January 2010

[3] An analytically based process is available to help ensure the accuracy of monitoring. Measurement Systems Analysis (MSA) is a Six Sigma-based process for analyzing the monitoring processes for potential variation and defects. For further information on how to create and use an MSA process, refer to a Six Sigma Black Belt resource or to web sites such as *iSixSigma.com.*

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1 US president who said: "The plan is nothing. Planning is everything."
3 Key tool for conducting fraud and IT audits, abbr.
7 Obsessive computer enthusiasts
10 Data ___
11 Reputation
12 Plans, with out
14 Combine into a working whole
16 Place, for short
17 Old, for short
18 One of the three core capability areas around which the DGPC framework is organized
19 Expert in underhanded activities
20 Privacy protection concern, abbr.
22 Member of a colony
25 Selects
27 More secret
30 Certificate of insurance, briefly
32 Go head __ head
33 Jellied delicacy
35 Dynamic connection from 3 across to the operational database, abbr.
36 Green light
38 Oracle's huge system of more than 130 integrated business applications
39 Attack
40 Lack of growth and expansion
42 Identifier associated with a piece of data
43 Last in a series
44 Scenario for a data center after a disaster (2 words)
45 Web application framework
47 It wasn't built in a day
49 Description of most CIO positions (2 words)
50 Undisciplined

DOWN

1 Technologies that help protect information from unauthorized access while enabling use by legitimate users, abbr.
2 Take advantage of
3 Continuous auditing and monitoring, abbr.
4 Walkway
5 "___ questions?"
6 Top score in many tests
7 "Reformed" criminal cracker: ____ hacker (2 words)
8 Google's promise: not to be ___
9 Budgeting figure
11 Acid measurement, abbr.
13 Copy
15 Source of danger
17 Outdated
18 Another of the three core capability areas around which the DGPC framework is organized
21 Piece of code used for converting parameters
23 Connecticut (USA) locale
24 Security and penetration specialists (2 words)
26 Kind of chart
28 Go online (2 words)
29 ____ Analysis Matrix (2 words)
31 Period of business interruption
34 Escape, as in business secrets (2 words)
37 Overtime, for short
39 "_____ policies throughout the confidential data life span"
41 Demanding strict attention to rules and security
43 Affordability and risk maxim: "the more downtime and data loss approach ____, the higher the cost will be"
46 Watch
48 Hawaiian bird

(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 My organisation got certified for BS 7799 and then later got the certificate upgraded to ISO 27001:2005. One area in which we feel the organisation is weak relates to security compliance. We believe and have been told by our auditors that we do not have appropriate measurement systems in place to measure the effectiveness of our levels of security compliance.

What is your advice? Should we implement any tools? How do we achieve our objectives with minimal costs? Ours is a small to medium-sized organisation and we cannot afford a huge expenditure to make this happen.

A A famous quote of management's: 'What you cannot measure, you cannot manage'. I strongly agree with the quote. If we need to manage something effectively, we should be able to lay our hands on metrics relating to the same.

Having dealt with topics on security metrics in the past, let us discuss more in terms of a generic framework and the need for a structured methodology to determine the metrics. Not all metrics or measures are essential or useful to all organisations.

My formula on effectiveness metrics is very simple and straightforward. We should aim for the measurement of the following metrics:

- Exceptions to policies and standards
- Incidents
- Status of compliance with key control parameters
- Tracker on issues identified and reported in audits

Policies and standards dictate the baseline controls expected to be in place across the organisation. Unless specifically stated in polices and standards, the tenets of the policy will, or rather must, apply to everyone in the organisation. At the same time, it is understood that there will be compelling business needs where exceptions to the policies and standards have to be granted.

However, it is essential to have is a foolproof exceptions-approval process in place. The requests for all such exceptions must be tracked using a repository of any form; the risks that get opened due to the granting of exceptions must be clearly documented in the same repository, against each of the requests. The compensating controls to mitigate any potential risks and outstanding residual risks must also be documented in the repository. Depending on the quantum of residual risks and exposure, there should be a multi-staged approval process to give a green signal in terms of exceptions.

Exceptions granted must be for set or predefined periods only, after which they must expire automatically. The repository system must have inbuilt features, ideally, to notify the users in advance that their exceptions requests will be expiring soon and asking them to reapply for the same.

If such a system were to exist and function, the *information on exceptions* in the repository would be of value to measure the effectiveness of security and it would form part of the framework.

Tracking of incidents is the next most important part of the framework. An incident-free regime is next to impossible. No number of security controls can ever lead to or guarantee zero incidents. If people tell you that they have nil security incidents in their organisations, it means that they are kidding you or themselves. Something may be fundamentally wrong in their definition of incidents and/or their incident management policies.

It is essential to develop and roll out a process to report and track incidents. The size of the potential or actual impact caused should determine the various escalation levels of reporting. Needless to say, all incidents reported must be tracked centrally, through a repository system.

It is essential to determine and understand whether any patterns or trends emerge out of the reported incidents. Trend analysis of incidents renders better information than incidents looked

at in isolation. I am not ruling out the need to do a post-incident review in terms of lessons learnt individually, but my point is that taking a holistic view can render better information whilst we undertake any trend analysis.

The third component of this framework relates to the *compliance status of the various control parameters* chosen in terms of security. Whilst a number of controls may get implemented and rolled out as enunciated by the various policies and standards, it is important to classify the controls and segregate the most important ones amongst the various others. Not all controls may be measurable and not all of them may be subjected to measurement. Once the key controls are identified, it may be easier to seek the status of compliance for those key controls. Let us take the simple example of desktops or workstations. Whilst there can be a multitude of parameters against which standards can be set, it may work out to be a costly proposition in terms of time and efforts to measure the status of all parameters. So, key parameters such as domain membership (assuming the organisation is operating in a typical Windows environment) and antivirus precautions may alone be measured. Given that various controls are pushed through the central domain policy, a domain membership can, in general, mean that a lot of controls are in place, eliminating the need for doing any individual checks.

The last component relates to the *tracking of issues identified during the course of various internal and external audits*. A culture in which people fear audits and feel that they may get penalised for adverse findings reported in audit reports is not going to help the organisation in the long run. Appearance and reporting of issues in any audits should never be construed as something linked to an individual's performance in that area. Audits are there to identify and unearth issues given their independent perspective, and it is essential to track them to closure. People can be penalised for not closing the issues effectively or if the same issues recur again and again in audit reports.

Given the size and complexity of your small to medium-sized organisation, I do not envisage any other special requirements. Of course, you know your organisation better than anyone else and can best determine the right requirements.

CPE Quiz

Prepared by Kamal Khan

Quiz #133

Based on volume 4, 2010—Toolbox for IT Auditors

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

TRUE OR FALSE

HOESING ARTICLE

1. The VMware ESX 3.5 virtualization host can provide details of the current configuration by issuing the config-info command.
2. Kismet is a commercial software tool used to assess Payment Card Industry Data Security Standard compliance for wireless access points.
3. Analyzing a single file may not produce useful audit information; often, additional data in secondary files are needed to fully understand the original file.

BELL ARTICLE

4. Statement on Auditing Standards No. 70 is a defined standard developed by the American National Standards Institute as a set of criteria a service or user organization's auditor should use while assessing the outsourced internal controls of a service organization.
5. A Type I service auditor's report is a thorough report of a Statement on Auditing Standards No. 70 audit because it contains a description of the controls in place following a minimum testing period (generally six months or longer). A Type II report examines controls over only one or two days, which arguably has limited value to a user organization.
6. Triple Constraint consists of scope (project size, goals, requirements), cost (people, equipment, material) and schedule (task durations, dependencies, critical path), with quality a requirement for all three constraints.

REED, WANG AND DUTTA ARTICLE

7. A number of studies show that much of the data warehouse information available to business users is not accurate, complete or timely.
8. Causes of information errors within data warehouses include changes in the source system and process failures.
9. Control X2—validation that the extraction, transformation and loading (ETL) process is accurate and complete—involves monitoring transactions and processes, e.g., source to ETL, and data warehouse to data mart.

EE ARTICLE

10. In September 2009, the Public Company Accounting Oversight Board found, from a review of more than 250 audits, that areas for improvement include risk assessment, consideration of fraud, entity-level controls and deficiency evaluation.
11. Four key risk factors for fraud are inherent susceptibility, keys to the kingdom, process maturity and organizational maturity.
12. According to the article, there was a real-life situation in which a systems administrator planted a logic bomb that cost the company more than US $4 million in remediation efforts.
13. One example of an SDLC-related risk is the introduction of trapdoors in new or modified code from a lack of code review.

FARAHMAND ARTICLE

14. The American Institute of Certified Public Accountants defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources."
15. Use of the cloud is contingent on accessing the Internet and the cloud servers.
16. Individuals are less likely to perceive information collection procedures as privacy-invasive if information is collected in the context of an existing relationship and they believe the information will be used to draw reliable and valid inferences about them.
17. Merrill Lynch estimates that within the next five years, the annual global market for cloud computing will surge to US $9 million.

ISACA Journal
CPE Quiz
Based on volume 4, 2010—Toolbox for IT Auditors

Quiz #133 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC# _____

Quiz #133

True or False

HOESING ARTICLE

1. _____
2. _____
3. _____

BELL ARTICLE

4. _____
5. _____
6. _____

REED, WANG AND DUTTA ARTICLE

7. _____
8. _____
9. _____

EE ARTICLE

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

FARAHMAND ARTICLE

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

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

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

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

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

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

Answers—Crossword by Myles Mellor

See page 50 for the puzzle.

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

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 Revised May 2003

Advertisers/Web Sites

CA technologies	*www.ca.com*	Back Cover
CCH Teammate	*www.CCHTeamMate.com*	Inside Back Cover
Citrix Online	*www.gotoassist.com/isaca*	6
ExamMatrix	*www.ExamMatrix.com/ISJ*	16
Modulo Risk Manager	*www.modulo.com*	1
University of Maryland University College	*www.umuc.edu/cyberedge*	12
Visual Click	*www.visualclick.com*	9

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

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

ISSN 1944-1967

Leaders and Supporters

ISACA Bookstore

Resources for your Professional Development

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

2011 CISA® EXAM REFERENCE MATERIALS

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

CISA REVIEW MANUAL 2011

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

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

QAE-11	English Edition	(900 Questions)
QAE-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-11FS	French Edition	(100 Questions)
QAE-11GS	German Edition	(100 Questions)
QAE-11IS	Italian Edition	(100 Questions)
QAE-11JS	Japanese Edition	(100 Questions)
QAE-11SS	Spanish Edition	(100 Questions)

CISA PRACTICE QUESTION DATABASE V11

(1,000 Questions)

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

CANDIDATE'S GUIDE TO THE CISA EXAM AND CERTIFICATION

CAN (No charge to paid CISA exam registrants)

2011 CISM® EXAM REFERENCE MATERIALS

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

CISM REVIEW MANUAL 2011

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

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

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

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011 SUPPLEMENT

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

CISM PRACTICE QUESTION DATABASE V11

(750 Questions)

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

CANDIDATE'S GUIDE TO THE CISM EXAM AND CERTIFICATION

CGC (No charge to paid CISM exam registrants)

2011 CGEIT EXAM REFERENCE MATERIALS

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

CGEIT REVIEW MANUAL 2011

CGM-11 English Edition

CGEIT REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CGQ-11	English Edition	(50 Questions)

CANDIDATE'S GUIDE TO THE CGEIT EXAM AND CERTIFICATION

CACG (No charge to paid CGEIT exam registrants)

2011 CRISC EXAM REFERENCE MATERIALS

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

CRISC REVIEW MANUAL 2011

CRR-11 English Edition

CRISC REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CRQ-11	English Edition	(100 Questions)

CANDIDATE'S GUIDE TO THE CRISC EXAM AND CERTIFICATION

CACR (No charge to paid CRISC exam registrants)

COBIT®

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

COBIT® 4.1

IT Governance Institute

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

COBIT AND APPLICATION CONTROLS: A MANAGEMENT GUIDE

ISACA

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

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

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

COBIT SECURITY BASELINE, 2ND EDITION

IT Governance Institute

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

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

IT Governance Institute

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

COBIT QUICKSTART, 2nd EDITION

IT Governance Institute

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

COBIT USER GUIDE FOR SERVICE MANAGERS

IT Governance Institute

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

IMPLEMENTING AND CONTINUALLY IMPROVING IT GOVERNANCE

ISACA

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

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

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

IT ASSURANCE GUIDE: USING COBIT

IT Governance Institute

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

SHAREPOINT DEPLOYMENT AND GOVERNANCE USING COBIT 4.1: A PRACTICAL APPROACH

Dave Chennault and Chuck Strain

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

(cont. p.S-2)

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

2010, 176 pages. **SDG**

RISK IT AND RISK RELATED TOPICS

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

INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS

Jake Kouns and Daniel Minoli

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

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

THE RISK IT FRAMEWORK

ISACA

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

2009, 104 pages. **RITF**

THE RISK IT PRACTITIONER GUIDE

ISACA

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

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

2009, 134 pages. **RITPG**

Val IT™

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

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

THE VAL IT FRAMEWORK 2.0

ISACA

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

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

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

GETTING STARTED WITH VALUE MANAGEMENT

ISACA

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

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

VALUE MANAGEMENT GUIDANCE FOR ASSURANCE PROFESSIONALS—USING VAL IT 2.0

ISACA

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

THE BUSINESS CASE GUIDE—USING VAL IT 2.0

ISACA

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

AUDIT, CONTROL AND SECURITY—ESSENTIALS

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

ACCOUNTING INFORMATION SYSTEMS, 8TH EDITION

NEW

Ulric J. Gelinas, Richard B. Dull

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

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

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

NEW

Ramesh Subramanian

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

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

COMPUTER SECURITY: PROTECTING DIGITAL RESOURCES

NEW

Robert C. Newman

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

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

NEW

Robert K. Wysocki

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

GFI NETWORK SECURITY AND PCI COMPLIANCE POWER TOOLS

NEW

Brien Posey

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

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

EMC

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

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

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

ITAF: A PROFESSIONAL PRACTICES FRAMEWORK FOR IT ASSURANCE

ISACA

ITAF: A Professional Practices Framework for IT Assurance consists of compliance and good practice setting guidance. The IT Assurance Framework™ (ITAF™):

- Provides direction on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge, skills and diligence, conduct, and reporting requirements

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

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

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

APPLIED ORACLE SECURITY: DEVELOPING SECURE DATABASE AND MIDDLEWARE ENVIRONMENTS

NEW

David Knox, Scott Gaetjen, Hamza Jahangir, Tyler Muth, Patrick Sack, Richard Wark and Bryan Wise

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

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

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

NEW

ISACA

This updated edition of one of ISACA's most popular guides reflects the many changes that the business environment and Oracle ERP application have undergone since the second edition was published. In response to customer needs and an increased market awareness of governance, risk and compliance (GRC), Oracle Corporation has continued to boost its GRC offerings and released the updated and improved Oracle E-Business Suite R12.1 (EBS) in 2009.

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

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

ISACA

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

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

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

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

Deloitte Touche Tohmatsu Research Team and ISACA

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

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

This in-demand new edition has been updated to reflect:

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

2009, 470 pages. **ISAP3**

NON-ENGLISH RESOURCES

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

AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.

Piattini, M. y otros

2008, 732 Págs. **3-RAMA**

CISA EXAMINATION REFERENCE MATERIAL

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

CISM EXAMINATION REFERENCE MATERIAL

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

COMPUTACIÓN FORENSE: DESCUBRIENDO LOS RASTROS INFORMÁTICOS

Jeimy Cano

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

GOBIERNO DE LAS TECNOLOGÍAS Y LOS SISTEMAS DE INFORMACIÓN

M. Piattini y F. Hervada

2007, 489 Págs. **2-RAMA**

SECURITY, AUDIT AND CONTROL FEATURES ORACLE E-BUSINESS SUITE: A TECHNICAL AND RISK MANAGEMENT REFERENCE GUIDE

Japanese Edition. 2006, 368 pages. **ISOAJ**

SECURITY, AUDIT AND CONTROL FEATURES SAP R/3: A TECHNICAL AND RISK MANAGEMENT REFERENCE GUIDE

Japanese Edition. 2006, 255 pages. **ISAPJ**

INTERNET AND RELATED SECURITY TOPICS

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

24 DEADLY SINS OF SOFTWARE SECURITY: PROGRAMMING FLAWS AND HOW TO FIX THEM

NEW

Michael Howard, David LeBlanc and John Viega

Fully updated to cover the latest security issues, *24 Deadly Sins of Software Security* reveals the most common design and coding errors and explains how to fix each one—or better yet, avoid them from the start. This book has been completely revised to address the most recent vulnerabilities and has added five brand-new sins. This practical guide covers all platforms, languages and types of applications. Eliminate these security flaws from your code:

- SQL injection
- Use of magic URLs, predictable cookies and hidden form fields
- Format string problems
- C++ catastrophes
- Command injection
- Information leakage
- Poor usability
- Executing code with too much privilege
- Insecure mobile code
- Weak random numbers
- Failing to protect network traffic
- Trusting network name resolution

2009, 432 pages **19-M24**

CLOUD COMPUTING: IMPLEMENTATION, MANAGEMENT, AND SECURITY

John W. Rittinghouse and James F. Ransome

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

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

COMPUTER AND INFORMATION SECURITY HANDBOOK

John Vacca

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

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

HACKING EXPOSED COMPUTER FORENSICS SECRETS AND SOLUTIONS, 2ND EDITION
Aaron Philipp, David Cowen and Chris Davis

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

HACKING EXPOSED WIRELESS: WIRELESS SECURITY SECRETS & SOLUTIONS, 2ND EDITION
NEW
Johnny Cache, Joshua Wright, Vincent Liu

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

MOBILE APPLICATION SECURITY
NEW
Himanshu Dwivedi, Chris Clark, David Thiel

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

NETWORK SECURITY BIBLE, 2ND EDITION
Eric Cole

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

IT GOVERNANCE AND BUSINESS MANAGEMENT

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

THE BUSINESS MODEL FOR INFORMATION SECURITY
NEW
ISACA

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

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

ENTERPRISE INFORMATION SECURITY AND PRIVACY
C. Warren Axelrod, Jennifer Bayuk and Daniel Schutzer

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

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

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

HACKING EXPOSED MALWARE AND ROOTKITS: MALWARE & ROOTKITS SECRETS & SOLUTIONS
NEW
Michael A. Davis, Sean Bodmer, Aaron LeMasters

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

INFORMATION TECHNOLOGY GOVERNANCE AND SERVICE MANAGEMENT: FRAMEWORKS AND ADAPTATIONS
Aileen Cater-Steel

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

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

INTERNAL CONTROLS POLICIES AND PROCEDURES
Rose Hightower

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

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

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

IT FINANCIAL MANAGEMENT
Maxime Sottini

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

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

MONITORING INTERNAL CONTROL SYSTEMS AND IT
NEW
ISACA

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

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

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

OUTSOURCING IT: A GOVERNANCE GUIDE
NEW
Rupert Kendrick

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

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

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

TECHNOLOGY SCORECARDS: ALIGNING IT INVESTMENTS WITH BUSINESS PERFORMANCE
Sam Bansal

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

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

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

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

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

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

ISACA Bookstore Price List

2011 CISA® EXAM REFERENCE MATERIALS

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

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

2011 CISM® EXAM REFERENCE MATERIALS

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

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

2011 CGEIT EXAM REFERENCE MATERIALS

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

Code	Title	Nonmember	Member
CGM-11*	CGEIT Review Manual 2011	115.00	85.00
CGQ-11*	CGEIT Review Questions, Answers & Explanations Manual 2011 English Edition (50 Questions)	60.00	40.00
CACG*	Candidate's Guide to the CGEIT Exam and Certification 2011 (No charge to paid CGEIT exam registrants)	15.00	5.00

2011 CRISC EXAM REFERENCE MATERIALS

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

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

COBIT®

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

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

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

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

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

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

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

VAL IT™

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

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

ISACA Bookstore Price List

AUDIT, CONTROL AND SECURITY—ESSENTIALS

Code	Title	Nonmember	Member
1-IT8	Accounting Information Systems, 8th Edition	225.00	215.00
70-WAS	Accounting Information Systems: Controls and Processes	155.00	145.00
6-PAW	Applied Security Visualization	65.00	55.00
45-WAP	Audit Planning: A Risk-Based Approach	75.00	65.00
6-PL	Auditing IT Infrastructures	105.00	95.00
53-WAG	Auditor's Guide to Information Systems Auditing	108.00	98.00
7-EL	Biometric Technologies and Verification Systems	79.00	69.00
76-WSL	Build Your Own Security Lab: A Field Guide for Network Testing	60.00	50.00
43-CRC	Building an Effective Information Security Policy Architecture	90.00	80.00
31-CRC	Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI	135.00	125.00
79-WCAF	Computer Aided Fraud Prevention and Detection: A Step by Step Guide	70.00	60.00
4-IGI	Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions	110.00	100.00
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		
Enterprisewide Identity Management			
WIM*	E-book—PDF Format (purchase online only)	20.00	10.00
PIM*	Print Format	35.00	25.00
71-WCF	Essentials of Corporate Fraud	50.00	40.00
60-WESO	Essentials of Sarbanes-Oxley	45.00	35.00
82-WACL	Fraud Analysis Techniques Using ACL	210.00	200.00
62-WFC	Fraud Casebook: Lessons from the Bad Side of Business	80.00	70.00
10-EL	GFI Network Security and PCI Compliance Power Tools	73.00	63.00
68-WHF	Healthcare Fraud: Auditing and Detection Guide	80.00	70.00
36-CRC	How to Achieve 27001 Certification: An Example of Applied Compliance Management	94.00	84.00
2-W404	How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control, 3rd Edition	90.00	80.00
7-ART	Implementing the ISO/IEC 27001 Information Security Management System Standard	95.00	85.00
9-CRC	Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd Edition	94.00	84.00
28-CRC	Information Security: Design, Implementation, Measurement and Compliance	104.00	94.00
83-WIS	Information Storage and Management: Storing, Managing, and Protecting Digital Information	70.00	60.00
4-CRC3	Information Technology Control and Audit, 3rd Edition	100.00	90.00
35-CRC	Insider Computer Fraud: An In-depth Framework for Detecting and Defending Against Insider IT Attacks	94.00	84.00
STDPK*	IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals	20.00	15.00
WITAF*	ITAF: A Professional Practices Framework for IT Assurance e-book—PDF (purchase online only)	45.00	FREE
11-PL	IT Auditing: IT Governance	105.00	95.00
8-PL	IT Auditing: The Process	105.00	95.00
15-MIT	IT Auditing: Using Controls to Protect Information Assets	70.00	60.00
IT Control Objectives for Basel II			
WITCOB*	E-book—PDF Format (purchase online only)	35.00	FREE
ITCOB*	Print Format	50.00	20.00
PSOX*	IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition	40.00	20.00
9-SYN	The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments	80.00	70.00
5-ART	Outsourcing Information Security	103.00	93.00
7-SYN9	PCI Compliance, Second Edition	70.00	60.00
26-CRC	A Practical Guide to Security Assessments	94.00	84.00
1-RIA	Practical IT Auditing with current Supplement	400.00	390.00
69-WPS	Public Sector Auditing: Is IT Value for Money?	70.00	60.00
8-ART	Role Engineering for Enterprise Security Management	95.00	85.00
75-WSO	The Sarbanes-Oxley Section 404 Implementation Toolkit: Practice Aids for Managers and Auditors, 2nd Edition	95.00	85.00
1-IGI	Securing the Information Infrastructure	110.00	100.00
5-PSM	Security Metrics: Replacing Fear, Uncertainty, and Doubt	60.00	50.00
1-SCC	Spreadsheet Check and Control: 47 Key Practices to Detect and Prevent Errors	50.00	40.00
2-WG	Standard for Auditing Computer Applications	470.00	460.00
2-BAY*	Stepping Through the InfoSec Program	45.00	35.00
1-BAY*	Stepping Through the IS Audit, 2nd Edition	45.00	35.00

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

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

NON-ENGLISH RESOURCES

Code	Title	Nonmember	Member
3-RAMA	Auditoría de Tecnologías y Sistemas de Información	70.00	60.00

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

CISM Examination Reference Material
Study aids available in Japanese and Spanish for the June or December 2011 CISM exam—see page S1

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

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

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

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

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

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

INTERNET AND RELATED SECURITY TOPICS

Code	Title	Nonmember	Member
19-M24	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	60.00	50.00
7-MOA3	Anti-Hacker Toolkit, 3rd Edition	70.00	60.00
37-WAI	The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers	27.00	17.00
1-NBS	The Big Switch: Rewiring the World, from Edison to Google	27.00	17.00
45-CRC	Cloud Computing: Implementation, Management, and Security	90.00	80.00
10-MOC	The Complete Reference Network Security	73.00	63.00
9-EL	Computer and Information Security Handbook	130.00	120.00
Cybercrime: Incident Response and Digital Forensics			
WCC*	E-book—PDF Format (purchase online only)	45.00	25.00
PCC*	Print Format	55.00	40.00
1-CAP	Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 2nd Edition	47.00	37.00
34-CRC	Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition	84.00	74.00
4-MGH	Gray Hat Hacking, 2nd Edition	60.00	50.00
1-MHF	Hacking Exposed Computer Forensics Secrets and Solutions, 2nd Edition	60.00	50.00
2-MCG6	Hacking Exposed: Network Security Secrets & Solutions, 6th Edition	60.00	50.00
17-MHE2	Hacking Exposed Wireless: Wireless Security Secrets & Solutions, 2nd Edition	60.00	50.00
8-SYN	How to Cheat at Configuring Open Source Security Tools	60.00	50.00

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

ISACA Bookstore Price List

Code	Title	Nonmember	Member
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	74.00	64.00
1-GL	NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning	60.00	50.00
56-WPC	Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft	100.00	90.00
1-HA	Scrappy Information Security: The Easy Way to Keep the Cyber Wolves at Bay	30.00	20.00
30-CRC	Securing Converged IP Networks	90.00	80.00
1-OSM	Security Monitoring	55.00	45.00
6-EL	XSS Exploits—Cross Site Scripting Attacks and Defense	70.00	60.00

IT GOVERNANCE AND BUSINESS MANAGEMENT

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

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. 6 -10

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

the cloud is the answer. it's also the question.

The cloud has the potential to transform business by offering faster, cheaper, on demand access to services and resources. But it's also one of the great business questions. How much cloud? How to secure it? How to make it work with what I already have?

CA Technologies can help you answer those questions. We have solutions to plan, implement, and monitor cloud services as part of your existing infrastructure.

And as you move to the cloud, with our security solutions you can control users, their access and how they use information in the cloud. You'll know who accessed your cloud service. You'll know what they accessed. And you'll know how they used the information.

It's a level of security no one else can provide.

To find out more about how our cloud technologies can help you manage and secure the cloud, visit ca.com.

we can

ca technologies