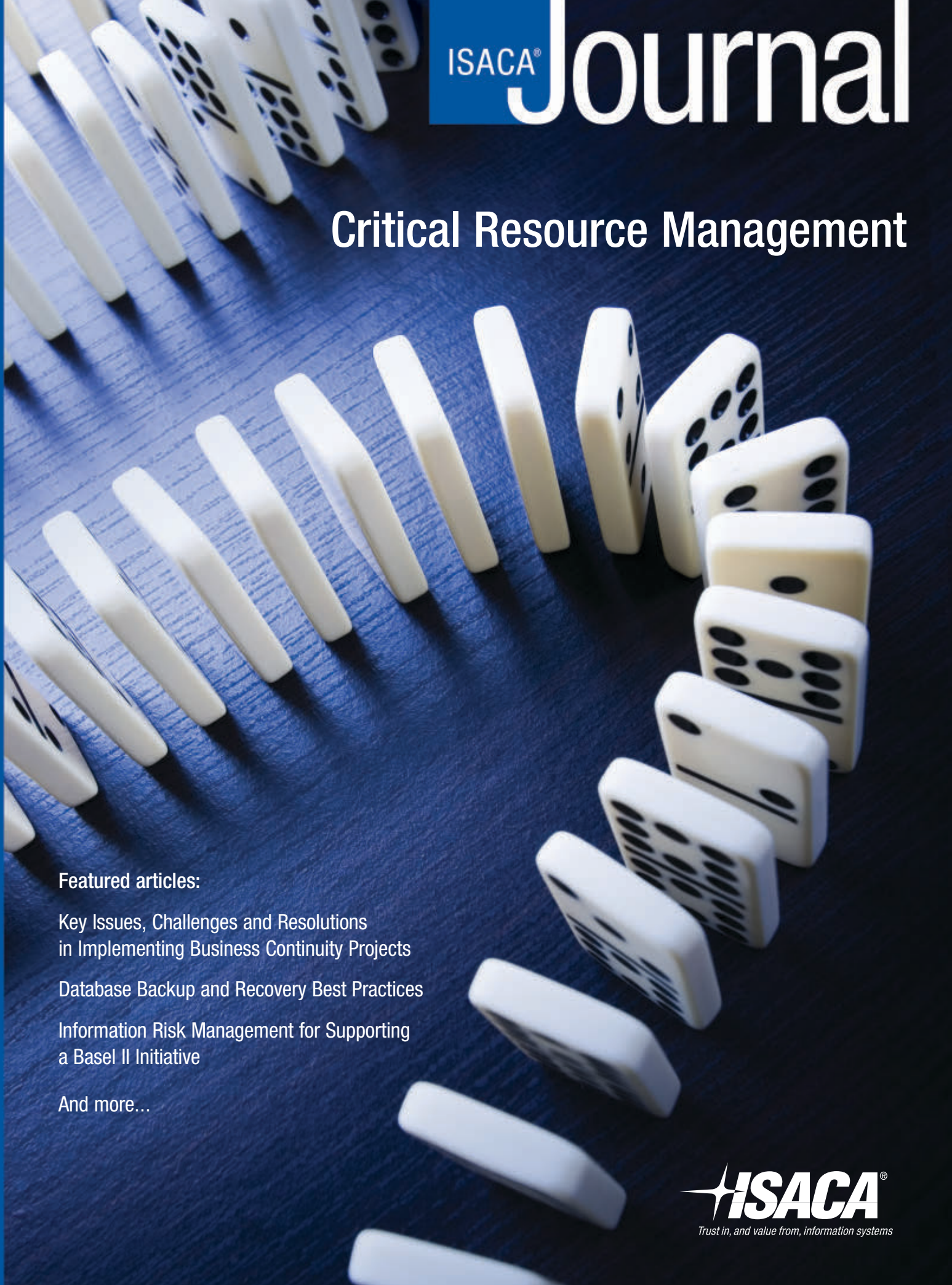
VOLUME 1, 2012

ISACA® Journal

Critical Resource Management



Featured articles:

Key Issues, Challenges and Resolutions in Implementing Business Continuity Projects

Database Backup and Recovery Best Practices

Information Risk Management for Supporting a Basel II Initiative

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

Key Performance Indicator.

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

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

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

Exam Date: 9 June 2012

Registration Deadline: 4 April 2012

www.isaca.org/certification-Journal

ISACA®
Trust in, and value from, information systems

KEEP YOUR CAREER ON TRACK

Regis University offers a Graduate Certificate as well as a Master's Degree in Information Assurance. With both programs, you have the option to take classes online or on-campus. Regis University is also designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency.

MASTER'S DEGREE

- Two year program
- Specialize in cybersecurity or policy management

GRADUATE CERTIFICATE

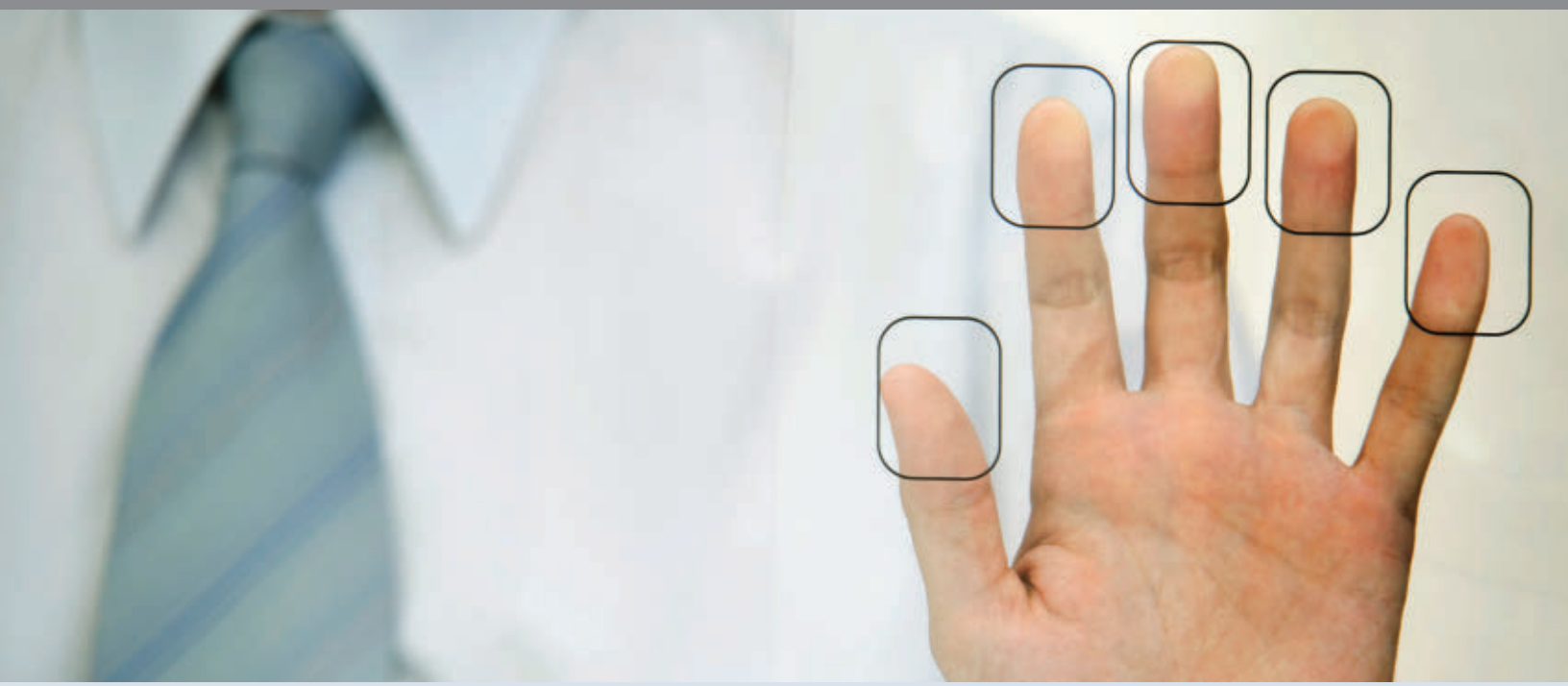
- Can be completed in less than a year
- Four classes (12 credit hours)

The curriculum is modeled on the guidelines and recommendations provided by:

- The Committee on National Security Systems (CNSS) 4000 training standards
- The (ISC)² Ten Domains of Knowledge
- ISACA

Our Information Assurance programs are grounded in security but also focus on delivering the essential combination of IT and business acumen — **creating a link between the server room and the boardroom.**

The program can be taken on campus or completely online



REGIS UNIVERSITY
School of Computer & Information Sciences

LEARN MORE

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

Volume 1, 2012

ISACA® Journal

Columns

Features

Plus

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

Journal Online

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

Online Features
The following articles will be available to ISACA members online on 1 February 2012.

Books Review: Cyber Attacks: Protecting National Infrastructure
Reviewed by Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS

Books Review: Information Security and Privacy
Reviewed by Horst Karin, Ph.D., CISA, CRISC, CISSP

Log Management: A Pragmatic Approach to PCI DSS
Prakhar Srivastava and Tarun Verma

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

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

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

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

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

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

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

No matter where you are on your career path, ISACA® equips you with the resources you need to enhance your skills, expand your professional knowledge and experience a vibrant local and global community of peers. Be sure to utilize all of the benefits offered through your ISACA membership.

Renew now!

If you aren't currently a member, visit ***www.isaca.org/join*** and join today!

ISACA®

Trust in, and value from, information systems

www.isaca.org/benefits-Journal

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

A Room With Machines

We are all rather focused on advanced technology. Cloud computing, virtualization, storage tiering, resilient network protocols, thin-client provisioning, deduplication and other arcana seem to be on everyone's lips. (Well, perhaps not everyone's, but these are frequently encountered terms in recent discussions among IT people, or at least those interested in IT infrastructure.) To the degree that most business information is still processed in a centralized manner, ones and zeroes are transformed and transmitted in rooms full of expensive, specialized machinery. For a few paragraphs, I would like to look down rather than up and consider the physical layer in a technology stack: the data center itself.

If there is to be any advanced technology, the data center and the machines in it need to be operated and maintained in a manner consistent with prudent business practices—management of risk and controls sufficient to marry them both. The first issue, therefore, is to determine the importance of a data center and its machines to the functioning of a business. Now, there may be some businesses whose data centers are of relatively minor importance. If so, I have not encountered one in several decades, so I will proceed with the assumption that, in a modern business enterprise, prudent management needs to have its data centers operating reliably and well. Just *how well* is a function of risk and, not surprising, money.

UPTIME INSTITUTE'S TIER RATINGS

There is a standard that establishes relative measures of "functionality, capacity and expected availability (or performance)" for data centers.[1] The Uptime Institute's *Data Center Site Infrastructure Tier Standard: Topology* defines four tiers of infrastructure reliability based on the redundancy of the resources needed to run a data center.

> *This standard is predicated on the fact that data centers are dependent on the successful and integrated operation of separate site infrastructure subsystems, the number of which is dependent upon the individual technologies (e.g., power generation, refrigeration, uninterruptible power systems, etc.) selected to sustain the operation.*[2]

In other words, the reliability of a data center is built upon its wiring, pipes, batteries, air conditioning, and all the elements characterized as mechanical, electrical and plumbing (MEP).

The least resilient data centers are Tier I and are characterized by nonredundant capacity components and a single distribution path for power and cooling to the equipment. Tier II data centers have redundancy; Tier III's have multiple redundant capacity components;[3] and Tier IV data centers, considered to be "fault-tolerant," have multiple, independent, physically isolated systems supporting computing equipment.[4] Put another way, nothing other than a Tier IV data center can be considered fault-tolerant, but there is a significant economic investment in achieving this rating. The difference between the reliability that has been built into a data center's physical infrastructure and what would be needed for a Tier IV rating is, in essence, the risk of downtime that management has decided to accept (or has accepted by default).

ELECTRICAL POWER

Computing equipment needs electricity. Power-draining equipment such as computers and storage need a lot of electricity. Older data centers built to house mainframe computers typically were provisioned for less than 50 kilowatts per square foot (kW/sq. ft.),[5] whereas modern data centers that are built for stand-alone and blade servers typically require more than 100 kW/sq. ft. and sometimes up to 200 kW/sq. ft.[6] Therefore, it is

important to consider the power supply to an older data center and whether it is sufficient for current usage.

For the electrical power to be considered redundant, there need to be two sources of electricity. One way—in my opinion, the ideal way—is to have two different lines from two separate utility substations enter the building housing the data center through two distinct entry points.[7] It may also be achieved by a single utility power supply and a backup generator as a second power source. However, to have a spare source of supply at all times, there need to be either two lines and a generator or one line and two generators, and true redundancy would call for two of each.

An uninterruptible power supply (UPS) is basically a large battery that takes a rather rough feed from a utility and converts it to a smoothly conditioned power. At the same time it ensures that if a utility fails, there is time to allow the supported equipment to fail softly and to switch over gracefully to generated power. Therefore, a UPS needs to be sufficiently large to run the equipment it supports, and since it is a part of the delivery system, there needs to be a second, redundant UPS to take over in case the first one fails.

COOLING

Computers and storage generate a lot of heat. Just as the kilowattage per square foot of older data centers may be insufficient, so the ability of an older data center to dissipate heat needs to be considered. A room whose floor is raised one foot above the plinth and whose dropped ceiling is 12 feet high will typically not draw off all the hot air around the equipment. (I have seen older data centers with their doors propped open and large fans pushing air into hallways. Believe me, this is not the way to run a data center.) The ceilings should be 18 feet high, with enough underfloor clearance (approximately three feet) for all the wiring that is needed for all the gear. Actually, a more modern approach is to use overhead racking for the wires, which may eliminate the need for raised flooring altogether. And, of course, large air conditioning units are *de rigueur*.[8]

In addition, much computing equipment needs internal cooling, which can be supplied by chilled water, cold air or a chemical refrigerant. Chillers are typically very large and heavy devices and are often placed on the roof of a building; there are also split or direct expansion systems with some of the cooling in the data center and the rest outdoors.[9] Thus, the cooling system needs piping into the data center and the equipment. As with electricity, there need to be redundant routes in which the coolant can circulate, two sets of pumps to get the coolant back to the chillers and redundant power to drive the pumps.

INFRASTRUCTURE ASSURANCE

Now, I am not an engineer or an architect, just a security geek and a data center rat, so the foregoing is all rather summary in nature. However, I have learned over the course of a lifetime and a career in IT that an organization overlooks the basics at its peril. As with any other aspect of security—which includes availability, of course—attention needs to be paid to the details of how management's objectives are met. The objective of reliability may be expressed in terms of the Uptime Institute's tiers or as the characteristics of the supportive infrastructure in a data center, of which power and cooling are but two. They are very complex subjects that require very specialized knowledge, not usually the domain of us security geeks…or of auditors, for that matter.

Security professionals and IT auditors are not usually called upon to investigate such specialized matters. They should, however, make sure that someone does carry out processes to give management assurance that the "low" technology of the MEP infrastructure is robust and reliable enough for all the "high" technology to take place.

ENDNOTES

[1] Uptime Institute Professional Services LLC, *Data Center Site Infrastructure Tier Standard: Topology*, Uptime Institute LLC, USA, 2009

[2] *Ibid.*, p. 1

[3] To be more specific, the standard calls for the applicable number of components plus a spare (n + 1) for both Tier II and Tier III.

[4] *Op cit,* Uptime Institute Professional Services., p. 1–3

[5] Neudorfer, Julius; "Data Center Cooling Optimization in the Virtualized-server World," *SearchDataCenter.com*, April 2008, *http://searchdatacenter.techtarget.com/tip/Data-center-cooling-optimization-in-the-virtualized-server-world*

[6] Mitchell, Robert L.; "Data Center Density Hits the Wall," *Computerworld*, 21 January 2010, *www.computerworld.com/s/article/9144466/Data_center_density_hits_the_wall*

[7] Of course, if the feeds are on the same grid, they are both subject to regional power outages, hence the need for generators.

[8] The correct term for these large air conditioning units is "computer room air conditioning" (CRAC—an industry acronym that I despise).

[9] Evans, Tony; *The Different Types of Air Conditioning Equipment for IT Environments*, American Power Conversion, USA, 2004, p. 4

Securing Cloud-based Applications

How Enterprise Single Sign-on Was Implemented to Drive Value

Michael Mendelsohn, CISSP, is the director of application security at CA Technologies and works in the global IT security department responsible for protecting against security threats.

Antoine Philipovitch is the senior specialist of IT security at CA Technologies and works in the global IT security department responsible for web application security.

William Welch, CISM, is the senior director of global IT security at CA Technologies.

Robert Zanella, CISA, is vice president of IT service management and compliance for CA Technologies and is responsible for service desk, compliance and continual service improvement activities within IT.

One of today's big security marketing pushes is enterprise single sign-on (ESSO). Many companies struggle with the stresses associated with forgotten passwords, lost productivity characterized by end-user frustration and high service-desk costs associated with resetting the numerous passwords of users. The ESSO solution primarily touts lower operational costs for enterprises and stronger enterprise security, but how does ESSO reduce the risk, especially when it comes to public cloud-based services? This article outlines how CA Technologies implemented ESSO to drive value.

CA Technologies has several cloud environments for which security is required, and ESSO was implemented to federate identities in the cloud. In this example, CA-SiteMinder was utilized, but there are numerous products in this space. In a summary-level example, when a user joins the organization, CA Technologies no longer has to worry about managing the namespace at the cloud-based application after implementing ESSO; instead, the internal identity store (such as Active Directory) is leveraged to authenticate the individuals. Nothing granular is done with SiteMinder to manage the access roles inside the cloud-based application. Instead, the enterprise is quickly able to provision/deprovision users to that application, at least from an authentication perspective, by leveraging its own identity store to provide timely security access.

ESSO TECHNOLOGY

In an ESSO implementation, the ESSO takes an authentication token processed on CA Technologies' internal system and sends it to the cloud. The cloud-based application will take the token and authenticate it through a "handshake," using Security Assertion Markup Language (SAML) as the protocol. A few years ago, security protocols were not standardized, but SAML has become more of an industry standard recently. Therefore, most of the ESSO products on the market are based on the SAML protocol.

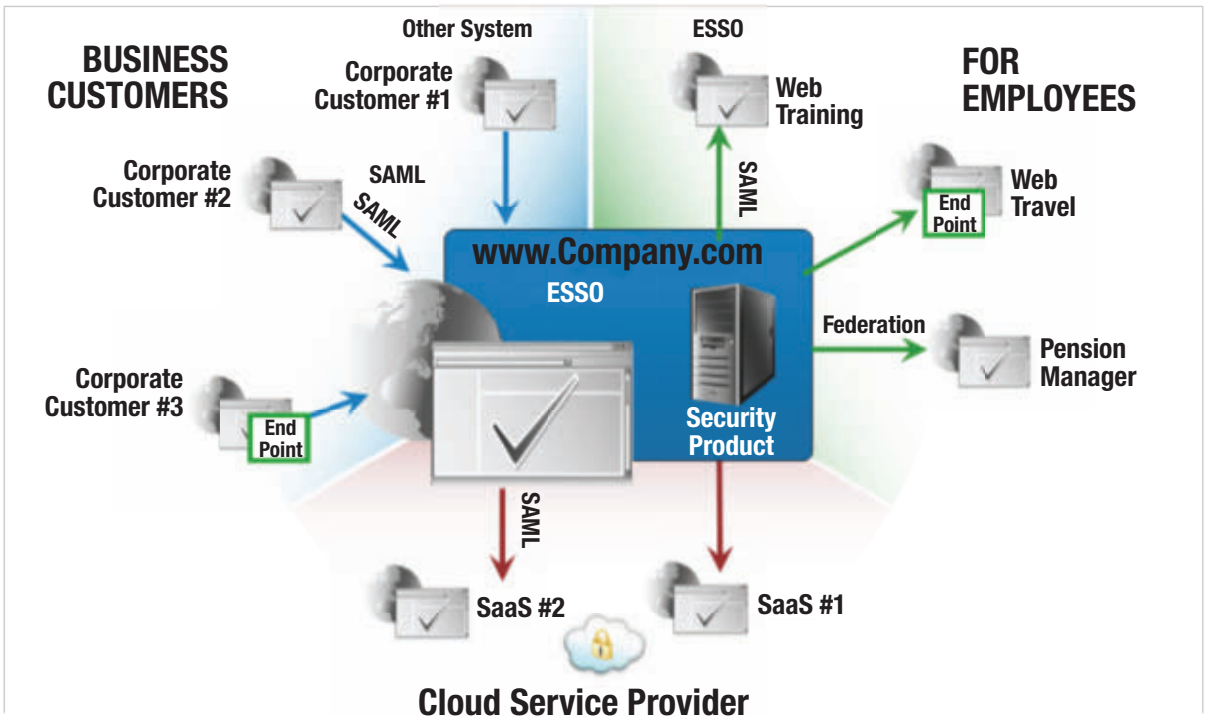
ESSO helps drive consistent levels of access and security across all applications. However, all of the following tools are needed to make secure access across environments work properly: identity management, provisioning and role management. ESSO is not about one technology; it is about how technologies work together.

HOW IT WORKS

Using ESSO federation with a cloud-based, publicly hosted Software as a Service (SaaS), the user gains access to the cloud-based application with a single click. If the user is not already logged onto the corporate network, the user is redirected to a login screen; however, if the user is on the corporate network, then the corporate credentials are sent to the ESSO federation site using SAML for automated login. The user information is constructed in an eXtensible Markup Language (XML) format, is secured and is sent to the service provider. The service provider checks the document to validate that the user exists and has permission to access the requested application (**figure 1**). No password is exchanged in the process since the user is already validated by the ESSO prior to getting access to the cloud-based application.

ESSO is not to be confused with identity management. ESSO is about authenticating, not about provisioning/deprovisioning. Only if the person is listed as active in the identity store will that person be authenticated. If a person is terminated, the transaction will not process. The enterprise is not provisioning/deprovisioning access to the application; ESSO will simply not allow access if the individual is not active in the corporate identity store. The business sees value in this because the security is strong and there is less management on the part of the business. By leveraging ESSO, it does not matter where

Figure 1—A Single Identification Across Multiple Environments Secured by ESSO



the application resides. It can be on-premise or off-premise, SaaS, Platform as a Service, or Infrastructure as a Service. The technology is the same regardless of the platform, and the end user has the same experience whether in the corporate office or coming in from the web/outside. The user goes to the application wherever it may reside. The authentication takes place using the user's domain credentials, which are passed to ESSO. ESSO validates the credentials and, in turn, passes a secure token to the application, which then grants access to the user. It is a seamless, simple method of gaining access to the application. In this example, the security model is location-agnostic; the application does not have to be on-premise or off-premise or cloud-based, legacy or hybrid.

IDENTIFICATION FEDERATION IN THE CLOUD

Cloud is part of the delivery of services to IT customers. Federation is the concept of having an application running internally within the enterprise and somewhere else in the cloud, but an enterprise may want them working together as if they are one application when presented to the end user. For example, suppose a portion of an enterprise resource planning (ERP) system is with a service provider (the majority being internally hosted). In this example, after entering the ERP system and clicking on "SRM" (for "Supplier Resource Management"), the user leaves the enterprise's system and goes to the service provider's. With federation, the user would not be redirected to the SaaS, but the screens would appear seamlessly from an identity perspective. ESSO needs federation to work between an external cloud and internal systems. Federation is a way to have the systems collaborate without having to integrate. The goal is to manage security and access to all core systems whether they are cloud, ERP, legacy applications or a combination.

REDUCING THE NEED FOR ADDITIONAL SIGN-ONS

ESSO provides convenience for end users so that they do not need to authenticate multiple times. It also provides security in the workplace by reducing the need for multiple sign-ons. Many ESSO users utilize multiple applications. When users have multiple applications to access, they tend to write down their passwords, stick them under their keyboards or post them on their monitors. ESSO helps eliminate those activities

by reducing the number of passwords that people need to remember, thus reducing the risk of compromising passwords. Without passwords, the risk of e-mail scams requesting usernames and passwords is substantially reduced.

An identity manager is the provisioning piece of the puzzle. Depending on the trigger, the identity manager (in this example, CA-Identity Manager was used) will provision the account to the application where ESSO picks up and authenticates access. There are several ways an identity manager can be triggered. Two examples include a human resources (HR) feed from an ERP system or from a role management tool (CA Technologies uses CA-RCM). The role management tool handles end-user requests for new roles. It seeks business-access-reviewer approval and, once approved, triggers the identity manager.

THE RISK

The biggest risk for ESSO is that the enterprise is putting all its eggs in one basket. If the solution is not architected with proper resiliency, an outage of the ESSO will have a profound effect: Access to *all* applications will be denied. Careful consideration needs to be given to the design of the solution. Significant redundancy, load balancing and monitoring *must* be in place to mitigate risk. This is a tough lesson to learn—better to learn it from this article than from real-life experience.

By introducing ESSO, an enterprise reduces the security risk around human error—provisioning improper access. With ESSO, one provision/deprovision can handle all applications for an individual as opposed to separately provisioning access to the multitude of applications to which a user typically needs access. When not properly planned, certain bulk upload functions such as deprovisions of groups can cause significant exposure if controls are not in place to ensure that the bulk change is completely accurate.

THE OUTCOMES AND VALUE OF APPLYING ESSO

From an end-user perspective, the biggest win from implementing ESSO is that the users do not have to manage more passwords. Although thrilled, they do not necessarily see the security value, but the enterprise does. Worrying about thousands of salespeople writing down passwords to key financial applications is no longer necessary. The big value is in IT: With a large workforce, even a small amount of turnover can represent a lot of manual effort to provision and deprovision access across multiple systems and environments. Now, through this integrated security solution, the enterprise is able to provision and deprovision access in a timelier manner, with greater accuracy and less effort. For example, when the HR department receives notice that someone is being terminated, the master employee/contractor file is updated by HR. The identity manager gets the feed periodically throughout the day, and when it sees a difference in the file, it updates the identity store. ESSO then uses the identity store for authentication, and if the person is no longer in the identity store, the user does not get authenticated. Because of the proliferation of cloud-based applications, business units are finding it easier to add cloud applications. With the low cost of cloud services, old procurement controls do not necessarily catch departments that procure these services. Once procured, departments wonder how they can manage access to the application for their people. ESSO makes it easier for IT to be responsive to the needs of these departments, despite the fact that, in these situations, IT was not included in the plan-and-analyze phase of the cloud project.

Evaluating Access Controls Over Data

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

Logical access controls have become a vital part of IT audit, both in IT reviews by internal auditors and by external auditors in the IT audit portion of a financial attest engagement. This focus is rational given the inherent risk associated with logical access controls to applications, data and systems in general.

This article offers some basic guidance to IT auditors in evaluating the access controls over relevant data files. In doing so, management may be able to gather ideas on how to better secure not only accounting data, but other data assets as well.

ACCESS METHODS TO DATA

The obvious method of access to data is via the applications that create, edit, maintain and report data; however, there are other methods through which one can get to data. They include the network operating system (NOS), primary server, database (and database administrator [DBA]) and operating system (OS). Each of these data-related components has its own risk and its own role in securing data.

Generally speaking, access to data is available through the "front door" and the "back door." "Front door" refers to access via legitimate applications and their functionality. That is, through normal activities of the application, users are able to gain access to data from many of the programs.

"Back door" refers to a different kind of access. Certain staff members or positions in IT, and possibly other functional areas, have the ability to access raw data by going around the application and accessing data files directly with some tool other than the application. These positions can include system administrator, server administrator, network administrator, DBA and OS administrator (some of these will likely overlap in small and medium-sized enterprises [SMEs]). These positions are at risk because they are able to gain unauthorized access rather easily, without adequate controls.

In addition, there is likely to be at least one person who has "keys to the kingdom." When the previously mentioned positions overlap and a single person performs all of those functions, when access rights are read-write (RW) universally, or when "root" access rights to servers are granted, that person has keys to the kingdom and is a high risk in terms of data security.

DATA STATES

Conventional wisdom identifies data as being in one of three states of being: at rest, in transit or in process. "At rest" refers to data storage when data are simply located on a storage device with no current activity related to those data. "In transit" refers to data that are being transmitted across some communication lines, such as the data's own network or the Internet. "In process" refers to data that are being created, modified or otherwise managed via applications. Each of the states is affected by one or more methods (**figure 1**).

Figure 1—Data States and Methods: Access Risk

Method	State		
	At Rest	In Transit	In Process
Applications		☑	☑
Network/NOS		☑	☑
Server		☑	☑
Database Management System (DBMS)	☑	☑	☑
DBA	☑		
OS	☑		☑

One common control for data at rest or in transit is encryption. For instance, for credit card data that are stored on a server connected to the Internet, the data file should be encrypted in all states. Protocols and secured connectivity are also important for data in transit, especially over the Internet. Tools such as Secure Sockets Layer and virtual private networks provide mitigating controls for the security of data in transit.

Data that are in process need controls in the application to help protect their integrity. The perimeter, NOS, server, OS and DBMS all provide means to increase or decrease the risk associated with data security. The following discussion provides some procedures to assess the level of risk for a particular entity at a particular time.

IT AUDIT IMPLICATIONS FOR DATA SECURITY

The IT auditor needs to assess the risk associated with each of the venues as it relates to the particular audit objectives. In order to properly audit the security of data, IT auditors will need to consider people, processes, IT, control—including access controls—*and* the state of the data. Therefore, assuming the constraint of access controls, the following sections present an illustrative description of the types of procedures the IT auditor should consider.

General Rules for Access Control/Passwords

Logical access controls related to login credentials, and especially passwords, overlap several of the components and methods related to data security. Therefore, the password principles that follow are used repeatedly in the procedures described in further sections. Passwords are considered more reliable if they follow these guidelines.

The first guideline relates to the ease of guessing or hacking passwords based on their length. The shorter the length of a password, the easier the password is to guess and the less time it takes for a hacker to crack a password with hacker tools. The general consensus is that a password should have a minimum of eight characters in order to be protected from being cracked and to protect unauthorized access to data assets.

The second guideline is a related one—the strength of the password. "Strength" means the complexity of the characters used to create a password; passwords should not be words in the dictionary, easy-to-guess names or only lowercase letters of the alphabet. To increase the strength of the password, a mix of lowercase letters, uppercase letters, numbers (at least one) and special characters (at least one) introduce a sufficient level of complexity to cause that password to become fairly difficult to guess or hack.

The third guideline aims to prevent unauthorized access via "piggy-backing," in which an authorized user walks away from a workstation without logging off and a fellow employee uses that system to conduct unauthorized activities. Because the authorized user is logged on, the coworker is able to gain unauthorized access to the system and potentially some access to the underlying data in the DBMS. To prevent this kind of unauthorized access, reliable systems provide for automatic logoff of sensitive accounts after some amount of time of inactivity by the user (also referred to as a "timeout"). The IT auditor should verify that an auto logout is in place for users who have access to sensitive data.

The fourth guideline deals with the response of the access control system to a failed login attempt. That is, when someone inputs login credentials that are incorrect, how does the system respond to that attempt? Best principles designate that the system should lock out the account after three successive failed attempts—the assumption being that there may be a malicious attempt to hack or guess the password.

The fifth guideline is associated with the duration of lockouts. Systems usually allow a system administrator to set the length of time before allowing anyone another attempt to log in once a user has been locked out. That should be something other than zero; 60–90 minutes will probably successfully frustrate hacker attempts. It could also be indefinite for more sensitive accounts/access, forcing a user who forgets login credentials to reestablish credentials.

The sixth access control principle involves terminated employees. For whatever reason, many entities fail to remove the login credentials of terminated employees. There should be sound policies and procedures to ensure that the credentials of terminated employees are removed in a timely

manner. The IT auditor should conduct procedures to ensure that terminated employees' credentials are removed or disabled; usually, a sample of terminated employees should be pulled and their credentials should be traced in the system to determine whether access was removed and, if so, when.

The last guideline states that there should be some segregation of duties (SoD) for the person responsible for password policies, settings and configuration to not perform incompatible duties, tasks and functions (e.g., entering data, having access to applications). For instance, monitoring changes to the password policies and files, along with proper altering tools to show elevation of access privilege changes, should be completed by someone other than the administrator who makes the changes.

Reviewing password policies and procedures is not always easy. Often, the OS will provide a way to at least view them; however, that may require a cumbersome set of screenshots to document them. The password policy strength can be tested by creating a password with weak strength to see if the system recognizes the password as weak and in opposition with policy, enforcing strong passwords. There are some freeware tools that generally make it fairly easy to print and/or view those internal password policies, settings and configurations.[1]

Applications

The procedures for applications involve logical access controls. Because the applications that are RW give the user access to the underlying data, those applications should be restricted to users who need the ability to read and write. Put another way, not all users should have access to all applications, especially those with RW capability. Some applications provide their own access controls. The IT auditor needs to gain an understanding of the application and whether it has its own access controls and, if so, if they are independent of or subservient to the network. That is, the application may inherit user access rights from the network (e.g., Microsoft Dynamics can inherit users, groups and access rights from Active Directory in Microsoft SQL Server). The objective is to restrict access to those applications, regardless of how the application assigns the access rights.

Server and NOS

The server and NOS have multiple risk factors related to data security. First, there are access rights that are established for users and administrators. The password principles outlined previously apply to the server.

In addition to logical security, "shares" should be examined. The share function allows folders and files to be shared with various users or groups. The key is to prohibit the sharing of critical data except to a few authorized users or one group. For instance, if a spreadsheet is used in the financial reporting process (which is often the case), that file should not be shared with users other than the person authorized to use it, the person authorized to review it, etc. In fact, restricting the file/folder is one way to mitigate the risk associated with using a spreadsheet. In general, shared permissions for data access should be used sparingly and judiciously.

The next risk is that of the users who and groups that have access to the server. Those users and groups should be established in such a way as to minimize access rights, using restricted rights for each user and each group. One good policy is to establish group rights and then add users to the appropriate group, limiting the number of individual users who have specific access rights—usually unique rights. Thus, the IT auditor should review the access rights file to see who has access and what kind of access. Usually, the OS will provide a tool to view that information. Terminated employees should be tested as well.

Sometimes, the server vendor will ask for access to the server to maintain, debug and solve problems that occur. These accounts must be guarded carefully. Auditors should ensure that any access is read-only (RO) and should even consider setting up a temporary vendor account when needed, which can be removed or disabled until it is needed again.

Servers come with default settings for users and groups, and sometimes, those accounts are not established in a secure manner. For instance, sometimes, access is granted to "everyone." Sometimes, the administrator credentials are "admin" (username) and "admin" (password) and, thus, easy to guess. Likewise, the database system administrator default is sometimes "sa" and "sa," which is also easy to guess. Therefore, at first use, any default accounts should be examined and changes made where appropriate. The IT auditor should look for these default accounts to ensure that they have been "sanitized."[2]

The IT auditor should test the process of adding, removing and modifying users and groups in regard to access rights. For instance, the add process should be tested to see whether it picks up the password policies correctly. The removing process should be tested to ensure that access is truly removed. The IT auditor should gather evidence of any breach, violation or abuse of password policies and procedures—and internal password policy settings/configuration. Any intrusions from outside of the system should also be determined and evaluated.

Firewalls

Firewalls can allow or disallow access to external users, and can lead to unauthorized access to data. Therefore, the firewall should be tested for appropriate access controls for users who enter the system externally.

Here, too, the default settings from the manufacturer can be troublesome. The default setting for access should be to deny the credentials "any" and "any," which forces the system to verify each external user against some access rights established for users and groups.

Change controls and updates/patches are risk factors that can lead to data being susceptible to misuse, theft or unauthorized access. Therefore, the IT auditor should test change controls and update/patch controls to ensure that the firewall is being properly managed to mitigate the risk of unauthorized access. SoD applies in the same way here as it does for passwords.

OS and Network Administrators

OS and network administrators, by the nature of their functions, have back-door access to data. Thus, when IT auditors examine password policies and review users and groups, the IT auditors should see a limited number of people with OS or network server administrator rights. That is, a firm with 10 staff members in the IT department does not need all 10 to have OS administrator, server administrator or network administrator rights. In SMEs, two or three people are probably sufficient to manage and perform the administrator functions. Thus, the IT auditor should see a reasonably limited number of administrators. Also, the rights granted need to be least-privilege access.[3]

DBA

In the same manner as administrators, the DBA has an unusual amount of risk related to the data. Unlike OS, server and network administrators, the DBA knows more about the data, data structures and data files than anyone else in the entity. Therefore, the DBA is not only able to access data via the back door, he/she can also conduct any number of malicious or deleterious activities related to the data and potentially hide that unauthorized activity for a long time—after all, this person is the oversight and manager of the DBMS.

Also in the same manner as administrators, the DBA should have rights assigned at the least-privilege level. The DBA should also be segregated from all other IT- and data-related functions. On the organizational chart, the DBA should appear similar to an island, with no connection to other functions and no oversight of the people who do them. Also in the same manner as administrators, there should be a reasonably limited number of DBAs. Obviously, the more DBMSs that exist, the more DBAs are needed, but for any one DBMS, the number should be limited to just a few.

In addition, the DBMS often comes with default users, and sometimes, the access granted to these accounts is too broad or risky. The IT auditor should look for those accounts and ensure that they have been changed or removed, if necessary, for data security.

SAMPLE IT AUDIT PROCEDURES FOR DATA SECURITY

The previously mentioned guidelines provide a benchmark for the procedures and for evaluation of evidence in IT audit procedures that are related to passwords and access control. The venues and possible procedures and IT audit objectives are compiled in **figure 2**.

CONCLUSION

Data security has become a vital need for almost all entities due to the expansion of data stored, technical standards and increased malicious activities. There are some basic principles for auditing data security, including auditing password policy, administrative rights and other aspects of logical access. While logical access is not the only IT audit procedure for data security, it is generally considered a key one, and a basic one applied to audits and reviews of all types. This article provides some basic IT audit procedures for security over data, including logical access over the front door (e.g., applications) and the back door (e.g., DBAs, administrators), and access to the database in general.

ACKNOWLEDGEMENT

A special thanks to my colleague at Carr Riggs & Ingram, David Mills, for his invaluable input into this article and for his encouragement.

Figure 2—Sample IT Audit Procedures for Data Security	
Method	**Sample Procedures**
Passwords	• Print or view password policies established on the network, server, applications and/or OS, and review to ensure that users and groups are adhering to the password guidelines mentioned previously. • Pull a sample of terminated employees, and trace removal of access rights. • Verify proper SoD for the password administrator. • Ensure the existence of independent review of password changes. • Obtain evidence of any known failures, breaches, intrusions or abuses. • Determine who monitors the changes and who manages/administers the changes. • Determine appropriate SoD for those individuals who are associated with password management.
Applications	• Determine and verify logical access controls (restricted access)—independent, inherited or absent. • Verify the use of password procedures (as outlined previously).
Server	• Verify the enforcement of logical access controls (least-privilege access). • Verify the use of password procedures (as outlined previously). • Verify that there is limited permission on shares, especially of sensitive data files. • Verify the use of standard principles for establishing access to users and groups. • Verify that vendor accounts are evaluated. • Determine whether default settings and accounts have been changed or removed, if necessary. • Verify that there is a limited number of administrators.
Firewalls	• Verify the enforcement of appropriate access controls to limit external user access. • Determine whether default settings have been changed. • Test patches and updates. • Test change controls. • Verify that is a limited number of administrators.
OS	• Verify the enforcement of logical access controls (least-privilege access). • Verify the use of password procedures (as outlined previously). • Verify that there is a limited number of administrators.
Network/NOS	• Verify the enforcement of logical access controls (least-privilege access). • Verify the use of password procedures (as outlined previously). • Verify that there is a limited number of administrators.
DBMS	• Determine whether default user accounts have been changed or removed, if necessary. • Verify the use of password procedures (as outlined previously).
DBA	• Verify the enforcement of least-privilege access. • Verify proper SoD. • Verify that there is a limited number of DBAs.

ENDNOTES

[1] One such tool is DumpSec, which can gather password access rights and policies and "dump" them to a printout or screen. See *SystemTools.com*, SomarSoft Utilities, *www.systemtools.com/somarsoft/?somarsoft.com*. Another tool is Netwrix, which can examine lockouts, password configurations/settings, changes to passwords and more. It works on a number of servers such as Active Directory, SQL Server and Microsoft Exchange. See Netwrix Corp., USA, 2011, *www.netwrix.com.*

[2] The exact default accounts depend on the server, but usually the IT auditor should be able to determine the pertinent information by doing a web search for the server manufacturer and model and "default accounts."

[3] US Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, USA, 1985, affectionately known as the "orange book," is a commonly accepted standard for computer and data security. It defines "least privilege" as "a principle that requires each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks."

Database Backup and Recovery Best Practices

Ali Navid Akhtar, OCP, has more than two decades of experience with databases. He works as a lead database administrator at Solo Cup Co.

Jeff Buchholtz has more than 18 years of design, implementation and support of global IT technology solutions. He works in an IT leadership role and is an Oracle database administrator.

Michael Ryan, CIA, CPA, is the director of internal audit for Solo Cup Co., with the primary responsibility of building and executing US Sarbanes-Oxley Act 404 compliance strategies.

Kumar Setty, CISA, has more than 10 years of experience in the areas of data analysis, systems administration, auditing and computer security. He is a manager at PricewaterhouseCoopers LLP.

The ability to restore databases from valid backups is a vital part of ensuring business continuity. Backup integrity and restorations are an important piece of the IT Governance Institute's *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*. In many instances, IT auditors merely confirm whether backups are being performed either to disk or to tape, without considering the integrity or viability of the backup media.

This article covers the topics related to data loss and the types of database backup and recovery available. Best practices that can assist an auditor in assessing the effectiveness of database backup and recovery are also provided. This article focuses on the technologies and capabilities of the Oracle relational database management system (RDBMS) and Microsoft (MS) SQL Server because, together, they cover approximately 40 percent of all database installations. **Figure 1** provides a short comparison of Oracle and MS SQL Server.

One of the key responsibilities of a database administrator (DBA) is to prepare for the possibility of media, hardware and software failure as well as to recover databases during a disaster. Should any of these failures occur, the major objective is to ensure that the database is available to users within an acceptable time period, while ensuring that there is no loss of data. DBAs should evaluate their preparedness to respond effectively to such situations by answering the following questions:

- How confident is the DBA that the data on which the company business depends are backed up successfully and that the data can be recovered from these backups within the permissible time limits, per a service level agreement (SLA) or recovery time objective, as specified in the organization's disaster recovery plan?
- Has the DBA taken measures to draft and test the procedures to protect as well as recover the databases from numerous types of failures?

The following is a checklist for database backup and recovery procedures that are explained throughout this article:

1. Develop a comprehensive backup plan.
2. Perform effective backup management.
3. Perform periodic databases restore testing.
4. Have backup and recovery SLAs drafted and communicated to all stakeholders.
5. Have the disaster recovery plan (DRP) database portion drafted and documented.
6. Keep your knowledge and know-how on database and OS backup and recovery tools up to date.

COMPREHENSIVE BACKUP PLAN

DBAs are responsible for making a comprehensive backup plan for databases for which they are accountable. The backup plan should include all types of RDBMSs within the enterprise and should cover the following areas:

- **Decide what needs to be backed up.** It is imperative that the DBA be aware of database and related OS and application components that need to be backed up, whether via an online backup or an offline cold backup. The following are details of what needs to be backed up:
  - OS software—An event such as a hardware failure will require a complete system restore, starting with the OS, so there is a need to back up the database server OS initially and after any system updates or configuration changes.
  - RDBMS software—The RDBMS software should be backed up initially and after any patches/upgrades.
  - Application software where applicable—This applies especially to Oracle E-Business Suite, Oracle Application Server and Oracle Enterprise Manager (OEM). The application DBA should complete an initial full backup of the applications to disk using an appropriate OS command and, then, schedule future incremental backups, e.g., after any patches/upgrades. These backups should also be transferred to tape.

Figure 1—Comparison of Oracle and MS SQL Server		
Item	**Oracle RDBMS**	**MS SQL Server RDBMS**
General	In Oracle, a database when started refers to the entire Oracle RDBMS environment, including memory structures and background processes called Oracle instance and control files, datafiles, online redo logs and some other files, such as the parameter or server parameter file and the password file.	An instance of SQL Server when executed allocates memory pools, uses background processes, and has multiple databases including system and user databases. The master database is the main system database that contains the system catalog as well as some information about individual databases.
Catalogs	Each Oracle database runs on one centralized system catalog, or data dictionary, which resides in the SYSTEM tablespace.	In SQL Server, the system catalog, which is analogous to the Oracle data dictionary, is broken up among the individual databases, the master database, and the (hidden and read-only) resource database (found in later versions).
Storage structures	The Oracle RDBMS is comprised of logical structures called tablespaces, which, in turn, are comprised of physical datafiles. Tablespaces/datafiles are formatted into internal units, called blocks. An Oracle extent contains a chain of contiguous blocks and varies in size.	SQL Server uses filegroups, which are logical containers of one or more files. Data contained within a filegroup is proportionally filled across all files belonging to the filegroup. SQL Server formats files into internal units called pages, which are organized into extents that are fixed in size.
Logins	Oracle provides logins for authorized users to connect to the database, which are referred to as the user or username, and any operation the user can perform is controlled by the privileges granted to the login.	In SQL Server, the login enables a user to connect to an instance. However, access to other databases within the instance is not automatic and is controlled by additional accounts (called users) that are created in each of the databases to which the login requires access. The privileges at the instance level are assigned to the login, and privileges inside a database are given to the related database user. A database user is mapped back to an instance login.
Authentication	Authentication is the process of verifying that the login ID or username supplied by a user to connect to the database belongs to an authorized user. Oracle allows authentication through the OS or through the database (server).	SQL Server also allows authentication through the OS or through the database (server). In SQL Server, the OS mode is called Windows Authentication, and the database mode is called SQL Server Authentication.
Logging mode	Online redo logs are used by Oracle to record transactional changes made to the database before those changes are committed to the database files. Oracle also uses rollback or undo segments to capture an image of data before they are changed to facilitate transaction rollback, recovery and read consistency.	In SQL Server, the redo logs are called transaction logs. A transaction log combines the functionality of Oracle redo logs and the rollback or undo segments. Each database in SQL Server has one or more transaction log files.
Automatic recovery	Oracle performs automatic recovery each time it is started. It verifies that the contents of the datafiles are coordinated with the contents of the online redo log files. If they are not, Oracle applies the contents of the online redo log files to the datafiles, and then removes any uncommitted transactions that are found in the rollback or undo segments. If Oracle cannot obtain the information it requires from the online redo log files, it consults the archived redo log files.	SQL Server also performs automatic data recovery by checking each database in the system each time it is started. It first checks the master database, and then launches threads to recover all of the other databases in the system. For each SQL Server database, the automatic recovery mechanism checks the transaction log for any committed and uncommitted transactions and applies these to the database. Each database has its own transaction log, which records all changes to the database.
Backup and recovery	In Oracle, backup methods can be categorized as physical and logical. There are two ways to perform Oracle physical backup and recovery: Recovery Manager (RMAN) and user-managed backup and recovery. Oracle segments its backups by consistent and inconsistent states. These can also be viewed as cold or hot backups.	SQL Server offers full, differential, partial and transaction log backups, which aid in complete recovery of databases during disk, server or instance failure. There are a variety of hot and cold backups available in SQL Server to suit any business environment. SQL Server databases can also be quickly detached and the files copied, and then they can be attached to another instance.
Logical backups	The goal of a logical backup is to be able to recover at the individual schema object level. In Oracle, logical backups are mainly performed using the Export or Data Pump utility. This utility exports the schema objects into a binary file, which can be read only by the Import or Data Pump utility, and imports the schema objects into a database.	In SQL Server, individual schema objects can be backed up to flat files in any of the supported file formats. Then flat files can be restored using tools such as the bulk copy program (bcp) utility, the Import and Export Wizard, or the SQL Server Integration Services tools.

– Passwords—All superuser passwords that may be required during recovery should be preserved. It is a good idea to ensure that the default passwords that came with the initial installation of the RDBMS are changed.
– All components of Oracle databases:
  · Database parameter file—A parameter file or server parameter file (SPFILE) defines persistent initialization parameters of a database, including information about database control files.
  · Database control file(s)—The control file stores the status of physical structure of the database. If it becomes unavailable, the database cannot operate. It is imperative that these files be backed up while backing up other components of the database. In later versions of Oracle (9i onward), the DBA can configure automatic backup of the parameter file as well as the control file to ensure that these get backed up after each backup and after any structural changes in the database.
  · Database data files—These should be backed up during cold backup as well as during online backup, using Oracle's Recovery Manager (RMAN) or, in Oracle Database versions in which RMAN was not introduced, by putting tablespaces in backup mode. The DBA should try to run all production databases in Archive log mode so that recovery to the point of failure is possible.
  · Redo log files and archived redo logs—While making a cold backup, the DBA needs to backup redo logs. When the database is running in archive log mode and doing and online backup, the DBA needs to archive redo logs manually or automatically and then back up all archive redo logs.
  · Oracle network files—It is important to back up all Oracle network files initially and after any change.
  · Password files—Password files when used should be backed up initially and after any change.
– MS SQL Server databases:
  · Back up both system and user databases.
  · Have a separate maintenance plan for system databases, i.e., master, model, msdb. Master supports only full backups; tempdb backup is not required, as it gets rebuilt during SQL Server startup.
  · Back up all user databases. Set up all user databases for full recovery model, and back up both database and transaction logs.

• **Determine the appropriate backup type to use for your data.**
– Oracle databases:
  1. Logical backups—This type of backup is performed through Oracle utilities "exp." From version 10g onward, Data Pump can also be used. The whole database, individual schemas, tables or tablespaces can be backed up. Restore is done using "imp" or Data Pump. With such backups, recovery to the point of failure is not possible.
  2. Physical offline or cold backups—The database must be shut down and a copy must be made of all essential data files and other components of the database.
  3. Physical online or hot backups—This method enables the database to be backed up while the database is up and running. The following points should be kept in mind while doing online backups:

- Either put the tablespaces in backup mode and back up the associated data files using an OS copy command, or use RMAN, a robust tool provided by Oracle for backup and recovery with version 8.x onward. Oracle adds new functionality to this tool with each version. RMAN can use the database control file to keep its catalog, or the DBA can setup schema for each database, in a separate database for RMAN catalogs.
- The DBA must review and keep in mind the RMAN compatibility matrix for the database being backed up/restored as well as the RMAN executable and RMAN Catalog Database/Schema.
- DBAs must familiarize themselves with full, incremental and differential backups and set these up using RMAN scripts. DBAs must review their RDBMS edition, e.g., incremental backups are not possible in standard editions prior to Oracle 10g. To restore/recover a database to the point of failure or a previous point in time, the DBA must put the database in archive log mode and back up all archived redo logs.
- It is important not to forget to back up the RMAN catalog at the end of each backup. DBAs can do an export backup of RMAN catalog schema.

– SQL Server databases:

1. Logical backups—In SQL Server, individual schema objects can be backed up to flat files in any of the supported file formats. Then flat files can be restored using tools such as the bcp utility, the Import and Export Wizard, or the SQL Server Integration Services tools.
2. Physical backups—It is recommended that all user databases be set up for full recovery model, and both database and transaction logs should be backed up to restore/recover the database to the point of failure. DBAs should thoroughly familiarize themselves with database recovery models and full, differential and transaction-log backups, and set these up accordingly. File or filegroup backup strategy can be used if the databases to be backed up are very large databases (VLDBs) that are partitioned among multiple files.

- **Establish a strategy for handling VLDB backups**—In Oracle, the DBA can reduce the backup window for VLDBs by allocating multiple channels and fine-tuning backups, can save disk space by using compressed backups, and can block tracking with incremental backup techniques with the latest versions. The DBA must review the version and edition of the database to confirm availability of this option. If this does not do the trick, the DBA can consider setting up split mirror backups. For SQL Server, the DBA can partition the database among multiple files and use the file or filegroup backup strategy. Also, using multiple backup devices in SQL Server allows backups to be written to all devices in parallel.
- **Establish an appropriate backup schedule and window**—It is good practice to select a backup window at a point when the lowest amount of activity affects the database so that the backup does not reduce available database server resources and slow down the database user's activity. The DBA can tune the backup window by parallelizing backups using multiple channels; however, the DBA must review the version and edition of the database to confirm availability of this option. In the vast majority of cases, it is best to set up a weekly backup cycle starting with full backups on Friday night or Saturday morning and incremental/differential backups throughout the weekdays. Archive/transaction log backups can be scheduled for every few hours, depending on the volatility of the database.
- **Decide where to store backups**—Both Oracle and MS SQL Server databases can be backed up directly to tape or disk (locally or over the network), and then the backups can be archived to tape. It is good practice to back up to disk, transfer to tape and store tapes offsite for disaster recovery (DR). The backups to disk are faster; DBAs have more control and can better monitor these and, with this method, DBAs hold two sets of backups—one on disk, the other on tape. During restore, if backups are still on disk, it will be a faster restore, reducing mean time to recover (MTTR).

- **Develop a backup retention policy**—The backup retention policy relates to both the disk and tape rotation schedule and should be decided upon based on the SLA established with the business-user community. The data owner should specify the retention period for the data. The retention period may vary from months to years, depending on local laws. Accordingly, the DBA should be deleting old backups to create space for current backups. The data retention policy should be chosen carefully, making sure that it complements the backup media subsystem retention policy and requirements for the backup recovery strategy. If not using a catalog, the DBA must ensure that the control file record keep time instance parameter matches the retention policy.

EFFECTIVE BACKUP MANAGEMENT

After making a solid backup plan and completing initial work, the DBA should properly manage backups, keeping the following points in mind:

- **Automating backups**—For Oracle, either set backups through OEM or use an OS scheduling tool, and Spool output to a log file that can be reviewed for any errors. In SQL Server, use Maintenance Plans for scheduling backups.
- **Monitoring backups**—Set up monitoring using appropriate tools so that the DBA gets an e-mail or alert through a pager or cell phone for any failed backups, which should be rerun as soon as possible.
- **Backup logs and catalogs**—Review backup logs and backup catalog information periodically for any issues. Use RMAN reporting to show backup status. For Oracle, back up the RMAN catalog database by exporting all catalog schemas periodically as well as by doing an export backup of RMAN catalog schema at the end of each backup. For SQL Server, backup system databases, especially master and msdb.
- **Database catalog maintenance**—With Oracle databases, use "delete obsolete" to remove backups that are outside the organization's retention policy. If obsolete backups are not deleted, the catalog will continue to grow and performance will become an issue. Cross-checking (cross-check backup) will check that the catalog/control file matches the physical backups.
- **Validating backups**—Validate and verify backups without doing actual restores.
- **Setting up dependencies**—When backing up to disk, archive these backups to tape as soon as backup to disk completes. Set up a process so that disk backups get transferred to tape without loss of time.

BACKUP RESTORATION TESTING

Imagine the following scenario: A flood has hit the area in which a company's headquarters resides, and the entire IT infrastructure has been damaged, but not destroyed. Before the event, the DBAs performed backups to the backup media, following all of the processes noted previously in this article, and had these stored offsite. In the enterprise's most recent IT audit, the auditor rated the backup process as "effective."

> "Backups are of no use if the IT team cannot restore the data to the system at the time of need."

The backup media from the offsite storage is retrieved and loaded. A message appears on-screen that states that the backup media are "unreadable" due to integrity issues. What could have happened?

Many things could have happened. However, it is clear that a critical step did *not* happen. The restoration from the backup media was never really tested. The control was marked as effective because a backup process was in place and being performed. In addition, no errors were ever received when the enterprise backed up to the backup media.

Backups are of no use if the IT team cannot restore the data to the system at the time of need. A DBA should formulate a detailed strategy for this task:

1. **Databases restore testing**—There should be a requirement to test database restores from disk as well as from tape backups.
2. **Validating restores where possible**—The DBA can validate and verify backups without doing actual restores. Validating backups using the "restore validate database" command will do everything except actually restore the database. This is the best method to determine if the backup is good and usable before being in a situation in which it becomes critical.
3. **Refreshing nonproduction databases from production backups**—It is good practice to periodically build nonproduction databases from production backups using appropriate backup/restore utility commands as a restore practice.
4. **Performing annual/biannual restore testing from tape as part of audit**—The DBA will have to explain the process

through a narrative, preserve logs and take screenshots to show this type of restore testing.

5. **Actual restores**—During actual restores, the DBA should back up the database before doing the restore. Depending on the type of loss and backups available, the DBA must decide on whether to go for complete (point-in-time) or incomplete recovery. Incomplete recovery can be time-based, cancel-based or change-based.
6. **Strategy to recover from database corruption**—For Oracle databases, the DBA can turn on block checking using appropriate parameters to detect the presence of corrupt blocks in the database. This has a slight performance overhead, but will allow early detection of corrupt blocks caused by underlying disk, storage system or input/output (I/O) system problems. By default, RMAN also checks for corrupt blocks during backup. In later versions of Oracle, RMAN can be used to repair corrupted blocks in the database.

BACKUP AND RECOVERY SLA

The DBA team must draft a backup and recovery SLA, covering details of backup procedures and including a timeline for recovery, and have management sign off on it. The SLA does not assist in the recovery process itself, but sets the user community's (and management's) expectations for the recovery process, which may provide the team more time to complete the restore process.

DISASTER RECOVERY PLAN

The DBA should take care to ensure that databases are included as a key element in the company's overall DRP. All stakeholders need to understand the elements of the recovery plan and in what order the IT team will restore the databases. The business must provide its input at this stage so that the most business-critical applications are available as soon as possible.

DATABASE AND OS BACKUP AND RECOVERY TOOLS

It seems obvious, but DBAs play the final and most important role in the process in that they must keep their knowledge of backup and recovery tools for RDBMSs up to date. During the actual restore event, DBAs will not have time to figure out any advancements in backup and recovery tools.

CONCLUSION

The primary responsibility of the database administration team is to review all types of RDBMSs in the enterprise and to develop a comprehensive backup plan to conduct effective backup management by proactively monitoring backups, getting alerted for failed backups and rerunning these seamlessly, without loss of time. It is good practice to back up data to physical disk and to then archive the data to tape for disaster recovery purposes.

Once an approach has been established, it is imperative to test data restoration periodically as part of the backup and restore strategy, and to review all options before executing the actual restoration/recovery. It is important to confirm that the DBA team is abreast of the latest backup and recovery tools and to ensure that the team has a clearly documented process in place with clear responsibilities. If DBAs maintain proper backups, monitor these proactively and can provide assurance of the recovery of data up to the point required by the business, they have done a major part of the job for which they were hired.

IT auditors can assist data administration teams in strengthening their controls and data recovery processes by validating the DBA operations, including the testing of the recovery of data. This continuous, proactive and cooperative effort between internal audit and the DBA team can provide assurance to management that, in the event of a disaster, the business's data can be recovered.

Key Issues, Challenges and Resolutions in Implementing Business Continuity Projects

Rama Lingeswara Satyanarayana Tammineedi, CISA, BCCE, CBCP, CISSP, PMP, has more than 24 years of IT experience in diverse business and technology organizations, which enables him to deliver client-focused services and value as an information security consultant. His experience spans all phases of the IT system life cycle (system analysis and design, development, software maintenance, testing, and implementation) and includes user training, documentation, quality assurance, internal quality auditing, project management and information security consultancy.

Business continuity management (BCM) is a holistic process to ensure uninterrupted availability of all key business resources required to support critical business activities, whether manual or IT-enabled, in the event of business disruption. Business continuity planning (BCP) involves planning and procedural aspects, encompassing emergency response, crisis communications, business continuity and disaster recovery. Disaster recovery planning (DRP) is the technical component of BCP and focuses on the continuity of information and communication technology systems that support business functions.[1]

BS 25999 *Business continuity management* establishes the process, principles and terminology of BCM and highlights the benefits and outcomes of an effective BCM program.[2] BCM goes beyond BCP and also covers management aspects such as policy, training and awareness, maintenance and exercise, and continuous improvement, as well as understanding the organization and embedding BCM into its culture. An effective BCM program protects the interests of the organization's stakeholders and reputation. The main BCM assets are the six organizational resources—people, premises, technology, information, supplies and stakeholders—for which continuity strategies may be required.

Successful execution of BCM projects results in robust BCM processes and organizational resilience. Adoption of an inappropriate approach and/or incorrect assumptions by BCM practitioners in the execution of a BCM project renders the outcome of the project—BCM documentation—unfit for use and results in a waste of scarce resources. This article describes key issues and challenges faced and observed by the author and his team during the execution of BCM projects, and suggests resolutions.

KEY ISSUES, CHALLENGES AND RESOLUTIONS

The key issues and challenges in implementing BCM projects revolve around four major areas:

1. Senior management commitment and involvement
2. Lack of thorough understanding of the data dynamics and dependencies involved in data recovery by BCM practitioners
3. Inappropriate approach in executing BCM processes
4. Incorrect and/or inappropriate assumptions in formulating business continuity and disaster recovery plans

COMMITMENT AND INVOLVEMENT

This section presents the key issues, challenges and resolutions related to senior management commitment and involvement in implementing a BCM project.

Delegation by Senior Management

In some organizations, the executive sponsor of the BCM project is too busy to oversee the project, and the responsibility is delegated to a mid-level manager. This reduces the visibility of the project at the organizational level and may also result in lack of serious cooperation from relevant departments/functions.

This challenge is resolved by setting up a cross-functional project steering committee that consists of key stakeholders. The committee should meet periodically (e.g., every one to two weeks) to resolve issues, if any, in project execution.

BCM Implementation for the Wrong Reasons

In some organizations, senior management tends to think that since a disaster has never been experienced, there is no business case for expending scarce resources. This often results in a lackadaisical attempt at implementing business continuity to satisfy only regulatory requirements or close audit observations.

This is addressed by undertaking a sustained BCM awareness campaign among key stakeholders, highlighting the benefits of achieving resilience from their perspective: meeting current and prospective customer demands and regulatory compliance, avoiding liability, and maintaining a competitive edge.

Business/IT Disconnect

Organizations in highly competitive industries are often compelled to respond dynamically to a competitor's offerings. Under pressure to reduce the time to market for newly conceived products and services, business managers sometimes do not give advance notice to the infrastructure team to address capacity issues.

This failure to align technological capability with business needs and growth projections often results in solution gaps, false expectations and performance issues that adversely affect organizational reputation. These issues can be avoided by systematic planning and collaboration between business and IT.

Technology-only Approach Toward Resilience

When planning for organizational resilience, some organizations focus more on technology and do not give equal importance to other organizational resources such as people, premises, data, processes and supplies.

This is addressed by creating appropriate awareness among stakeholders, identifying risks and single points of failure for organizational resources, recommending suitable risk mitigation measures to ensure the continuous availability of resources, and incorporating BCM processes into day-to-day operations.

Lack of Consensus Between Senior Management and Operations Management

Lack of consensus between senior management and operations management is prominent when conducting business impact analysis (BIA). BS 25999-1:2006 *Business continuity management—Code of practice* expects senior management to be actively involved in BIA.

In some organizations, senior management may prefer to understand the ground realities before committing any values for the maximum tolerable period of disruption (MTPOD) and recovery time objectives (RTOs) because it is aware of the financial implications of such decisions. In such cases, breaking the BIA into two parts makes sense. The first part of the BIA should be conducted with senior management to obtain MTPOD values for all services/products and respective functions that support the delivery of the services/products. The second part of the BIA has to be conducted with operational management in a more detailed way at the department level to identify department-specific MTPOD values and RTOs.

The department-specific MTPOD values given by senior management should be treated as preliminary values and need to be validated by the operational management of respective departments. Any difference in the MTPOD values of senior management and operational management need to be resolved by achieving consensus of opinion.

Absence of a Single BCM Framework Across Multiple Offices

The BCM framework followed across all offices may not be consistent for organizations that have multiple locations in multiple countries.[3] Consistency in approach and BCM documentation can be achieved by adopting an international BCM standard/framework across the enterprise.

LACK OF UNDERSTANDING

This section presents the key issues, challenges and resolutions related to a lack of thorough understanding of the data dynamics and dependencies involved in data recovery by BCM practitioners.

Incomplete Understanding of Data Recovery Requirements

Many organizations check only whether their core data are backed up and recoverable, and few consider the data dynamics and dependencies involved in data recovery.

These include:

- Are there any end-user computing systems outside enterprise backup? Some organizations depend on end-user computing resources such as department-developed scripts, spreadsheets and local databases to support *ad hoc* business requests that may be part of business-critical operations. These end-user computing resources need to be incorporated into the backup cycle to ensure that data backup is available for retrieval when required. Alternatively, the functionality provided by the end-user computing systems should be incorporated into the enterprise applications.
- Is there a need for synchronized recovery of lost data, backed-up data and data from any continuing business transactions during an outage?
- At what rate do unprocessed backlogs accumulate for continuing business transactions during an outage?
- How much of a backlog can be accumulated before local disk storage capacity is exceeded?
- Is there a means to pull data from remote transaction sources (e.g., automatic teller machines or points of sale) out of the normal processing windows and on a metered basis?
- What are the assumptions about the sudden spurt in data volumes that will hit the systems post recovery? Are there any capacity or processing time/speed issues that will impair the speed of data recovery or require metering to avoid overwhelming any applications that cannot cope with the volume? If so, are these factors considered in the estimation of total time to full recovery?

Failure to Consider Full Recovery

Most business continuity and disaster recovery plans address failover to a hot site or alternate site. Very few address the need to move operations back to a restored primary location, which can be as problematic as the failover itself.

INAPPROPRIATE APPROACH

This section presents the key issues, challenges and resolutions related to an inappropriate approach in executing BCM processes.

Location-based Risk Assessments

Tailoring a risk assessment to suit an organizational context is a challenge faced in some BCM projects. Conducting a buildingwide risk assessment may not always be sustainable. For example, some organizations may not have a single owner for a building (such as a data center) in which each team takes care of its own systems or common units/agencies may be provided by facilities management (e.g., physical security, cleaning, cooling, heating).

In such cases, adopting a service/product-based approach for risk assessment is more effective and sustainable. This approach is also in line with the BS 25999 requirement of evaluating threats to critical activities and activities that support the delivery of products/services within an organization. In this approach, each team conducts a risk assessment for its resources, including technology, data, people, processes, premises and supplies. A corporate team such as a BCM organization can coordinate the risk assessments; consolidate and analyze the results; and facilitate selection, approval and deployment of risk mitigation measures at the enterprise level.

Equal Weight Assigned to All Risk Attributes

Another challenge relating to risk assessment is the risk assessment approach itself. There are different methodologies to carry out a risk assessment. When the Failure Modes and Effects Analysis (FMEA) methodology is used for risk assessment, a risk priority number (RPN) is computed. RPN is the product of three attributes of risk—severity, likelihood and nondetectability—that are given equal weight. If the RPN is used alone to denote risk acceptance criteria, it may result in unnecessary investments for low-severity risks. To avoid this, another parameter, criticality—the product of severity and likelihood—is suggested.

Figure 1 illustrates three risk scenarios with the same RPN.

Figure 1—Three Risk Scenarios With the Same RPN

Risk No.	Severity	Likelihood	Nondetectability	RPN
1	1	5	5	25
2	5	1	5	25
3	5	5	1	25

The third risk in **figure 1** is more critical than the other two risks. When risks are prioritized for treatment, this risk should be given higher priority than the other risks that have equal RPN values. Therefore, the effective way to establish risk acceptance criteria is to use both RPN and criticality.

Inappropriate BIA Approach

BIA tools lead BCM practitioners to conduct analysis in silos by functional area, out of context of the impact of a disaster on the entire location. This kind of approach will ultimately skew all BIA findings to a higher availability and cost of strategies and solutions, and will lead to a significant and consistent failure of BIA efforts because the management of individual business functions will tend to overstate the importance of its function. However, if questioned correctly, management will give an entirely different answer about its relative importance in the context of a broader disaster impact. BIA has to be approached in the context of a sitewide disaster that affects all business functions at the site.

Challenge in the Deployment of a BCM Tool

Some organizations deploy a BCM tool to manage the BCM life cycle. Depending on the BCM tool and the version deployed, this may not be a challenge for enterprises. It is possible that the approach adopted by the BCM team when conducting certain activities (such as BIA and risk assessment) may not map exactly with the approach built into the tool. For example, during BIA, a business impact owing to an outage is determined for different durations. The durations used by the BCM team may be different from those used in the tool.

Knowledge of the tool and its workflows at the time of developing BCM documentation will help in avoiding rework during implementation of the BCM tool.

INCORRECT AND/OR INAPPROPRIATE ASSUMPTIONS

This section presents the key issues, challenges and resolutions related to incorrect and/or inappropriate assumptions in formulating business continuity and disaster recovery plans.

Failure to Consider All Relevant Assumptions and Limiting Factors

Many business continuity plans are built on assumptions that may not include all relevant assumptions and limiting factors. For example, many plans are predicated on an unstated assumption that only the organization in question will be impacted by a disaster. In reality, many disasters can be local or regional in nature and impact a number of organizations, businesses, infrastructures and transportation types. The competition for scarce resources, as well as travel limitations, can greatly impair recovery efforts.

Another typical assumption is that employees will go long distances to support operations at an alternate site. Local area or regional disasters, especially those that may result in injury and death, can make employees reluctant to go far from home.

Plans need to address an organization's expectations and the permissions or requirements it will communicate to its employees. A hard-line, help-the-enterprise approach will not be well received, but one that tells employees to first take care of themselves and their families during a disaster may garner more employee support. Business continuity planners should recognize and document relevant assumptions and factors that may limit recovery from a business disruption event and bring such assumptions and limiting factors to the attention of management.[4]

CONCLUSION

BCM is a business-owned and business-driven process and is a good corporate governance practice. However, there is no one-size-fits-all approach to implement BCM. BCM practitioners need to adapt relevant standards and best practices to suit their organizational cultures and requirements, which leads to certain challenges in implementing BCM projects. Resolving the relevant issues and challenges appropriately based on organizational context helps in establishing a sustainable BCM program and in enhancing an organization's BCM maturity.

ACKNOWLEDGEMENT

The author wishes to thank Brian V. Cummings for his review of and feedback on the article.

ENDNOTES

[1] For a discussion of the concepts of business continuity and ICT continuity and their relationship, please see Hamidovic, Haris; "An Introduction to ICT Continuity Based on BS 25777," *ISACA Journal*, vol. 2, 2011.

[2] For a detailed description of the process, principles and terminology of BCM and the benefits and outcomes of an effective BCM program, please see British Standards Institution, BS 25999-1:2006 *Business continuity management—Code of Practice*, UK, 2006.

[3] Please see International Organization for Standardization, ISO/IEC 27002:2005 *Information technology—Security techniques—Code of practice for information security management*, section 14.1.4 Business Continuity Framework, Switzerland, 2005.

[4] For a discussion of the factors that may limit recovery from a business disruption, please see Australian National Audit Office, *Better Practice Guide: Business Continuity Management—Building Resilience in Public Sector Entities*, Australia, 2009.

Feature

Effective IT Governance Through the Three Lines of Defense, Risk IT and COBIT

Ronke Oyemade, CISA, CRISC, PMP, is principal consultant and chief executive officer of Strategic Global Consulting LLC and has more than 14 years of consulting experience in industries such as oil and gas, health care, education, hospitality, data management, finance, telecommunications, retail, manufacturing, and insurance. Her areas of expertise include IT audit and security, software development, data analytics and mining, and US Federal Trade Commission and US Sarbanes-Oxley Act compliance. Oyemade has worked with firms such as Ernst & Young and Deloitte and is an experienced training instructor who has trained employees of Fortune 500 companies. She can be reached at *strategicglobalconsult@gmail.com.*

When the US Senate Banking Committee asked US Federal Reserve Chairman Ben S. Bernanke what lessons were learned from the current economic crisis, he replied, "The importance of being very aggressive and not being willing to allow banks, you know, too much leeway, particular when they're inadequate in areas such as risk management."[1]

Many financial institutions incurred large losses during the current, ongoing economic crisis with various external factors being held responsible for the losses; however, it was observed that despite this, there were a small number of banks that thrived during this period and actually prevented many losses. A close study of the latter banks revealed that they thrived because they benefited from a strong risk culture combined with a sharp focus on three effective lines of defense. This strong risk culture was found to be functioning ineffectively at the failing banks. The lines of defense and strong risk culture, combined with an effective governance structure, provide a stronger and more effective route for banks and other corporations to find their way out of this economic crisis and also to address the fundamental issues within their operations that resulted in the economic downturn.[2]

This article defines IT governance, addresses its importance, and describes how to apply the three lines of defense by implementing a combination of the Risk IT and COBIT® frameworks to produce a more effective IT governance framework to strengthen IT governance.

IMPORTANCE OF IT GOVERNANCE

IT is a powerful resource used by enterprises to achieve their most important objectives. For example, IT can represent a core driver of cost savings for large transactions such as mergers, acquisitions and divestitures; it can enable automation of key business processes such as the supply chain; and it can be the cornerstone of new business strategies or models. Even though IT has the potential for business transformation, it represents a very significant investment at the same time, typically from 1–8 percent of gross revenue. In some cases, the true cost is not clear, and budgets could spread across business units, functions and geographic locations with no overall oversight. This often ends up in failure to deliver expected outcomes and, therefore, results in a spectrum of IT-related risks such as the nonavailability of customer-facing business systems, disclosure of customer or proprietary data, or missed business opportunities due to an inflexible IT architecture. These and the complex regulatory environment faced by enterprises today have led to a significant focus on IT governance.[3]

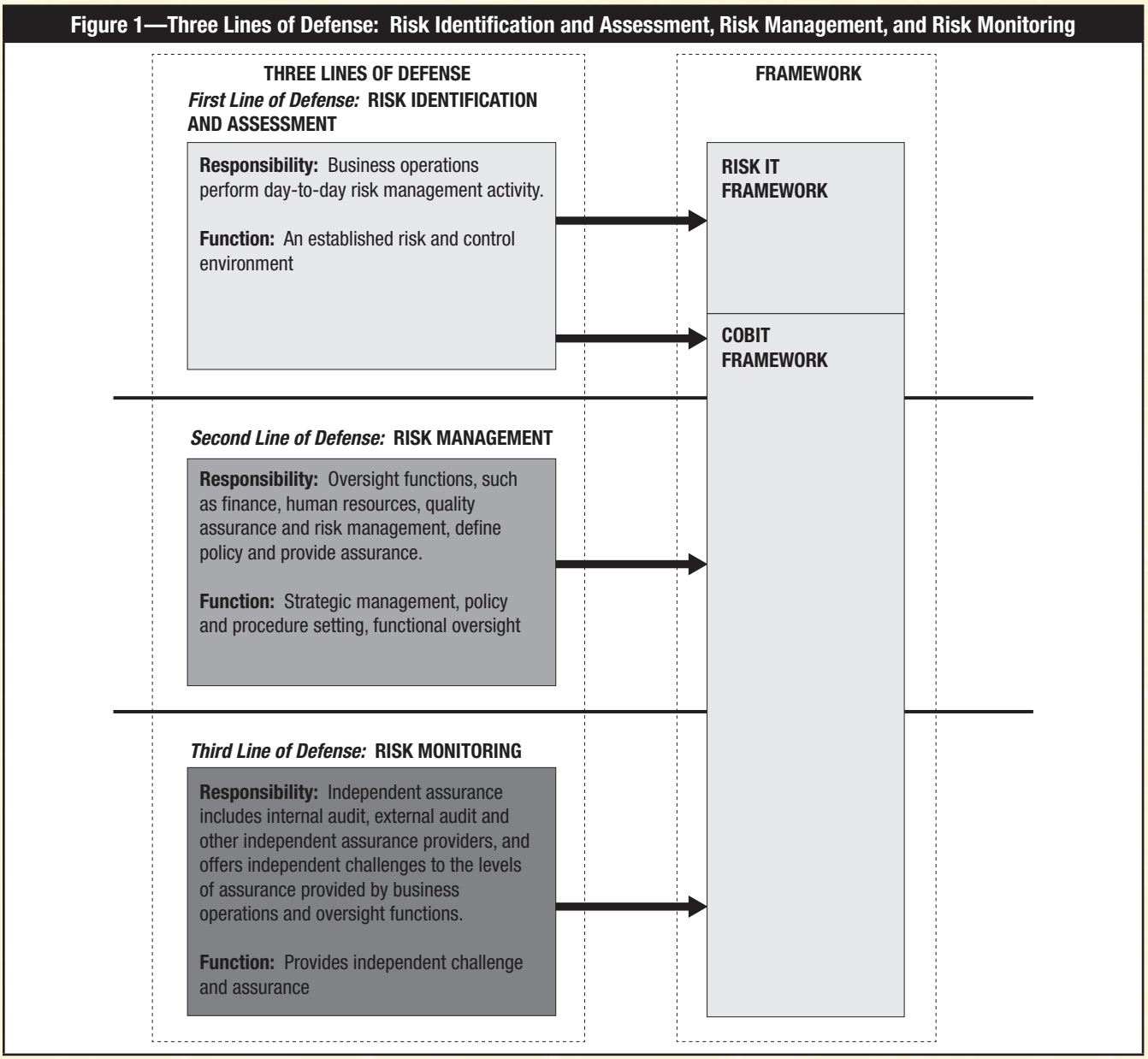
IT governance is an integral part of enterprise governance. While the need for governance at the enterprise level is driven primarily by demand for transparency across enterprise risks and protection of shareholder value, the significant costs, risks and opportunities associated with IT call for a dedicated, yet integrated, focus on IT governance. While the terms "enterprise governance" and "IT governance" may have different meanings to different individuals, they can be defined as follows:

> *Enterprise governance is the set of responsibilities and practices exercised by the board and executive management with the goals of providing strategic direction, ensuring the objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly, while IT governance is the responsibility of executives and boards 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.*[4]

APPLICATION OF THE THREE LINES OF DEFENSE MODEL

The three lines-of-defense model can be used as the primary means to demonstrate and structure roles, responsibilities and accountabilities for decision making, risk and control to achieve effective governance risk management and assurance.[5] This model is based on the resilient yet flexible compliance risk management framework that is comprised of three key elements: risk identification and assessment, risk management, and risk monitoring. As shown in **figure 1**, to successfully implement this model, two frameworks—Risk IT and COBIT—can be adopted. Risk IT sets good practices by providing a framework for enterprises to identify, govern and manage IT risks, while COBIT sets good practices for the means of risk management by providing a set of controls to mitigate IT risk.[6]

Figure 1—Three Lines of Defense: Risk Identification and Assessment, Risk Management, and Risk Monitoring



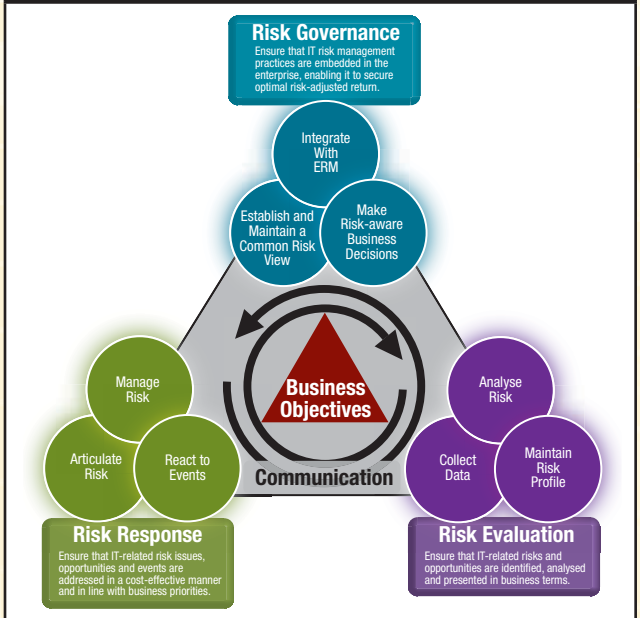
The first line of defense entails the identification and assessment of IT risk, providing risk responses, defining and implementing controls to mitigate key IT risks, and reporting on progress. This means identifying threats to the enterprise and causes of potential losses and business disruptions, and then assessing the level of impact that the identified threats may have on the enterprise.

IT risk is a component of the overall risk universe of the enterprise. Since IT is extensively used in all areas of the enterprise, IT risk is a business risk and also a component of all other risks such as strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. As shown in **figure 2**, implementing the Risk IT framework helps ensure that:

- The enterprise identifies and analyzes IT-related risks and opportunities and presents them in business terms
- IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities
- IT risk management practices are embedded in the enterprise, enabling it to secure risk-adjusted return

The Risk IT framework enables the enterprise to establish its risk appetite, which is the amount of risk the enterprise is prepared to accept when trying to achieve its objectives (by assessing its objective capacity to absorb losses), and its management culture or predisposition toward risk taking, which could range from cautious to aggressive. In addition, the framework enables the enterprise to establish its risk tolerance, which is the tolerable deviation from the level set by the risk appetite and business objectives, and to provide risk awareness within the enterprise. Risk awareness enables IT risks to be well understood, known and managed by the enterprise.

Figure 2—The Risk IT Framework



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

Analyzing the reasons for the current economic downturn and changing business environments, it was found that even though banks had invested heavily in risk management tools and processes over the years, which made these banks compliant with regulations and could also have assisted in avoiding this economic downturn, they did not invest heavily in risk management tools because the enterprises could not resolve more fundamental risk issues. For example, many banks did not focus sufficiently on addressing the root causes of poor data integrity and quality, resulting in systems that have proved ineffective at producing timely, relevant, decision-oriented information. There was also an overreliance on complex models that were understood by too few people within the banks, and when adequate information was available, only a few managers had the experience, authority and oversight to make actionable decisions.[7] In addition, business models implemented by organizations have continuously evolved over the years, resulting in organizations increasingly providing business services via the Internet. For example, meters installed in a client's home are connected to the enterprise networks over the Internet. As soon as such services are opened up and transmitted via the Internet, companies provide more benefits to their customers, but at the same time, they increase the vulnerabilities and risks, e.g., inappropriate access to enterprise systems and data, customer identity theft, lost e-mails, and system outages.[8] These vulnerabilities and risks can become obstacles in achieving the desired corporate financial results sought by the organization. If

the three lines-of-defense approach had been adopted by these banks, risks such as those mentioned would have been identified and assessed.[9]

As shown in **figure 3**, the Risk IT framework provides the enterprise with risk responses to identified key risks. The purpose of a risk response is to bring risk in line with the defined risk appetite of the enterprise after risk analysis. This means that a response needs to be defined such that future residual risk (current risk with the risk response defined and implemented) is, as much as possible (usually dependent on budgets available), within risk tolerance limits. The four types of responses are:

1. **Risk avoidance**—Exiting activities or conditions that give rise to risk. Risk avoidance applies when no other risk response is adequate.
2. **Risk sharing/transfer**—Reducing risk frequency or impact by transferring or sharing a portion of the risk. Examples include insurance and outsourcing.
3. **Risk acceptance**—No action taken relative to a particular risk—loss accepted if or when it occurs. This is different from being ignorant of risk in that accepting the risk assumes that the risk is known and an informed decision has been made by management to accept it.

Figure 3—Risk Analysis and Responses

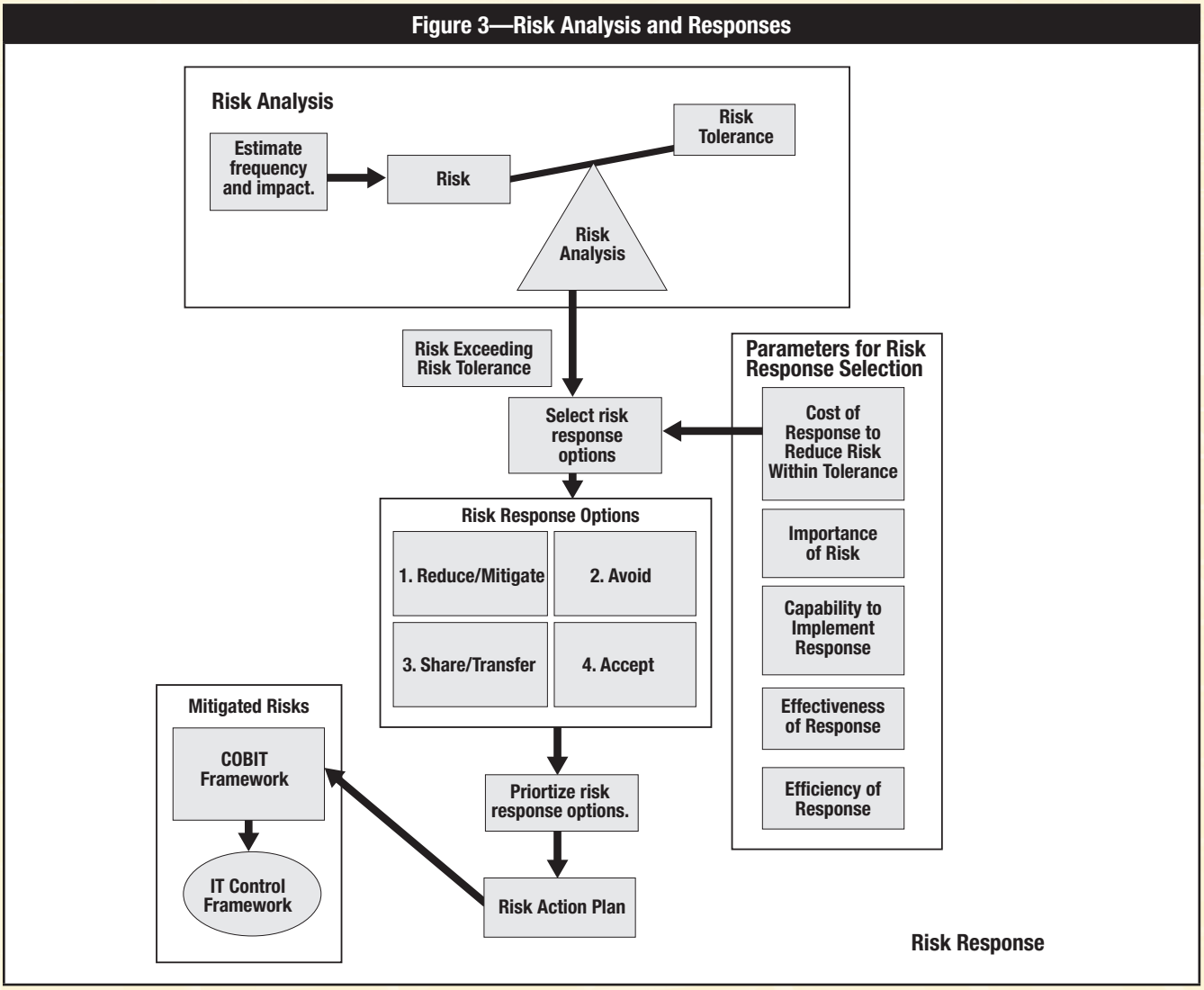


Figure 4—Mapping Key IT Risks (Risk IT) to Key Controls (COBIT)				
	IT Management Capabilities			
High-level Risk	Plan and Organize (PO)	Acquire and Implement (AI)	Deliver and Support (DS)	Monitor and Evaluate (ME)
Logical attacks	PO2 Define the information architecture		DS5 Ensure system security	
	PO3 Determine technological direction		DS 12 Manage the physical environment	

4. **Risk reduction/mitigation**—Action taken to detect risk, followed by action to reduce the frequency and/or impact of a risk. Mitigated risks can be managed through a control framework for IT governance, such as COBIT.[10]

COBIT provides a framework of processes and key controls that can be matched to identified key risks to which the enterprise has decided to respond via mitigation. As shown in **figure 4**, an example of a typical identified key risk is stated as "logical attacks." A risk response of mitigation results in this risk being matched to the COBIT IT processes PO2, PO3, DS5 and DS12 (from the Plan and Organize [PO] and Deliver and Support [DS] domains) and their associated control objectives.[11]

The second line of defense entails setting company boundaries by drafting and implementing policies and procedures and embedding the controls into these procedures, ensuring that existing procedures and policies are kept up to date, responding to new strategic priorities and risks, monitoring to ensure compliance with the updated policies, and providing surveillance over the effectiveness of the compliance controls embedded in the business.[12, 13] The COBIT framework provides a reference process model for the second line of defense because it defines IT activities in a generic process within four domains—PO, Acquire and Implement (AI), DS, and Monitor and Evaluate (ME). COBIT has defined processes with associated control objectives, and it also overarches IT controls. Therefore, these predefined processes and controls can be used as a starting point for an enterprise in drafting and creating its policies, procedures and controls. COBIT also encourages process ownership, enabling the definition of responsibilities and accountabilities.[14]

The third line of defense is the role of independent assurance providers such as internal and external audit, which offers independent review of the levels of assurance provided by business operations and oversight functions. This involves providing independent audit of the key controls and formal reporting on assurance.[15] As shown in **figure 5**, the list of typical activities of a risk-based assurance plan can be linked to the Risk IT and COBIT components, which can then be leveraged to make assurance activities more effective and efficient. To gain insight into an entity in which the IT assurance activities are to be performed, outputs from the Risk IT framework provide an insight to the key risks while IT assurance activities, such as planning, scoping and testing, extensively use the material that is at the heart of COBIT—the control objectives. Some of the strongest links between Risk IT and COBIT components and IT assurance activities are as follows:[16]

Figure 5—Mapping of IT Assurance Activities		
IT Assurance Activities	Risk IT	COBIT
Perform a quick risk assessment.	√	
Assess threat, vulnerability and business impact.	√	
Diagnose operational and project risk.	√	
Plan risk-based assurance initiatives.	√	√
Identify critical IT processes based on value drivers.		√
Assess process maturity.		√
Scope and plan assurance initiatives.		√
Select the control objectives for critical processes.		√
Customize control objectives.		√
Build a detailed assurance program.		√
Test and evaluate controls.		√
Substantiate risk.		√
Report assurance conclusions.		√
Self-assess process maturity.		√
Self-assess controls.		√

- Outputs of the Risk IT risk analysis process and COBIT goals and outcome measures with planning risk-based assurance initiatives
- Outputs of the Risk IT risk analysis process and COBIT risk and value statements with risk assessments and risk substantiation
- COBIT key activities and Responsible, Accountable, Consulted and Informed (RACI) charts with detailed assurance planning
- COBIT control objectives and practices with testing and evaluating controls
- COBIT maturity models and attributes with process maturity and other high-level assessments

CONCLUSION

IT is used by enterprises for automating business processes and transforming current business models, and significant investment is made by enterprises in this area. The increasing use of IT within an enterprise results in an increasing existence of IT-related risk that, if not properly managed, can deter an enterprise from achieving its business goals. An enterprise can manage IT-related risk effectively through establishing an IT governance framework. Such a framework can be achieved through the adoption of the three lines of defense model, which consists of risk identification and assessment, risk management, and risk monitoring. The adoption and implementation of the Risk IT and COBIT frameworks within the boundaries of the three lines of defense model further strengthen an enterprise's IT governance framework.

ENDNOTES

[1] Wyatt, Edward; "Fed Chief Says US Bolstered Its Ability to Handle Failure of a Big Bank," *The New York Times*, 17 February 2011

[2] Laplante, Phillip A.; Thomas Costello; *CIO Wisdom II: More Best Practices*, Prentice Hall, USA, 2005

[3] ISACA, *Implementing and Continually Improving IT Governance*, USA, 2009

[4] *Ibid*.

[5] Caprasse, Denise; Julien Laurent; Wendy Reed; "Three Lines of Defence: How to Take the Burden Out of Compliance," *Insurance Digest, www.pwc.com/en_GX/gx/insurance/pdf/three_lines_of_defence.pdf*

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

[7] *Op cit*, Caprasse

[8] Nelson, Fritz; Val Rahmani; Daniel Sabbah; Al Zollar; "Understanding IT Governance and Risk Management to Maximize IT Business Value," video

[9] Teschner, Charles; Peter Golder; Thorsten Liebert; "Banks' Three Lines of Defense," *Bringing Back Best Practices in Risk Management*, Booz & Co., Germany, 2008

[10] *Op cit*, ISACA, *The Risk IT Framework*

[11] IT Governance Institute (ITGI), COBIT® 4.1, USA, 2007

[12] KPMG, "The Three Lines of Defence," Audit Committee Institute, Quarterly 25, Belgium, 2009

[13] *Op cit*, Caprasse

[14] *Op cit*, ITGI

[15] *Op cit*, Caprasse

[16] *Op cit*, ITGI

Information Risk Management for Supporting a Basel II Initiative

The Role of Automated Controls and Continuous Monitoring

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. Dutta is a recognized thought leader and has published numerous articles.

Prasad Sista is a manager in the Products Group at Infogix. Prior to joining Infogix in 2011, Sista worked for more than a decade in multiple roles as a product manager, a project leader and an operations strategy consultant across various industry verticals such as high-tech, consumer electronics, food service and automotive.

Effective January 2008, Basel II stipulates the minimum capital requirements that financial institutions must possess in order to manage their risks. In addition to providing multiple risk capital calculation options, Basel II introduces operational risk as part of the risk portfolio. Operational risk is defined as the "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."[1]

The Basel II framework uses three pillars.[2] Pillar I provides detailed methods for calculating minimum regulatory capital. Organizations have the option to choose estimating credit risk exposures with a standardized approach, the foundation internal rating-based (IRB) approach, or the advanced internal rating-based (AIRB) approach. To calculate the capital requirements per the Pillar I directives, organizations need to collect various types of credit risk, market risk and operational risk information (e.g., loan information, market information) from multiple, often disparate, sources, including external sources. The trustworthiness of the calculated capital requirements will depend largely on the quality of the underlying information. In addition, the reliability of the internal models (as an alternative to the standardized approach to calculate regulatory capital requirements) depends on the quality of the information used for validating the model.

Pillar II refers to supervisory review standards that provide regulators with oversight, discipline and action over Basel II, and involves the demonstration of an adequate governance system, including the implementation of an effective enterprise risk management (ERM) system. A large percentage of the operational risk stems from information quality issues. For example, duplicate payment or service level agreement (SLA) violations can be attributed largely to poor information governance issues and stem from inherent information risks present within an information-driven environment. To effectively mitigate information risks, financial organizations need to use appropriate controls to detect and prevent information quality issues in their transactional systems.

Pillar III refers to market disclosure, and aims at promoting financial stability through increased transparency and disclosure requirements. This final pillar requires financial institutions to publicly provide details of their risk management activities, risk-rating processes and risk distributions. While reporting itself may be a daunting task, the reconciliation of financial information between Basel II and other statutory reports, such as International Financial Reporting Standards (IFRS)/Generally Accepted Accounting Principles (GAAP), will be a challenge. However, without such reconciliation, there will be questions around the accuracy of the reported risks.

To reduce information risk exposure through appropriate risk mitigation processes, financial organizations need to put a stronger focus on information quality management. Poor information quality in risk information repositories increases the uncertainties about the information used for risk calculation, possibly resulting in inaccurate risk capital calculation. In addition, poor information quality in transactional systems increases operational losses (e.g., fines incurred due to SLA violations). While this article primarily addresses the Basel II requirements applicable to financial services organizations, the information quality issues and mitigation principles outlined in this article are equally applicable to financial, insurance and nonfinancial corporations. Standard and Poor's,[3, 4, 5] a leading credit-rating agency, recently incorporated ERM, using frameworks similar to Basel II and Solvency II, as a factor in its credit-rating methodology. This is reflective of a growing market need to understand an organization's risk exposure and its ability to address risk. To achieve favorable ratings, organizations should be able to demonstrate sound practices in dealing with risk, including information risk.

INFORMATION RISKS IMPLICATIONS FOR OPERATIONAL RISK MANAGEMENT

The Basel Committee classifies operational loss data in seven distinct categories. **Figure 1** summarizes the result of the internal loss data collected from 119 institutions from 17 countries, representing a total loss of €59.6 billion.[6]

As shown in **figure 1**, approximately 30 percent of losses can be attributed to execution, delivery and process management. This category captures the losses due to, for example, failed or duplicate transactions, SLA-violation-related losses with trade suppliers and vendors, incomplete data, accounting errors, and compliance failure errors.

Based on the authors' work with large financial organizations and review of categories of operational loss events,[7] a large percentage of losses of this particular category (execution, delivery and process management) can be attributed to information-risk-related errors.

Based on the authors' work with large financial organizations and analysis of operational risk data,[8] the following four categories of information risk (**figure 2**) can be identified:

1. **Transaction processing risk**—With the considerable number of transaction processes occurring within financial institutions, there are complex information flows related to orders, settlements, automated teller machines (ATMs), deposits and money movement. If these transaction messages are lost or delayed, financial institutions will need to cope with a loss of revenue and an increase in customer complaints.
2. **External information exchange risk**—Financial institutions exchange information with third parties (e.g., credit card settlements, interbanking settlements, loan servicing). Errors in information exchanged with third parties result in subsequent incomplete transactions, dropped transactions and SLA violations. Unlike transaction processing risks, information risks associated with external information exchanges are extrinsic to the organization's technology

Figure 1—Operational Loss by Category

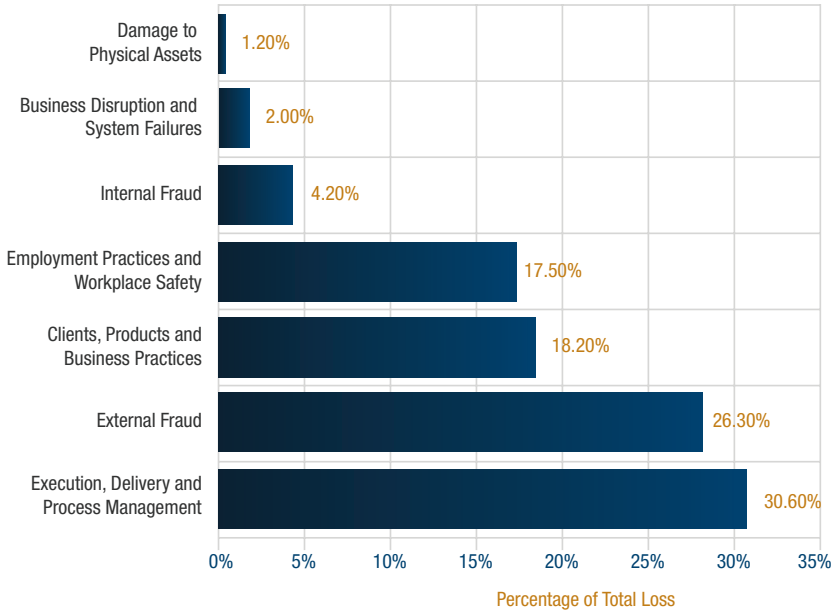
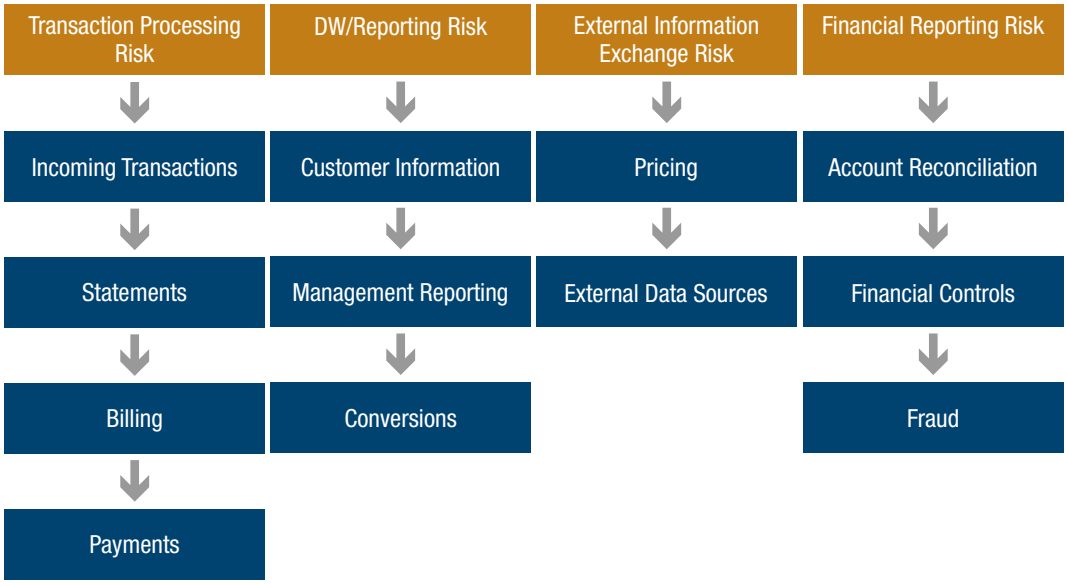


Figure 2—Categories of Information Risk



environment and cannot be completely mitigated through its internal systems. Organizations need to reduce this risk through detective reasonability controls.

3. **Financial reporting risk**—The financial reporting system must have complete and accurate information and must reconcile with the information present in other reporting systems such as credit risk repositories. In addition, incomplete or incorrect posting of accounts payable and accounts receivable information to the general ledger results may result in erroneous financial reports resulting in rework and loss in market credibility.
4. **Fraud risk**—Financial institutions incur additional costs due to internal fraudulent activities such as unauthorized trading, credit card fraud and improper cash movement.

INFORMATION RISK IMPLICATIONS FOR CREDIT RISK CALCULATION

IRB or AIRB approaches require financial organizations to collect transactional details of credit risk exposures from a diverse set of systems and lines of business supporting various credit-related products. Data from the source systems are often extracted and transformed to ensure a consistent format for risk calculation. For example, a large financial institution captures credit exposure information from 26 different systems for calculating credit risk under the IRB approach.[9] This organization identifies the following information risk factors that could result in information errors in the credit risk repository, resulting in inaccurate credit risk calculation:

- Data quality issues with the source system
- Changes in the source systems
- Extract, transfer and load process failures

To ensure the accuracy, consistency and reliability of the risk calculation process, the bank uses the following checks and balances:

- Verify the completeness, format and domain of values of the source systems prior to loading the source extracts to the line of business data warehouse.
- Verify the integrity of the data transformation process by comparing the source information with the data warehouse information.
- Reconcile the data warehouse information with the general ledger to ensure consistency between the risk calculation and the financial statements.

Figure 3 depicts the high-level architecture of information controls deployed within the Basel II credit risk repository of one large financial institution. This organization is currently assessing information risk exposure in its market risk calculation process.

ROOT CAUSES OF INFORMATION QUALITY ISSUES IN FINANCIAL INSTITUTIONS

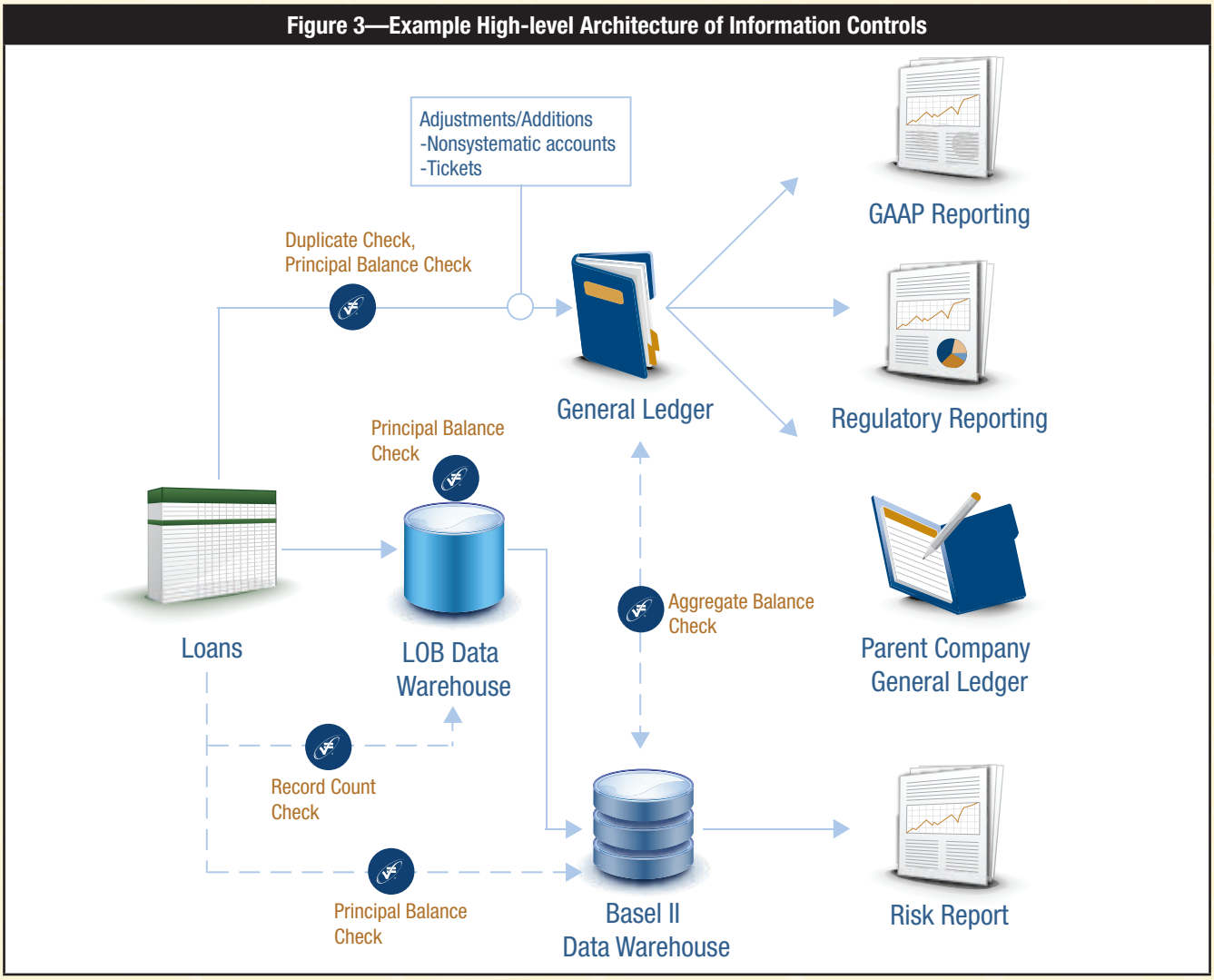
Data in financial organizations have primarily two states, and both states are susceptible to information quality issues:

1. **Data at rest**—Certain systems, such as customer relationship management systems and loan management systems, serve as the source of input information for other systems. Data in these systems are referred to as "data at rest."
2. **Data in motion**—Data are often exchanged between or processed by two or more systems. The data in this state are often referred to as "data in motion."

While several factors can be attributed to information quality issues, the following are the major causes of information errors experienced in most financial institutions:

- **Information quality issues with the source system**—Source system information may be incomplete or inconsistent. For example, a customer record in the source system may have a missing identification code. Similarly, source system information related to a policy may use an abbreviation of the policy names in their information base. These types of information issues can be attributed primarily to manual information input, lack of information standards and poor quality of third-party information used by the source system. Information errors in the source system propagate in the downstream systems, resulting in higher detection and clean-up costs. Incompleteness and inaccuracies in certain source system information will lead to quality issues in the target systems used for regulatory capital calculations.
- **External information provider**—Financial institutions routinely exchange critical information with third-party vendors and partners. Without appropriate completeness and accuracy checks, the probabilities of information quality issues are high.

Figure 3—Example High-level Architecture of Information Controls



- **Multiple systems**—To support Basel II, financial institutions need to pull information from multiple source systems located in a diverse set of technology platforms. Information extraction, transformation and normalization increases the inherent information risk present in the environment.
- **Process failures**—Information transfer processes may fail due to system errors or transformation errors, resulting in incomplete information loading. System errors may include process failures due to the unavailability of source system/extract or the incorrect format of the source information. Transformation errors may result from incorrect formats.
- **Changes/updates in the reference information**—Outdated, incomplete or incorrect reference information will lead to errors in the risk repository information.

CURRENT APPROACHES AND CHALLENGES

Most financial institutions recognize the importance of information quality and have some form of an information quality program in place. However, current approaches are often fragmented, *ad hoc* and costly, as a result of organizational silos and varying departmental needs. In most cases, the primary focus of the current initiatives is on data at rest (e.g., names and addresses in a customer relationship management system). The scope of these initiatives is often limited to periodic review and cleaning of critical information provisioning systems.

While the importance of clean information in data-at-rest systems is paramount, financial institutions must address the information quality issues when information is in motion (e.g., information exchanged between systems, people and organizations) to comply with Basel II. Current approaches to governing data in motion include:

- After-the-fact manual or semiautomated balancing, tracking and reconciliation to verify appropriateness, completeness and accuracy
- Extensive research and remediation to identify, diagnose and correct issues identified during the previous steps

More specifically, current approaches suffer from the following limitations as they relate to supporting the Basel II information quality requirements:

- **Detective vs. preventive**—Existing information quality initiatives rely on detection vs. prevention of information issues. The detective approach may result in costly calculation reruns and delays in internal model approval, and often require extensive manual interventions.
- **Narrow scope and focus**—Current information quality initiatives do not fully address the quality issues when information is in motion, resulting in increased operational risk and erroneous information for use in regulatory capital requirement calculations.
- **Lack of monitoring and visibility**—Current approaches do not focus on measuring and monitoring information quality on an ongoing basis, thus resulting in a delayed response to information quality issues. In addition, these initiatives do not provide comprehensive visibility across processes, resulting in an increased cost of resolving information errors.

More important, the effectiveness of these initiatives degrades due to the presence of multiple systems, complex information structure and increased adoption of a real-time distributed technology environment. The problem exacerbates when a financial institution is required to provide evidence of information quality in the risk information used for regulatory capital calculation. Typically, risk information is collected from multiple transactional systems and stored in a risk repository, which serves as the source for internal model and risk capital calculations. In this scenario, the requests for information quality evidence will be met by querying a myriad of log files, e-mail chains and risk repository tables. This not only increases the cost, it also, in some instances, may delay the certification of the risk capital calculation.

> "Financial institutions must address the information quality issues when information is in motion."

Current approaches provide short-term respites, but are not sustainable in the long term. The increased labor costs of manual processes and high development costs of *ad hoc* information quality detection and correction programs increase the ongoing operational costs.

REQUIRED CAPABILITIES FOR ENSURING INFORMATION QUALITY FOR BASEL II

To support information quality management, financial institutions must consider required minimum capabilities as described in the following sections. To reduce cost and increase efficiency, organizations should aim at automating these capabilities to the extent possible.

Information Controls

Information controls are application-independent, automated routines/procedures that can validate data at rest and data in motion to detect and prevent errors and to identify anomalies.

Ideally, information controls should have the following capabilities to validate data at rest and data in motion:

- **Verification**—Ability to verify the information content and format and the spatial and temporal reasonability of transactions
- **Balancing**—Ability to balance information as it traverses through various systems
- **Reconciliation**—Ability to reconcile information at an aggregated and transactional level
- **Tracking**—Ability to track information flows to ensure adherence to SLA agreements and timeliness requirements

Well-designed information controls can validate information at an aggregate level as well as at a transaction level.

Exception Management

Even with the most advanced control system in place, exceptions do occur. Exception management is an automated workflow that can support investigation and resolution of errors detected or prevented by information controls. Ideally, exception management should have the following capabilities to support resolution of errors within a certain time frame (**figure 4**):

- **Routing**—Ability to route the error to the appropriate resource for research and resolution
- **Research**—Ability to research secondary sources and audit the trail of the information flow
- **Resolution**—Ability to correct the issue
- **Reporting**—Ability to provide an audit-trail report on exception resolution and status reports on exceptions and their resolution status

Continuous Monitoring

Continuous monitoring enables organizations to achieve visibility and improve the information quality across processes.

Ideally, continuous monitoring should have the following capabilities to meet the integrated visibility needs by combining process, risk, control and performance information (**figure 5**):

- **Process monitoring**—Ability to measure and trend process information, such as information volume and information quality indicators
- **Control monitoring**—Ability to monitor the effectiveness of the information controls deployed to prevent information quality issues
- **Exception management**—Ability to monitor exception resolution progress
- **Reporting**—Ability to create standardized and *ad hoc* reports to support audit and business needs

Continuous monitoring should provide visibility into risk indicators, control performance and exception management status in the context of a process view as shown in **figure 6**.

Figure 5—Need Capabilities for Continuous Monitoring

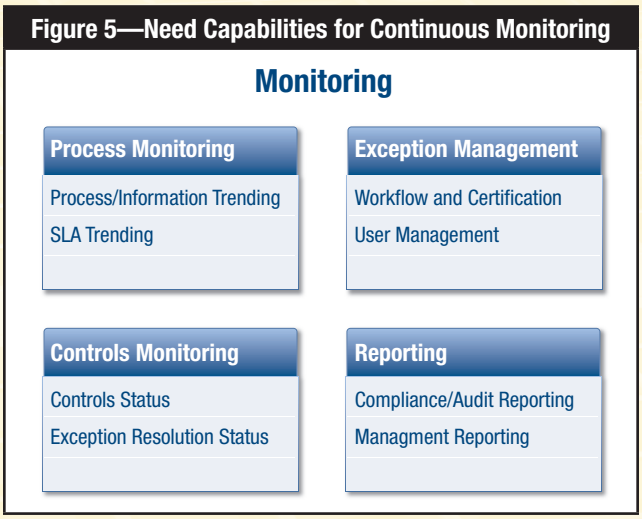


Figure 4—Needed Capabilities for Exception Management

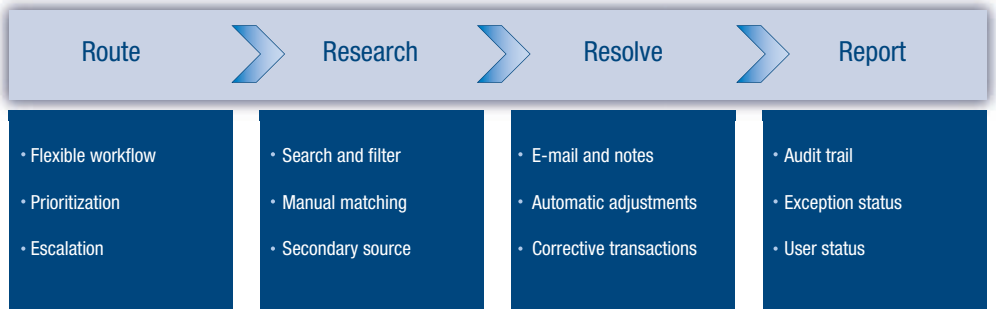
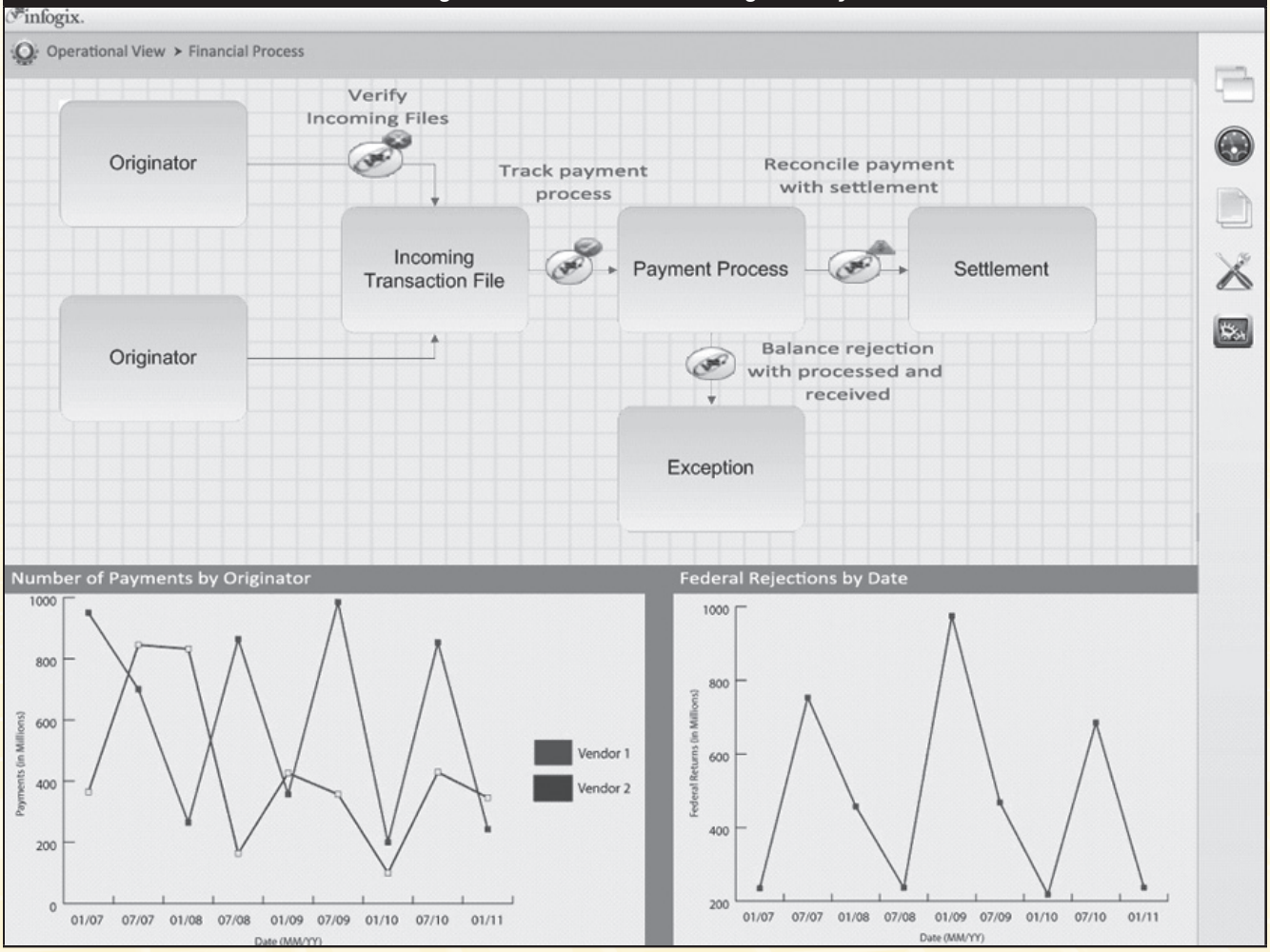


Figure 6—Continuous Monitoring Visibility



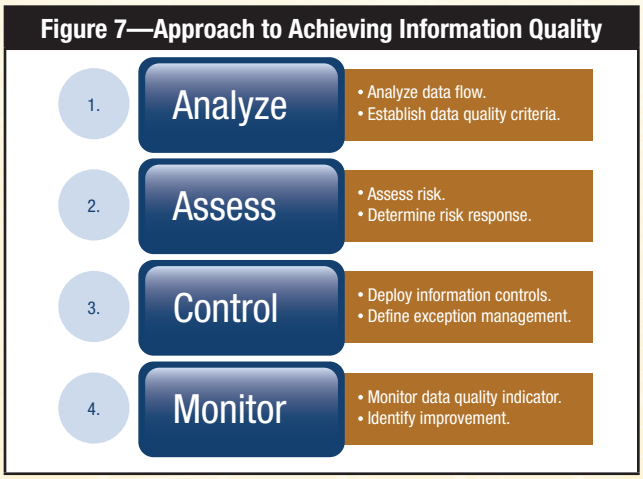
ESTABLISHING AN INFORMATION QUALITY MANAGEMENT FRAMEWORK

Establishing a comprehensive and sustainable information quality management program could be daunting in the absence of a structured approach. Financial institutions may consider adopting the following four-phase approach to achieve the information quality necessary to comply with Basel II (**figure 7**):

1. **Analyze**—In this phase, critical information flows relevant to Basel II need to be identified. All information provisioning systems, including external source systems along with their information lineage, need to be identified and documented. Special attention must be given to establish a common understanding of the key information elements between the source system and the target system. In this phase, source and target system owners should jointly establish information quality criteria and information quality measurement metrics for the key information elements.
2. **Assess**—In this phase, financial institutions must assess information quality risk for both data at rest and data in motion. Once the risks are evaluated and prioritized, financial institutions must determine an appropriate response based on a cost-benefit analysis.
3. **Control**—Appropriate information controls and exception management processes must be defined and deployed to address the risks identified in the assessment phase. Financial institutions should consider using automated controls to avoid sampling errors and to gain efficiency.
4. **Monitor**—Once appropriate controls are in place, business owners should monitor the information quality indicators established in the analysis phase and identify opportunities

for improvements by analyzing the microtrends in the information quality indicators. Automated continuous monitoring solutions provide the most cost-effective approach for monitoring.

Figure 7—Approach to Achieving Information Quality



CONCLUSION

Information quality issues in the information used for capital requirements for credit risk will impact the trustworthiness of the estimated capital requirements. More important, they may limit the method that can be used for risk calculation. Information risk inherently presents, within critical business processes, increases in operational risk, resulting in operational losses. As financial organizations further optimize their risk management processes for supporting Basel II directives, they need to put a stronger focus on managing information risk.

> "Organizations should use automated methods for mitigating, monitoring and reporting information risks."

Inefficiencies in existing information risk management processes stem from information silos across product lines, mergers and acquisitions, and the prevalence of manual steps within most processes. Wherever applicable, organizations should use automated methods for mitigating, monitoring and reporting information risks. Leading financial organizations have initiated projects to achieve efficiencies through automation, standardization and centralization of information risk management activities.

ENDNOTES

[1] Basel Committee on Banking Supervision, *Operational Risk*, Bank for International Settlements, Switzerland, 2001, *www.bis.org/publ/bcbsca07.pdf*

[2] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards*, Bank for International Settlements, Switzerland, 2004, *www.bis.org/publ/bcbs107a.pdf*

[3] Standard and Poor's, *A New Level of Enterprise Risk Management Analysis: Methodology for Assessing Insurers' Economic Capital Models*, USA, 2010

[4] Standard and Poor's, *Standard & Poor's to Apply Enterprise Risk Analysis to Corporate Ratings*, USA, 2008

[5] Standard and Poor's, *Assessing Enterprise Risk Management Practices of Financial Institutions*, USA, 2006

[6] Basel Committee on Banking Supervision, *Results From the 2008 Loss Data Collection Exercise for Operational Risk*, Bank for International Settlements, Switzerland, 2009, *www.bis.org/publ/bcbs160a.pdf*

[7] Global Risk Guard, "Operational Risk," *www.globalriskguard.com/html/operational_risk.html*

[8] *Op cit*, Basel Committee on Banking Supervision, 2009

[9] This example is taken from the authors' experience with this client.

The Devil's in the Details

Fighting Fraud With Audit Analytics

Seth Davis, CFA, CIA, CPCU, is vice president of internal audit at RLI Insurance in Peoria, Illinois, USA. He has more than 12 years of insurance and audit experience.

Pat Ferrell, ARe, AIC, CPCU, is a director of internal audit at RLI Insurance in Peoria, where his main responsibilities are managing audits and overseeing RLI's monthly analytics.

Sean Scranton, CISA, CISM, CCNA, CISSP, is IT audit director at RLI Corp. His background includes experience in router/firewall administration and performing IT security reviews, audits and Internet vulnerability assessments.

Peter Millar is the director of technology application at ACL Services Ltd. For the past 14 years, Millar has been involved in the evolution of analytic solutions for audit departments.

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.

Go directly to the article:

Fraud impacted 87 percent of organizations in 2010, according to the Kroll *Global Fraud Report*.[1] The evidence of this fraud often resides in an organization's data—whether the inappropriate activity is a payment to a phantom vendor or a doctored expense report. Unfortunately, these schemes often go undetected for months and even years, draining evermore revenue from the organization. A global study of 1,843 cases of occupational fraud compiled by the Association of Certified Fraud Examiners (ACFE) found that one-quarter of these ploys involved losses of at least US $1 million, while the fraudulent activities lasted a median of 18 months before discovery.[2]

HOW TO RESPOND

In the *11th Global Fraud Survey* from Ernst & Young, 65 percent of more than 1,400 respondents agreed that internal audit is an important line of defense against fraud for companies.[3] A systematic approach with a risk-based methodology is the best way to uncover fraud, revenue leakage and misuse of corporate resources.

To understand the techniques internal audit organizations are using to fight fraud, this article examines the internal audit group at RLI Insurance,[4] a specialty property and casualty insurance company. Armed with a mandate to uncover fraud and lost revenue, the internal audit group at RLI recently implemented an ACL audit analytic solution to fulfill this mandate more effectively and efficiently. Audit analytics can quickly examine large files and flag the digital markers of potentially fraudulent activity to help auditors work more efficiently.

At RLI, each audit begins with six weeks of planning, during which time staff completes narratives, workflows, risk assessments (which always include a fraud component) and detailed walk-throughs of audit processes. This is a critical phase for all internal audit groups. This disciplined approach is used to develop a risk-based audit program, with a heavy emphasis on data analytics. In its 2010 survey of more than 2,000 internal auditors from more than 50 territories worldwide, PricewaterhouseCoopers concluded that "leveraging technology should be directed at solving a business problem or issue rather than acquiring technology for technology's sake. This requires a clear assessment of the audit life cycle to find ways to use technology to enable measurable efficiency."[5] Audit analytics should be leveraged to achieve well-defined goals built on a sound examination of key risk areas.

Once data-analytic targets are established, analytic technology can be used to extract, scrub (standardize) and analyze data for a variety of anomalies. An automated solution should always provide independent access to source data, minimizing the need for IT intervention and protecting network integrity. Each audit should include analytics to pinpoint data irregularities that could indicate:

- Segregation-of-duties conflicts
- Transactions modified to avoid approval and/or authorization
- Funds leakage
- Inappropriate payments
- Abuse of corporate assets and/or fraud

> "Many companies also create a culture of innovation that encourages employees to develop additional tests and continually advance their technical skills."

At RLI, all members of the seven-person internal audit team are trained to use the technology and must include analytics in their audit plans, or provide valid reasons why analytics are excluded. Many companies also create a culture of innovation that encourages employees to develop additional tests and continually advance their technical skills.

Enjoying this article?

- Read *Data Analytics—A Practical Approach*.

www.isaca.org/white-papers

- Learn more about, discuss and collaborate on fraud in the Knowledge Center.

www.isaca.org/topic-fraud

EXAMPLE TESTS

To uncover relevant anomalies, data tests should use multiple parameters. For example, analytics can compare employee data fields (including names, addresses, phone numbers, bank accounts and tax identification [ID] numbers) that match—or partially match—vendor payments and invoices to identify potential conflicts of interest. Duplicate payment analyses should look for identical or near-identical invoice numbers, totals, dates and vendor ID numbers. Automated tests for expense fraud can highlight payments that meet or exceed specific monetary limits, or employees that regularly submit expense claims just below approval thresholds. Analytics should also target transaction dates to ensure that items are in the proper period and that liabilities are posted in a timely manner. Joining, matching and precise comparisons in the data can highlight exceptions in even the largest data files.

To battle procurement-card (corporate credit cards, used to purchase supplies and other items at RLI) fraud, analytics should identify instances in which the cardholder and the expense approver are the same person or should identify employees who split transactions to avoid authorization limits. Transactions may be split inappropriately among multiple invoices or between two or more employees. To identify these items, analytics may focus on multiple transactions on the same day to the same vendor for all cardholders. Other analytics should use key-word searches to target inappropriate purchases, such as prohibited items or products for personal use.

Financial reporting fraud is another common area of concern. The ACFE's 2010 *Report to the Nations* revealed that financial-statement fraud is the most costly form of occupational fraud for organizations worldwide, causing a median loss of more than US $4 million.[6] Tailored analytics can examine data to find journal entries made by unauthorized users and entries tagged as "write-offs," for example. Accounts payable data should also be tested to identify single vendors with multiple phone numbers, addresses and tax ID numbers, among other red flags.

A RISK-BASED APPROACH

The need for purpose-driven analytics has become increasingly clear. According to 2010 research from The Institute of Internal Auditors (The IIA), "the use of automated tools or techniques" by internal audit functions has become a top-five strategic priority.[7] Audit analytics enable audit teams to examine 100 percent of the transactions from a specific time period or business area, based on easily modifiable parameters. Auditors need a reliable way to determine which transactional exceptions represent significant internal control risks. Analytics quickly identify unusual data patterns or results, and while the full visibility ensures a comprehensive audit, reviewing the anomalies can be time consuming.

At RLI, the audit team first ensures that both the analytics and corporate data are understood to make certain the analytic test findings are valid. For example, in one case, an initial claim data import indicated that the company appeared to have added an impossibly large number of new transactions in a single month. Further investigation revealed that claim summaries, as well as new transactions, had inappropriately been included during the initial analysis. It was also learned that the "examiner" field should be used exclusively to analyze claim data, instead of the synonymous "adjustor" field.

> "Every organization has unique data issues, idiosyncrasies and patterns, so it is crucial to validate data."

Every organization has unique data issues, idiosyncrasies and patterns, so it is crucial to validate data before analysis and to understand the purpose of each input field. This is where experience with audit analytics and audit technology becomes especially valuable. In the 2010 IIA internal auditing survey, 56 percent of Fortune 500 respondents said they believed that auditors need data mining and analytic skills—a necessity that registered just below business and industry-specific knowledge (61 percent), as the most important career skill set for today's internal auditors.[8]

In the previous example, once the RLI team was familiar with the nuances of the payment data, a fraud-indicator approach was created that weights test results based on their propensity for fraud. Transactions or vendors flagged in multiple tests, for example, rank as a higher review priority

than a lower-risk anomaly that appears only once, such as an invoice submitted on the weekend or vendor payments directed to post office (PO) boxes. Each extract is assigned a weight on a numbered scale from one to three, with higher numbers representing an elevated level of risk. The total vendor score is the sum of the weights assigned to the extracts in which that vendor appears. For example, if vendor XYZ appeared in a PO box extract with a weight of one, a missing tax ID extract with a weight of three, and missing address extract with a weight of three, the vendor would be assigned a total score of seven. Auditors examine any vendors whose total score is five or more. By prioritizing results according to specific red flags and minimizing time spent reviewing false positives, the team is more risk focused and has cut review times by more than 25 percent.

VIGILANCE THROUGH ADAPTATION

Just as fraudsters modify their schemes to exploit internal weaknesses, audit teams must continually expand and refine their data testing. Each audit offers a new perspective on the organization's key risks and controls and prepares auditors to develop increasingly sophisticated data tests.

> "The analytics offer broad business insight that would be impossible to achieve through manual sampling practices."

At the end of each audit, team members should formalize their quality assurance process by completing a detailed review of the audit, e.g., evaluation of how to improve audits and data-access procedures and how specific tests could be strengthened and refined for future use. The most effective analytics can then be migrated into repeatable routines for review by the audit group, business stakeholders and management.

DETAILED INVESTIGATIONS PRODUCE BOTTOM-LINE RESULTS

Committing to audit analytics can improve data coverage and internal audit productivity and lead to the recovery of costs and lost funds. By embedding audit analytics in each audit project, the risks associated with manual sampling can be significantly reduced and more meaningful results can be delivered to management. Used proactively, analytic technology can uncover significant control gaps that would almost certainly go undetected without complete data coverage. For example, in another case, the RLI team used risk-based data tests to validate a liability deductible query and uncovered more than US $4 million in missed billings. The company has recovered a large percentage of those lost funds and has continued to use audit analytics to identify more than US $100,000 in annual funds leakage.

In a business environment that requires strict internal controls, technology is an effective way to identify conflicts of interest in a variety of forms. This capability not only enables management to address individual cases, it also promotes more airtight internal procedures and can enhance corporate disclosure processes. Strategic data analysis can also reveal costly control and visibility issues, such as data integrity, access and security concerns. The analytics offer broad business insight that would be impossible to achieve through manual sampling practices.

CONCLUSION

In a sluggish economic climate, financial pressures can tempt employees to take liberties with company policies and, in the most serious cases, to intentionally commit fraud. Strategic use of audit analytics can be an effective weapon against the abuse of corporate resources. The RLI internal audit group has found that embedding data analysis into the audit plan and using a weighted red-flag approach can deliver significant results.

Every organization has unique data patterns, issues and systems. Taking time to learn these nuances and to fully understand internal control risks is one key to successfully leveraging analytic technology. When the analyses are complete, it is equally important to look for ways to enhance the audit process and the logic behind the automated testing. The most valuable analytics can then be turned into repeatable routines that offer ongoing business insight.

For organizations eager to strengthen internal controls, audit analytics minimize sampling risk and promote efficient, highly focused audit practices. These solutions should provide full-population visibility and the power to uncover small anomalies in a virtual ocean of data—casting a wider net to more effectively fight corporate waste and fraud.

ENDNOTES

[1] Kroll, *Global Fraud Report*, 2010/11, *www.kroll.com/*

library/fraud/FraudReport_English-US_Oct10.pdf
[2] Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud and Abuse*, 2010, *www.acfe.com/rttn/rttn-2010.pdf*
[3] Ernst & Young, *11th Global Fraud Survey, Driving ethical growth—new markets, new challenges,* 2010, *www.ey.com/GL/en/Services/Assurance/Fraud-Investigation---Dispute-Services/11th-Global-Fraud-Survey---Driving-ethical-growth---new-markets--new-challenges*
[4] RLI Insurance, *www.rlicorp.com*
[5] PricewaterhouseCoopers, *A Future Rich in Opportunity: State of the Internal Audit Profession Study*, 2010, *www.pwc.com/us/en/internal-audit/publications/2010-study-internal-audit-profession.jhtml*
[6] *Op cit*, Association of Certified Fraud Examiners
[7] The Institute of Internal Auditors, *Internal Auditing in 2010: Shifting Priorities for a Changing Environment*, 2010, *www.theiia.org/download.cfm?file=56143*
[8] *Ibid*.

Incorporating COBIT Best Practices in PCI DSS V2.0 for Effective Compliance

Mathew Nicho, Ph.D., CEH, SAP-SA, RWSP, is an assistant professor of information systems at the College of Information Technology of the University of Dubai (UAE). He also conducts a professional course on ethical hacking for IT professionals. Nicho can be contacted at *mnicho@ud.ac.ae.*

Payment Card Industry Data Security Standard version 2.0 (PCI DSS v2.0) was released by the PCI Security Council in October 2010 and comes with clarifications and guidance that expand upon the previous version. With more and more transactions based on credit cards, merchants dealing with these are forced to comply with standards such as PCI DSS v2.0 or face huge penalties. As PCI DSS v2.0 is generic in nature while highly specific with in-depth, focused controls, merchants are finding it costly and increasingly difficult to implement and interpret this standard. COBIT, initially released in 1995 with the latest version released in 2007 (and an update scheduled for release in early 2012), has much in common with PCI DSS and comes with detailed methodology and guidance. A comparison of the two frameworks reveals that the effectiveness of PCI DSS can be enhanced by using the best practices of COBIT.

In 2008, US customers spent US $2.5 trillion in transactions via credit cards at 24 million locations in 200 countries and territories.[1] With 10,000 payment transactions made every second worldwide,[2] there is good reason to ensure that cardholder information is kept secure. By the end of 2009, there were 576.4 million credit cards and 507 million debit cards in circulation in the US alone, which equates to roughly 3.4 cards for every person in the US.[3] Since most transactions are done electronically using cardholder information, there is an ever-increasing need to ensure the protection of cardholder data. The security of cardholder data has become a more serious concern to businesses worldwide. The reasons for this include high-profile and persistent data breaches,[4] regulatory concerns in financial services and other industries, enactment of regulations regarding reporting of data breaches, changes to court rules requiring availability and proof of integrity of electronically stored information submitted as evidence, and tangible and intangible losses due to breaches.[5] As such, ensuring effective and efficient implementation of PCI DSS v2.0 goes a long way toward securing transactions and mitigating breaches. Viewed from a wider information systems (IS) perspective, the most critical issue facing IT executives is not securing cardholder data, but rather aligning (IT) goals with business goals. IT executives are under pressure to be more flexible, to manage constant change from internal and external sources, to align IT services with business requirements, and to implement business practices.

Experts have argued that PCI DSS should be integrated into the wider IT governance (ITG) domain, since ITG is made up of five core pillars—security, compliance, cost, enablement and efficiency—which are vital for a holistic implementation of IS security.[6] By focusing on these five areas, rather than on just compliance and security, IT managers can move away from an "in place—not in place" approach to PCI DSS v2.0 compliance to one of wider security governance. Since every IT control standard, tool and framework has its own strength and limitation, it makes sense to incorporate the best practices of an appropriate framework into PCI DSS v2.0. IT security, thus, cannot be confined to the PCI DSS focus of securing cardholder data alone, but needs to diverge to the wider IT security perspective to include IT control and assurance. While PCI DSS v2.0 is prescriptive, when a control cannot be implemented for business reasons, there is ample opportunity to replace the specific requirements of the standard with compensating controls, providing equal or greater protection.[7] Research on standard setting has found that incorporating the various interests of the IS network into the governance structure, along with flexibility to satisfy competitive interests, is the key to success.[8]

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.

Go directly to the article:

PCI DSS

Introduced in 2005, PCI DSS is the very first and perhaps the only industrywide standard that focuses mainly on protecting cardholder data. The PCI Security Council is an open, global forum founded by the five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The council was created for developing, managing, educating and communicating the PCI Security Standards, including PCI DSS, the Payment Application Data Security Standard (PA-DSS), and the Personal Identification Number (PIN) Transaction Security (PTS) requirements to merchants, vendors and financial institutions involved in credit card transactions. The objective of the council is to enhance the security of cardholder data and, thus, to help facilitate global adoption of consistent data security measures created to mitigate data breaches and prevent payment cardholder data fraud. Compliance is enforced, by the PCI Security Standards Council, on those dealing with credit cards, and there are penalties for nonconformance to PCI DSS.

ISSUES WITH COMPLIANCE

A study of 500 US and multinational organizations found that, on average, it was necessary to dedicate 35 percent of an organization's security budget to any compliance effort.[9] In a 2009 survey, the UK Corporate IT Forum (CIF) estimated that only 1 percent of the surveyed companies were fully PCI-compliant, that 9 percent failed their audit and that the rest were trying to achieve compliance.[10] Thus, merchants dealing with credit cards are faced with two cost extremes. First, enterprises face the risk of credit card transaction breaches and fraud along with penalties for not complying with the PCI standards. Second, they face huge costs in complying with the PCI standards. For example, in 2008, level-one merchants (those dealing with more than 6 million transactions per year) spent an average of US $3.38 million to become PCI-compliant, including the cost of PCI assessment services.[11] Since 2006, merchants have collectively spent in excess of US $1 billion on compliance to PCI DSS.[12] Becoming PCI-complaint does not mean that the company is insulated from all cyberfraud, but effective implementation can mitigate the risk to a great extent. While PCI DSS v2.0 promises better protection than the former version, there is still room for improvement.

> "Becoming PCI-complaint does not mean that the company is insulated from all cyberfraud, but effective implementation can mitigate the risk to a great extent."

Security Breaches—Lack of an Effective Compliance Mechanism

Even with increasing compliance to standards and regulations, there has been no decrease in attacks on networks. Symantec recorded more than three billion malware attacks in 2010.[13] If recent and former cases are analyzed, it is evident that attacks are becoming more nontechnical and targeted (targeted attacks target employees to penetrate an organization and stay hidden) in nature. A few significant cases follow:

- Starting with a sophisticated attack, one of the most sensational technical data breaches occurred at TJX Companies Inc. in 2006. That year, the enterprise ranked 133rd on the Fortune 500 list. With revenues reaching US $17 billion, 125,000 employees and more than 2,400 stores worldwide, TJX was classified as the largest off-price apparel and home fashions retailer in both the US and the world. However, in late 2006, hackers broke into the systems of TJX and stole vital customer information with estimated losses (tangible and intangible) amounting to US $1 billion—one of the largest security breaches ever reported.[14]
- A less technical breach occurred in 2008 at Hannaford, a PCI-compliant supermarket chain. The data breach, which resulted in reported thefts of 4.2 million customer credit and debit card numbers with 1,800 cases of fraud, began on 7 December 2007. Unusual credit card activity became known on 27 February 2008; the breach was not contained until 10 March 2008 or reported until 17 March 2008. It was later found that unauthorized software that was secretly installed on servers in most of the company's supermarkets enabled the massive data breach.[15, 16, 17]

- Moving toward a nontechnical attack, in 2010, two sensational cases of targeted attacks (spear-phishing) occurred—Stuxnet and Hydraq. The Stuxnet malware, which infected Iranian nuclear plant networks, was reported to have been inserted into the network through a Universal Serial Bus (USB) device. Rather than sabotage, the intention of the Hydraq malware was to steal intellectual property from companies through unsuspecting employees who downloaded the e-mail attachment that contained the hidden malware.
- The 2011 data breach of RSA, an enterprise that provides security, risk and compliance solutions, was disclosed on 17 March 2011 to the US Securities and Exchange Commission. In this case, the attackers used spear-phishing, in which e-mails were sent to two small groups of lower-level employees with the e-mail subject "2011 Recruitment Plan." The e-mail went to the junk mail folder, but one employee retrieved it from the junk mail folder and opened the Excel file attachment. The spreadsheet contained a zero-day exploit that installed a backdoor through an Adobe Flash vulnerability.[18, 19]

These breaches show that focusing on protecting cardholder data alone will not provide adequate security. **Figure 1** shows a comparative study of how breaches occurred for the years 2007 to 2010 based on statistical studies conducted by Verizon during these years.[20] As shown in **figure 1**, nontechnical and human factors are still regarded as a formidable threat, which the PCI DSS standard alone cannot prevent. Insertion of malware, physical theft, privilege misuse, social engineering and errors mostly fall under the nontechnical umbrella of hacking.

Figure 1—Methodology of Breaches

	2007	2008	2009	2010
Hacking	59%	64%	40%	50%
Malware	31%	38%	40%	49%
Physical theft	15%	9%	15%	29%
Privilege misuse	*	22%	48%	17%
Social engineering	*	*	28%	11%
Significant errors	62%	67%	*	*

*No studies on this type of attack are available for this year.

Source: Verizon, *2011 Data Breach Investigations Report*, USA, 2011

Compliance with PCI DSS considerably reduces risk and liability for the company, but it is not a guarantee for full protection against data breaches. According to the 2010 Verizon study on the payment card industry, organizations that suffered a data breach were 50 percent less likely to be compliant than the normal population of PCI clients.[21] However, it is not easy to become PCI-complaint. Of the merchant companies assessed by VeriSign Global Security Consulting Services, 79 percent were cited for noncompliance in their PCI audit due to failure to protect stored data.[22] Thus, it is vital for information security management programs to not only extend to other IS domains, but also to view IS security from a holistic ITG perspective rather than from an IT perspective.

ITG VIEW OF IS SECURITY

Viewing IS security from an ITG perspective, information security management is defined as the process of administering people, policies and programs, with the objective of assuring continuity of operations while maintaining strategic alignment with the organizational mission.[23] This strategic alignment requires PCI DSS v2.0 implementation not only to diverge from its focused domain and expand to its outer concentric rings of the greater IS domain, it also forces PCI DSS v2.0 to link to the organizational strategic goals, which is a major concern for IS managers. In surveys published by the IT Governance Institute (ITGI) in 2006 and 2008, the importance of strategic alignment of organizational goals with IT goals was cited as vital to the organization by 90 percent of the respondents.[24, 25] Hence, irrespective of the dynamic nature of the IS domain over the years, the issue of aligning the PCI DSS/IT goal of securing cardholder data with the higher-level organizational goals remains a concern even today. Therefore, an isolated solo approach to PCI DSS v2.0 implementation may not be effective in creating a secure IS environment for holding cardholder information.

Evaluating IT Controls

While PCI DSS has been grouped under information security standards,[26] COBIT, as a framework, incorporates perspectives of information security. COBIT is internationally recognized, accepted and widely used as a high-level governance and control framework with processes and control objectives that focus on information security. It is comprehensive and based on 41 international source

documents, providing a global perspective and a best practice point of view.[27] COBIT divides IT activities into four domains:
1. Plan and Organize (PO)
2. Acquire and Implement (AI)
3. Deliver and Support (DS)
4. Monitor and Evaluate (ME)

These domains comprise 34 processes and 222 control objectives. Incorporating one framework into another framework involves evaluation and comparison of the two. Like pieces of a jigsaw puzzle, each of the components of PCI DSS and COBIT have been analyzed, compared and contrasted to find common ground to converge on a strategic fit.

Integrating PCI DSS With COBIT

While COBIT is viewed as comprehensive and generic, PCI DSS guidelines/requirements have much depth, are specific and go into the finer details of compliance. PCI DSS v2.0 comes with six principles and 12 requirements. Each of these 12 requirements is further subdivided into lower-level requirements (with corresponding testing procedures). Experts have termed the 12 requirements as "core," "basic" and "high-level," and the lower-level requirements (with corresponding testing procedures) as "subrequirements."[28, 29, 30] As the PCI DSS v2.0 requirements follow a multilevel numbering format (e.g., 1, 1.1 and 1.1.1), for the purpose of differentiating them in this article, the 12 requirements are referred to as "core," and the lower-level requirements (with corresponding testing procedures) are referred to as "level-two" and "level-three" subrequirements. Thus, there are 45 level-two subrequirements and 75 level-three subrequirements (with corresponding testing procedures for each). In a similar manner, COBIT consists of four processes (corresponding to the six principles of PCI DSS v2.0) and 222 control objectives (corresponding to the 12 core requirements of PCI DSS v2.0). From a detailed analysis of the 222 control objectives, it can be seen that these can be segmented further to correspond to the 45 level-two subrequirements and 75 level-three subrequirements of PCI DSS v2.0. COBIT further elaborates the control objectives with "control practices" that can be equated with the "testing procedures" of PCI DSS v2.0. From the perspective of COBIT, the missing links in PCI DSS are seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability); the Responsible, Accountable, Consulted and Informed (RACI) charts; IT goals; and metrics.

Structurally, the COBIT controls and PCI DSS v2.0 have much in common. While COBIT encompasses IS entirely into four domains, 34 processes, 222 control objectives, corresponding IS control practices, and related goals and metrics, PCI DSS, when viewed from the perspective of COBIT, focuses on only a few COBIT controls (out of the 34 processes), such as DS5 *Ensure systems security.* Here, the difference between DS5 and the PCI DSS v2.0 is that the COBIT controls are broad and generic rather than specific, as in PCI DSS v2.0. Viewed from the perspective of PCI DSS, the standard corresponds to COBIT with its six principles, 12 core requirements, 120 level-two and level-three subrequirements (with corresponding testing procedures), and compliance checklist for the testing procedures.

As PCI DSS v2.0 is focused on a specific domain of IS, it covers only a small percentage of the COBIT framework; however, the standard can be incorporated either as a separate domain or within the controls. As COBIT offers flexible options for customizing its processes to suit different organizations, auditors take different approaches when implementing the framework. The rationale for using COBIT as an information security governance framework is that it integrates information security into the controls of the whole ITG framework.

While implementing COBIT, it is common to start at the high-level control processes and then define the activities, but it is not uncommon to take a more granular approach by starting at the high-level control processes, defining the corresponding detailed control objectives, defining detailed corresponding activities, and then arriving at the IT goals and metrics. At the same time, responsibility and accountability for the activities/task are addressed through the use of the RACI chart, which states that the enterprise and IT function personnel who are to be held responsible or accountable are to be informed or consulted for undertaking the activities. Finally, the activities are linked to the goals and are measured using quantitative measures that show the activities' current state in relation to the IT goal, using measures such as "degree of approval," "degree of compliance," "percent of," "level of satisfaction" and "delay between." The seven information criteria, RACI chart and specific measures provide a much more effective, efficient and focused overview of the different IS entities.

Integration of COBIT best practices within PCI DSS v2.0 entails analyzing the implementation process of both to evaluate the similarities and differences, so as to identify the areas where relevant COBIT best practices can be incorporated into PCI DSS v2.0. With this objective, a COBIT control process related to information security and a corresponding PCI DSS v2.0 requirement are used to illustrate the respective implementation process flow (**figures 2** and **3**).

Figure 2—COBIT Process DS5

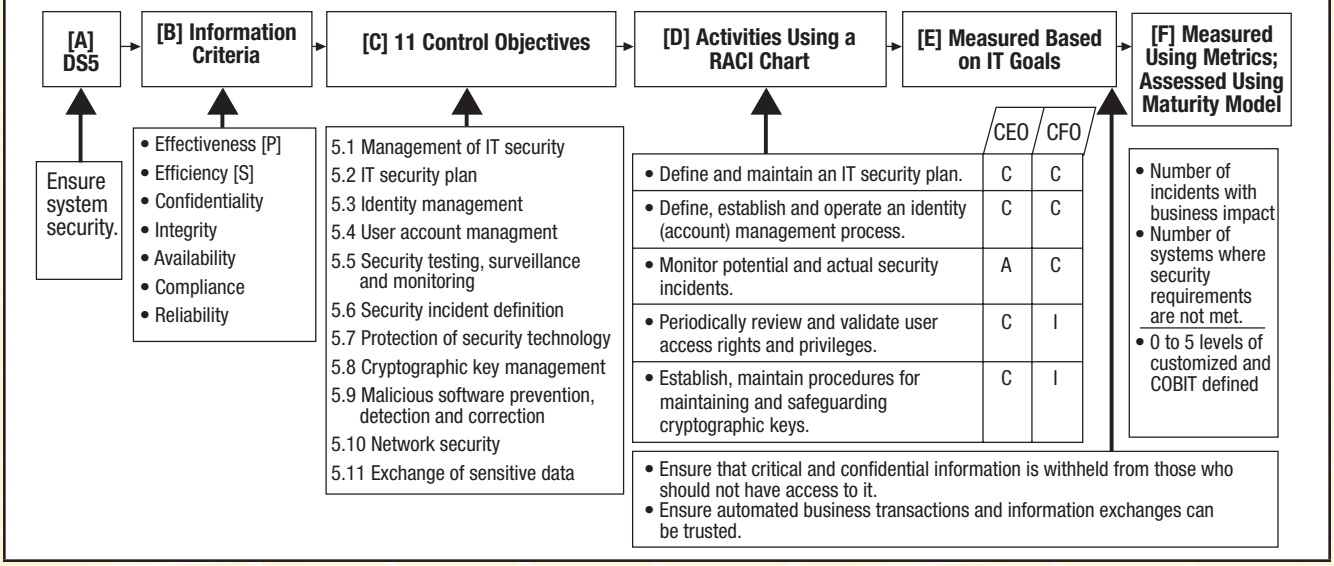
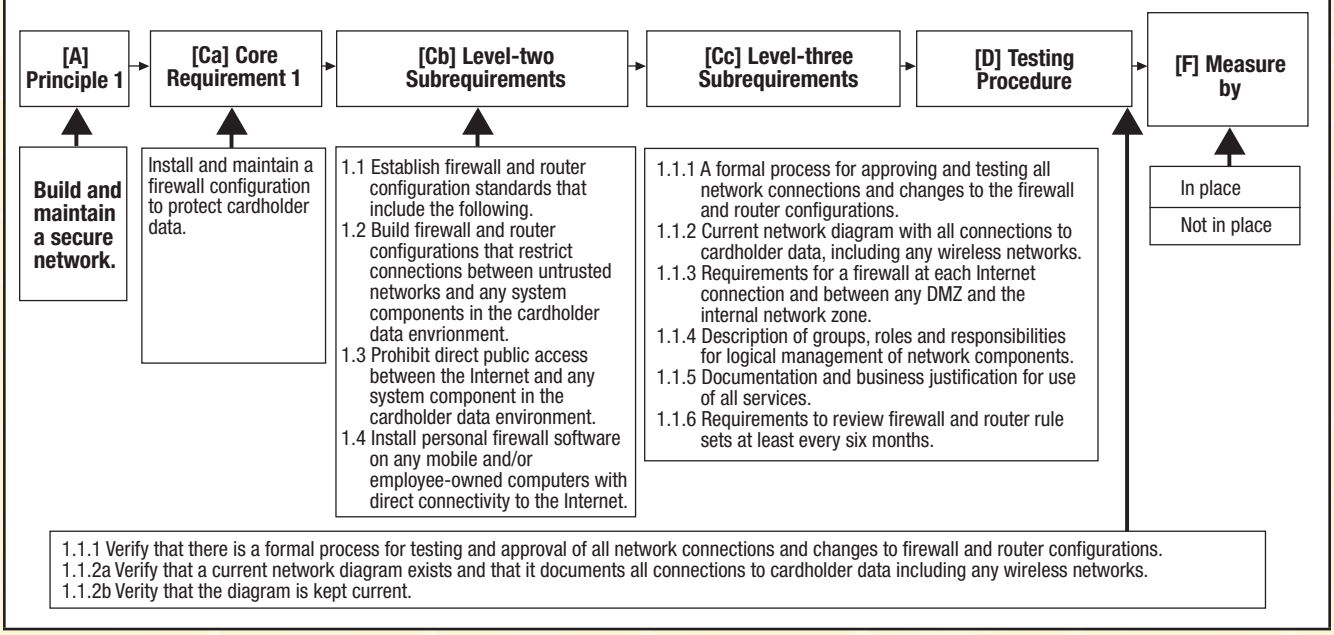


Figure 3—PCI DSS Core Requirement 1 of Principle 1



In the example, the COBIT high-level control process DS5 is evaluated using two of the seven information criteria. COBIT defines these criteria to evaluate a control process to characterize the controls and assign priority, whether any one or more of these criteria are primary or secondary to the selected control process. Since PCI DSS v2.0 does not include these criteria (see [B] in **figure 2**), a similar set of criteria has been defined in the expanded confidentiality, integrity, availability (CIA) triangle of the US National Security Telecommunications and Information Systems Security Committee (NSTISSC) model of information security, which focuses on IS security, namely confidentiality, integrity, availability, possession, utility, accuracy and authenticity.[31] This expanded CIA triangle can be applied to the six principles, 12 core requirements or the 45 level-two subrequirements of PCI DSS v2.0, which provide an IT security focus rather than an IT governance focus.

In **figure 2**, DS5 is further broken down into 11 control objectives and segregated into activities that correspond to the COBIT control objectives. Similarly, in **figure 3**, PCI DSS v2.0 principle one [A] is broken down into one requirement [Ca], and four level-two subrequirements [Cb], and six level-three subrequirements [Cc] (with corresponding testing procedure 1.1.1, 1.1.2a and 1.1.2b for level-three subrequirements 1.1.1 and 1.1.2 [D]). Here, PCI DSS v2.0 goes deeper technically than COBIT, but it is missing the RACI chart that equates to the level-two and/or level-three subrequirements and/or testing procedures.

> "PCI DSS v2.0, with just a unidimensional measurement visibility, lacks the measurement depth of COBIT."

As PCI DSS v2.0 is highly specific and detailed, incorporating the four components of the RACI chart ensures greater assurance and control with the standard. The RACI chart identifies the participants; to what degree they interact with defined activities; how they make decisions; and the positions, roles, activities, and decision areas or functions. The RACI matrix is a valuable tool for reducing the conflict between IT and business.[32]

Considering the measurement perspective ([F] in **figure 2**), COBIT uses compliance (similar to PCI DSS v2.0 "in place/not in place"), measures and metrics (such as number, rating scale, percentage and average), and the COBIT maturity model. In addition, consultants who implement COBIT also use red, amber and green color-coding to denote "noncompliant," "may be complaint" and "fully compliant," respectively. This multi-measurement approach not only provides greater visibility, it also aids in tracking the progress of a control over time. Moreover, the maturity level aids in assessing the level of the standard in relation to the industry. PCI DSS v2.0, with just a unidimensional measurement visibility, lacks the measurement depth of COBIT.

Proposed Model

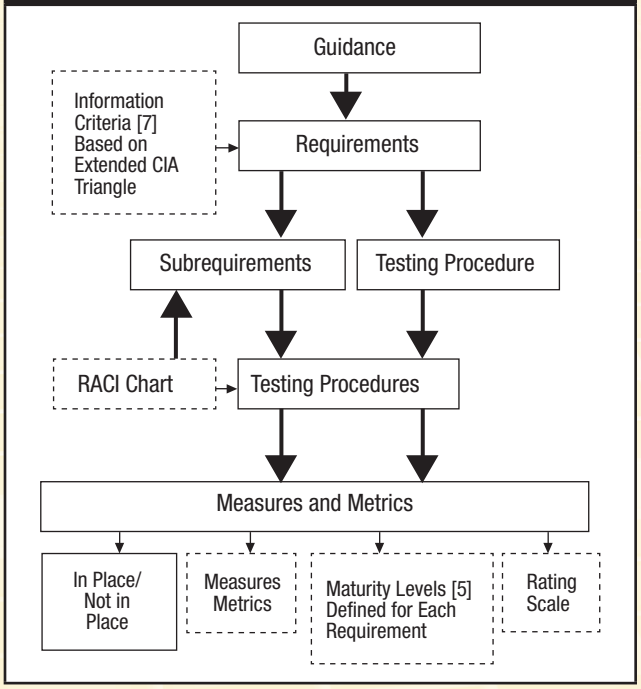
The most successful programs view PCI DSS v2.0 as a holistic cycle that needs to be continuously monitored and maintained.[33] Taking into account a holistic perspective of PCI DSS v2.0 and the gaps located in PCI DSS, the best practices of COBIT that can be incorporated into PCI DSS are:

- The expanded CIA triangle (based on the COBIT information criteria format) to provide prioritized context to the selected principles and/or requirements, which will not only provide more focus to the principle/requirement, it will also identify the criteria with which each of the PCI DSS requirements is assessed
- The RACI chart to specify roles and responsibilities, which will not only make IT personnel accountable and responsible for a particular principle/requirement, it will also provide guidance to the personnel on who is to be informed and/or consulted for each requirement
- A multidimensional measurement framework to provide a full view of the principle/process; to undertake regular trend analysis through tracking the performance of each of the principles, core requirements, and level-two and -three subrequirements over a period of time through the use of appropriate metrics and corresponding/rating scales; and to assess the maturity level of the entire PCI DSS in that company that is relative with the industry. The resulting model of PCI DSS v2.0 incorporating the relevant best practices of COBIT is given in **figure 4**.

While the expanded CIA triangle and the RACI chart can be incorporated into PCI DSS v2.0 without much effort or many amendments, incorporating a multidimensional measurement framework faces three hurdles. First, the main issue in developing the measurement framework is identifying a metrics generation model to define a set of metrics for the

core requirements, level-two subrequirements and/or level-three subrequirements because these metrics need to be aligned with the principles and the core requirements. Second, a PCI DSS v2.0 maturity model (MM) needs to be developed along the lines of the COBIT MM (**figure 5**) for each requirement (defining each of the five maturity levels in one, two or three sentences for each of the 12 core requirements). Third, for generating trend analysis reports on the level of compliance, appropriate rating scales need to be defined for

Figure 4—Extended PCI DSS V2.0



the core requirements, level-two subrequirements and level-three subrequirements or metrics that are recorded at regular intervals and tracked over time. Moreover, the huge number of lower-level quantified measures that are generated from the principles and the requirements need to be statistically aggregated and summarized to provide dashboards for different managerial levels.

CONCLUSION

Being PCI-compliant may not be enough to keep an organization's IS secure; hence, there is a need for enterprises that deal with cardholder information to integrate PCI DSS v2.0 with appropriate frameworks to fill the gaps in the

Figure 5—COBIT MM
1—Processes are *ad hoc* and disorganized.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

standard. It has been argued by practitioners and researchers alike that IT security research has failed to produce practical solutions to growing security threats.[34] Therefore, the extended PCI DSS v2.0 model proposed at a conceptual level in this article needs to be empirically tested and evaluated in different industry sectors and geographic locations to validate and generalize the model. The conceptual model can be automated into a user-friendly program using a front-end application and a back-end populated (PCI DSS v2.0) database. This model can be given to organizations for independent evaluation and the responses can be recorded, analyzed and incorporated into the current model to come up with a commercial solution for benefiting the wider business community.

ENDNOTES

1 Woolsey, Ben; Matt Schulz; "Credit Card Statistics, Industry Facts, Debt Statistics," *CreditCards.com*, 14 July 2011, *www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php*

2 *Ibid*.

3 *Ibid*.

4 Liebowitz, Matt; "2011 Set to Be Worst Year Ever for Security Breaches," *SecurityNewsDaily*, 9 June 2011, *www.securitynewsdaily.com/2011-worst-year-ever-security-breaches-0857*

5 Goodman, Seymour; Rob R. Ramery; "Global Sourcing of IT Services and Information Security: Prudence Before Playing," *Communications of the Association for Information Systems*, vol. 50, issue 20, 2007

6 Coburn, Alan; "Fitting PCI DSS Within a Wider Governance Framework," *Computer Fraud & Security*, September 2010

7 Owen, Michael; Colin Dixon; "A New Baseline for Cardholder Security," *Network Security*, June 2007

[8] Sullivan, Richard J.; "The Changing Nature of US Card Payment Fraud: Issues for Industry and Public Policy," paper presented at the Workshop on the Economics of Information Security Harvard University, 21 May 2010

[9] Everett, C.; "PCI DSS: Lack of Direction or Lack of Commitment?," *Computer Fraud & Security*, December 2009

[10] *Ibid*.

[11] Amato-McCoy, D. M.; "The Next Phase of PCI Security," *Chain Store Age*, July 2009

[12] First Data, *PCI DSS and Handling Sensitive Cardholder Data—Why You Care*, USA, 2009

[13] Symantec, Symantec Internet Security Threat Report vol. 16, 2010, *www.symantec.com/business/threatreport/*

[14] Xu, William; Gerald Grant; Hai Nguyen; Xianyi Dai; "Security Breach: The Case of TJX Companies, Inc.," *Communications of the Association for Information Systems*, vol. 23, 2008

[15] Wilson, Tim; "Hannaford, Security Industry Hunt for Cause of Massive Breach," Security Dark Reading, 18 March 2008, *www.darkreading.com/security/application-security/211201282/hannaford-security-industry-hunt-for-cause-of-massive-breach.html*

[16] Harkavy, Jerry; "Secret Software Blamed for Hannaford Breach," MSNBC.com, 28 March 2008, *www.msnbc.msn.com/id/23846014/ns/technology_and_science-security*

[17] ConsumerAffairs.com, "Hannaford Bros. Faces Class Action Over Data Breach," 21 March 2008, *www.consumeraffairs.com/news04/2008/03/hannaford_data2.html*

[18] US Department of Homeland Security (DHS), Vulnerability Summary for CVE-2011-0609, National Vulnerability Database, USA, 22 September 2011, *http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0609*

[19] Rivner, Uri; "Anatomy of an Attack," Speaking of Security, RSA, 1 April 2011, *http://blogs.rsa.com/rivner/anatomy-of-an-attack/*

[20] Verizon, *2011 Data Breach Investigations Report*, USA, 2011

[21] Verizon, *Verizon 2010 Payment Card Industry Compliance Report*, USA, 2011

[22] *Op cit*, First Data

[23] Choobineh, Joobin; Gurpreet Dhillon; Michael R. Grimaila; Jackie Rees; "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems*, vol. 20, 2007

[24] IT Governance Institute (ITGI), *IT Governance Global Status Report—2006*, USA, 2006

[25] ITGI, *IT Governance Global Status Report—2008*, USA, 2008

[26] Tsohou, Aggeliki; Spyros Kokolakis; Costas Lambrinoudakis; Stefanos Gritzalis; "A Security Standards' Framework to Facilitate Best Practices' Awareness and Conformity," *Information Management & Computer Security*, vol. 18, issue 5, 2010

[27] Lainhart, John W. IV; "COBIT: An IT Assurance Framework for the Future," *The Ohio CPA Journal*, January-March 2001

[28] Kadambi, S. Kiran; Jun, Li; Alan H. Karp; "Near-field Communication-based Secure Mobile Payment Service," paper presented at the 11th International Conference on Electronic Commerce, Taiwan, 2009

[29] Moeller, Robert; *IT Audit Control and Security*, Wiley, USA, 2010

[30] Ataya, George; "PCI DSS Audit and Compliance," *Information Security Technical Report 15*, 138–144, 2010

[31] Whitman, Michael E.; Herbert J. Mattord; *Principles of Information Security, 3rd Edition*, Course Technology Inc. USA, 2009

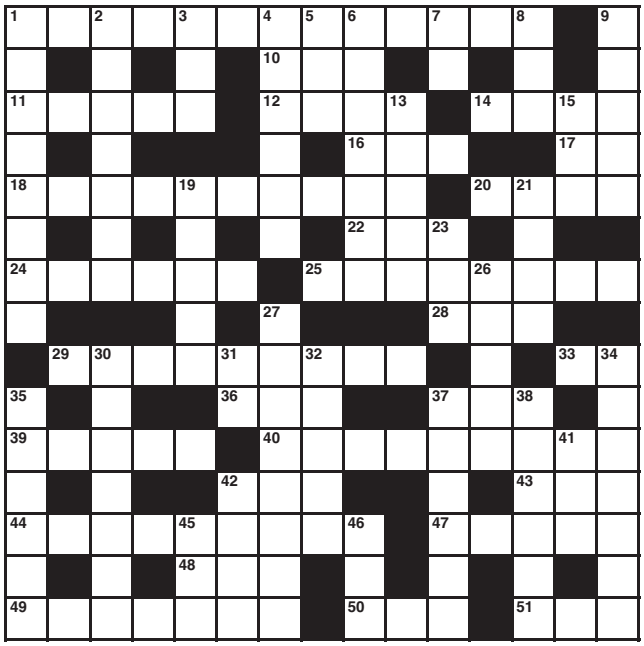
[32] Wende, Kristin; "A Model for Data Governance—Organising Accountabilities for Data Quality Management," paper presented at the 18th Australasian Conference on Information Systems, Australia, 2007

[33] Coburn, Alan; "Fitting PCI DSS Within a Wider Governance Framework," *Computer Fraud & Security*, September 2010

[34] Julisch, Klaus; "Security Compliance: The Next Frontier in Security Research," paper presented at New Security Paradigms Workshop, 2008, USA

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS
1 Elimination of redundant data
10 Trick
11 Installed infections
12 Makes a decision
14 Security marketing offering relating to access processes, abbr.
16 Brain scan, for short
17 __ licit (not legal)
18 Computer depending on its server to fulfill its traditional computational roles (2 words)
20 Software system that facilitates the creation and maintenance of a database, abbr.
22 Penpoint
24 Application combining its own resources and data with external web services
25 Make acceptable, in a security sense
28 Better
29 Access to all the enterprise data and network information (goes with 34 down, 4 words)
33 All right
36 Aussie bird
37 Add up
39 Increased
40 Give access in an ESSO system
42 Young animal
43 Fraction of a joule
44 Electrical supply backup
47 Destroy, physical documents
48 Consumption
49 Twitter user
50 Blueprint
51 Vendor relationship management, for short

DOWN
1 Period of nonoperational status
2 Goes off track
3 Software used by retailers, abbr.
4 Representative
5 Admit or acknowledge a wrongdoing or error
6 Aerial
7 Principal communications protocol used for relaying datagrams, abbr.
8 Dialoguer, for short
9 Reduces the temperature of hardware
13 _____ stone (2 words)
15 Cell phone, smart card
19 Indications that may solve a problem
21 Radar signal
23 Part of an encryption description?
26 Daily lists (2 words)
27 Information processing system
30 Erase
31 Tellurium symbol
32 _____ charge (increase the speed and power)
34 See 29 across
35 Approved spending
37 Invests (money) in one thing, so it is unavailable for others (2 words)
38 "Fault tolerant" data center categorization (2 words)
41 Bonanza find
42 Number assigned by customer service reps
45 Same old, same old
46 Memory

(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.

Go directly to the article:

Q Usage of collaboration tools is the order of the day. Smartphones have enough capacity and capability to store and process a lot of information. On the other hand, laptops and tablets can be used as devices enabling communications.

What kind of risks should organizations be cognizant about particularly when they outsource their internal processes and data processing to third parties? Can you also share your thoughts on the ideal control environment?

A Given the changes that occur in the technology and regulatory environment, the conventional controls operating in an outsourcing scenario are becoming less relevant and appropriate. Even some of the traditional controls keep evolving. Let me explain with the example of conducting background checks on employees. Conventionally, background checks were simple checks on educational qualifications and previous employment experience. Today, organisations conduct criminal verification checks, for example, to make sure that the candidates do not have any criminal history. They use hair samples, for example, of the candidates and conduct drug testing to find out whether the potential employee is a drug user.

A decade ago, social media did not exist as it does today. Imagine a scenario in which an employee tweets to the whole world about a security breach that just occurred. Loss of reputation can occur within a matter of seconds. The communication tools available on the Internet today enable instant communication to the whole world. At the same time, no company can operate today by isolating itself from social media.

Usage of desktops is decreasing as the number of laptops and tablets flood the market. Tablets are so powerful in terms of processing power and data storage capacity, and such capacities throw open a new arena of risks. On the other hand, with cheaper broadband costs and increased processing capabilities of devices, employee mobility has become the order of the day.

Laws and regulations governing personal data are also becoming more stringent, dictating increased penalties for non-compliance. Whilst laws on privacy and data protection were initially limited to US and Europe predominantly, today, even in a developing country such as India, privacy has been declared a fundamental right guaranteed by the constitution to all citizens. The outsourcing industry in countries such as India is demanding the passing of laws on privacy and protection of personal information as they see such changes as enablers to their businesses' growth. Lack of stringent laws impedes outsourcing, thereby hindering growth and expansion.

As the outsourcing industry matures, the nature of business processes that get outsourced is changing; outsourcing companies are asked to deliver higher-end work. With such jobs being outsourced, and as offshoring of the same occurs, data protection becomes more important.

Now, the question before us is whether these changes dictate any fundamental changes to the operating controls or to the control environment. Surprisingly, for a few, the answer is no. Traditional controls have not disappeared. Instead, they have been augmented and have become more effective than before.

The following are some of the key controls that continue to play a primary role in the changed environment. As usual, the list is only indicative and not exhaustive.

- The law of the land where the outsourcing happens must be conducive to outsourcing, both encouraging it and providing adequate protection of the clients who outsource. Gone are the days when jobs moved to 'cheaper destinations'; today they move to destinations where the law of the land ensures data protection.

- It is important to ensure that the sub-contracting entities by the primary outsourced service provider operate at an equivalent or a higher level of controls. Sub-contracting the work must not dilute the operating controls.
- Background checks are very important. Police recently arrested a convicted murderer from a business process outsourcing (BPO) company in India when the appeal court ordered the arrest of the accused, who was operating under a different name with fake certificates of experience and qualifications.
- Disaster recovery or business continuity arrangements have to be robust and strong enough to help the company face any crisis and successfully come out of it.

- Access controls have to be absolutely non-negotiable. With smartphone and tablet usage becoming the order of the day, it is essential to prevent any security breach or data spillage.
- New tools bring in or rather come with inherent vulnerabilities which require timely fixing.

There is no such thing as 'ideal' controls, and, as always, one size does not fit all.

CPE Quiz

Prepared by Sally Chan, CGEIT, ACIS, CMA

Take the quiz online:

QUIZ #140

Based on Volume 5, 2011—Governance, Tying Together the Three Lines of Defense

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

TRUE OR FALSE

DOUGHTY ARTICLE

1. The first line of defense related to risk governance is the enterprise's compliance and risk functions that provide independent oversight of the risk management activities of the second line of defense.
2. In the second line of defense, the board sets the risk appetite and provides oversight and audit provides independent and objective assurance on the overall effectiveness of the risk governance framework.
3. The responsibilities of the second-line functions typically include participating in the business unit's risk committees, reviewing risk reports and validating compliance to the risk management framework requirements, with the objective of ensuring that risks are actively and appropriately managed.

KIRKPATRICK ARTICLE

4. Security by abdication is when a company decides that, rather than accept the responsibility of securing and maintaining systems, people or processes, it will abdicate the responsibility by moving to the cloud.
5. Governance of any service provider should include monitoring its risk assessment results to evaluate whether its policies and procedures are comprehensive enough to identify threats to its systems. A closer look at a service provider's risk assessment and audit program discloses the matters that should be known by a customer using its services to host and manage sensitive data.

SPEED ARTICLE

6. For businesses to make prudent decisions regarding the adoption of cloud services, IT governance and risk managers need to work closely with business managers to promote understanding of key cloud computing principles and to help establish effective governance practices.
7. With cloud computing, customers have more visibility as to how secure the service is and regarding the causes of outages or issues of reliability.
8. Private clouds can be provided to businesses in generally two ways: either by having the business's systems firewalled off from everyone else's, or by having the business's systems virtually separated from others using an authenticated and encrypted environment within a public cloud.
9. One of the key benefits of operating the entire production application using public cloud-based Platform as a Service (PaaS) or Software as a Service is the reduced cost of maintaining production capacity that is underutilized during nonpeak periods.
10. One of the key risk factors to consider when using cloud Infrastructure as a Service or PaaS for developing new services during early release iterations, as features are evolving and demand is scaling, is data protection in the cloud when testing the use of live data or undertaking recovery activities.

ETGES AND RUYSAM ARTICLE

11. Solid identity management (IDM) governance must be applied to ensure that the relevant stakeholders are involved in the definition of principles and goals governing how business roles are managed within the organization. The ongoing message must be that IDM is a business issue affecting compliance, risk, privacy and cost efficiencies.
12. Unlike other complex technologies, such as customer relationship management and enterprise resource planning, IDM solutions do not touch and influence the way key revenue-generating business processes function.
13. Technology vendors will have a limited ability to understand the business issues driving the acquisition of the IDM solution by an organization and will not have insight into its business processes or the skill sets required to integrate and adjust its existing systems. The acquiring organization must be prepared to assess its own capabilities and gaps against best practices for managing roles and identities.

MARKS ARTICLE

14. The US Dodd-Frank Act identifies a central agency or authority that will be accountable for ensuring compliance to the Act. As a result, the potential for conflicting and inconsistent requirements between agencies will not exist.
15. The Act establishes an oversight group, called the Financial Stability Oversight Council. The council is responsible for identifying and responding to emerging risk throughout the financial system.
16. The Act requires hedge funds and private equity advisors to register with the US Securities and Exchange Commission as investment advisors and to provide information about their trades and portfolios necessary to assess systemic risk.

ISACA Journal

CPE Quiz

Based on Volume 5, 2011—Governance, Tying Together the Three Lines of Defense

Quiz #140 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC# _____

Quiz #140

True or False

DOUGHTY ARTICLE

1. _____
2. _____
3. _____

KIRKPATRICK ARTICLE

4. _____
5. _____

SPEED ARTICLE

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

ETGES AND RUYSAM ARTICLE

11. _____
12. _____
13. _____

MARKS ARTICLE

14. _____
15. _____
16. _____

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.

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

Standards Guidelines Tools and Techniques

ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

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

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

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

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

The titles of issued standards documents are:

IT Audit and Assurance Standards

S1 Audit Charter Effective 1 January 2005
S2 Independence Effective 1 January 2005
S3 Professional Ethics and Standards Effective 1 January 2005
S4 Professional Competence Effective 1 January 2005
S5 Planning Effective 1 January 2005
S6 Performance of Audit Work Effective 1 January 2005
S7 Reporting Effective 1 January 2005
S8 Follow-up Activities Effective 1 January 2005
S9 Irregularities and Illegal Acts Effective 1 September 2005
S10 IT Governance Effective 1 September 2005
S11 Use of Risk Assessment in Audit Planning Effective 1 November 2005
S12 Audit Materiality Effective 1 July 2006
S13 Using the Work of Other Experts Effective 1 July 2006
S14 Audit Evidence Effective 1 July 2006
S15 IT Controls Effective 1 February 2008
S16 E-commerce Effective 1 February 2008

IT Audit and Assurance Guidelines

G1 Using the Work of Other Experts Effective 1 March 2008
G2 Audit Evidence Requirement Effective 1 May 2008
G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
G5 Audit Charter Effective 1 February 2008
G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
G7 Due Professional Care Effective 1 March 2008
G8 Audit Documentation Effective 1 March 2008
G9 Audit Considerations for Irregularities Effective 1 September 2008
G10 Audit Sampling Effective 1 August 2008
G11 Effect of Pervasive IS Controls Effective 1 August 2008
G12 Organisational Relationship and Independence Effective 1 August 2008
G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
G14 Application Systems Review Effective 1 October 2008
G15 Audit Planning Revised Effective 1 Ma1 2010
G16 Effect of Third Parties on an Organisation's IT Controls Effective 1 March 2009
G17 Effect of Non-audit Role on the IS Auditor's Independence Effective 1 May 2010
G18 IT Governance Effective 1 May 2010
G19 Withdrawn 1 September 2008
G20 Reporting Effective Effective 16 September 2010
G21 Enterprise Resource Planning (ERP) Systems Review Effective 16 September 2010
G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
G24 Internet Banking Effective 1 August 2003
G25 Review of Virtual Private Networks Effective 1 July 2004
G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
G27 Mobile Computing Effective 1 September 2004
G28 Computer Forensics Effective 1 September 2004
G29 Post-implementation Review Effective 1 January 2005
G30 Competence Effective 1 June 2005
G31 Privacy Effective 1 June 2005
G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
G33 General Considerations for the Use of the Internet Effective 1 March 2006
G34 Responsibility, Authority and Accountability Effective 1 March 2006
G35 Follow-up Activities Effective 1 March 2006
G36 Biometric Controls Effective 1 February 2007
G37 Configuration and Release Management Effective 1 November 2007
G38 Access Controls Effective 1 February 2008
G39 IT Organisation Effective 1 May 2008
G40 Review of Security Management Practices Effective 1 October 2008
G41 Return on Security Investment (ROSI) Effective 1 May 2010
G42 Continuous Assurance Effective 1 May 2010

IT Audit and Assurance Tools and Techniques

P1 IS Risk Assessment Measurement Effective 1 July 2002
P2 Digital Signatures and Key Management Effective 1 July 2002
P3 Intrusion Detection Systems (IDS) Review Effective 1 August 2003
P4 Malicious Logic Effective 1 August 2003
P5 Control Risk Self-assessment Effective 1 August 2003
P6 Firewalls Effective 1 August 2003
P7 Irregularities and Illegal Acts Effective 1 December 2003
P8 Security Assessment—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
P9 Evaluation of Management Controls Over Encryption Methodologies Effective 1 January 2005
P10 Business Application Change Control Effective 1 October 2005
P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

Standards for Information System Control Professionals Effective 1 September 1999

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

Code of Professional Ethics Effective 1 January 2011

Advertisers/Web Sites

CA Technologies	*www.security.com*	**Back Cover**
ExamMatrix	*www.www.ExamMatrix.com/ISJ*	**16**
Regis University	*www.RegisDegrees.com/ISACA*	**1**

Leaders and Supporters

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

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

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

The *ISACA Journal* has been made aware that in the JournalOnline, volume 5, 2012, article "An Introduction to Information Security Management in Health Care Organizations," text directly quoted from ISO 27799 was inadvertently attributed as indirect quotations. The *Journal* regrets the situation and any inconvenience it may have caused its readers.

Code	Title		Nonmember	Member
2012 CISA® EXAM REFERENCE MATERIALS				
◆ To prepare for the June or December 2012 CISA exam, order ◆				
CISA Review Manual 2012*				
CRM-12	English Edition		$135.00	$105.00
CRM-12C	Chinese Simplified Edition		135.00	105.00
CRM-12F	French Edition		135.00	105.00
CRM-12I	Italian Edition		135.00	105.00
CRM-12J	Japanese Edition		135.00	105.00
CRM-12S	Spanish Edition		135.00	105.00
CISA Review Questions, Answers & Explanations Manual 2012 Supplement*				
QAE-12ES	English Edition	(100 Questions)	60.00	40.00
QAE-12CS	Chinese Simplified Edition	(100 Questions)	60.00	40.00
QAE-12FS	French Edition	(100 Questions)	60.00	40.00
QAE-12IS	Italian Edition	(100 Questions)	60.00	40.00
QAE-12JS	Japanese Edition	(100 Questions)	60.00	40.00
QAE-12SS	Spanish Edition	(100 Questions)	60.00	40.00
CISA Review Questions, Answers & Explanations Manual 2011*				
QAE-11	English Edition	(900 Questions)	130.00	100.00
QAE-11C	Chinese Simplified Edition	(900 Questions)	130.00	100.00
QAE-11G	German Edition	(900 Questions)	130.00	100.00
QAE-11I	Italian Edition	(900 Questions)	130.00	100.00
QAE-11J	Japanese Edition	(900 Questions)	130.00	100.00
QAE-11S	Spanish Edition	(900 Questions)	130.00	100.00
CISA Review Questions, Answers & Explanations Manual 2011 Supplement*				
QAE-11ES	English Edition	(100 Questions)	60.00	40.00
QAE-11CS	Chinese Simplified Edition	(100 Questions)	60.00	40.00
QAE-11FS	French Edition	(100 Questions)	60.00	40.00
QAE-11IS	Italian Edition	(100 Questions)	60.00	40.00
QAE-11JS	Japanese Edition	(100 Questions)	60.00	40.00
QAE-11SS	Spanish Edition	(100 Questions)	60.00	40.00
CISA Practice Question Database v12 (1,100 Questions)*				
CDB-12	CD-ROM—English Edition		225.00	185.00
CDB-12W	Download—English Edition (no shipping charges apply to download)		225.00	185.00
CDB-12S	CD-ROM—Spanish Edition		225.00	185.00
CDB-12SW	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
2012 CISM® EXAM REFERENCE MATERIALS				
◆ To prepare for the June or December 2012 CISM exam, order ◆				
CISM Review Manual 2012*				
CM-12	English Edition		115.00	85.00
CM-12S	Spanish Edition		115.00	85.00
CISM Review Questions, Answers & Explanations Manual 2012*				
CQA-12	English Edition	(700 Questions)	90.00	70.00
CQA-12J	Japanese Edition	(700 Questions)	90.00	70.00
CQA-12S	Spanish Edition	(700 Questions)	90.00	70.00
CISM Review Questions, Answers & Explanations Manual 2012 Supplement*				
CQA-12ES	English Edition	(100 Questions)	60.00	40.00
CQA-12JS	Japanese Edition	(100 Questions)	60.00	40.00
CQA-12SS	Spanish Edition	(100 Questions)	60.00	40.00
CISM Practice Question Database v12 (800 Questions)*				
MDB-12	CD-ROM – English Edition		160.00	120.00
MDB-12W	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
2012 CGEIT EXAM REFERENCE MATERIALS				
◆ To prepare for the June or December 2012 CGEIT exam, order ◆				
CGM-12*	CGEIT Review Manual 2012		115.00	85.00
CGQ-12ES*	CGEIT Review Questions, Answers & Explanations Manual 2012 Supplement (100 Questions)		60.00	40.00
CGQ-11*	CGEIT Review Questions, Answers & Explanations Manual 2011 English Edition (60 Questions)		60.00	40.00
CACG*	Candidate's Guide to the CGEIT Exam and Certification (No charge to paid CGEIT exam registrants)		15.00	5.00
2012 CRISC EXAM REFERENCE MATERIALS				
◆ To prepare for the June or December 2012 CRISC exam, order ◆				
CRR-12*	CRISC Review Manual 2012		115.00	85.00
CRQ-12ES*	CRISC Review Questions, Answers & Explanations Manual 2012 Supplement (100 Questions)		60.00	40.00
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

Code	Title	Nonmember	Member
COBIT®			
CB4.1*	COBIT 4.1, Print Format	190.00	75.00
COBIT and Application Controls: A Management Guide			
WCAC*	E-book—PDF format (purchase online only)	55.00	FREE
CAC*	Print format	75.00	35.00
CBX*	COBIT 4.1 Excerpt	5.00	5.00
CPS2*	COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition	110.00	55.00
CBQ2*	COBIT Quickstart, 2nd Edition	110.00	55.00
COBIT Assessor Guide: Using COBIT 4.1			
WCAG*	E-book—PDF format (purchase online only)	80.00	30.00
CAG*	Print format	100.00	50.00
COBIT Process Assessment Model (PAM): Using COBIT 4.1			
WCPAM*	E-book—PDF format (purchase online only)	40.00	FREE
CPAM*	Print format	50.00	30.00
COBIT Self-assessment Guide: Using COBIT 4.1			
WCSAG*	E-book—PDF format (purchase online only)	30.00	FREE
CSAG*	Print format	40.00	25.00
CBSB2*	COBIT Security Baseline, 2nd Edition	40.00	20.00
	Additional Set (5 each) Reference Cards		
	HRC2 Home Users	3.00	2.00
	PRC2 Professional Users	3.00	2.00
	MRC2 Managers	3.00	2.00
	ERC2 Executives	3.00	2.00
	SRC2 Senior Executives	3.00	2.00
	BRC2 Board of Directors/Trustees	3.00	2.00
COBIT User Guide for Service Managers			
WCUG*	E-book—PDF format (purchase online only)	35.00	FREE
CUG*	Print format	50.00	20.00
CB4A*	IT Assurance Guide: Using COBIT	165.00	55.00
ITG9*	Implementing and Continually Improving IT Governance	115.00	55.00
SDG*	SharePoint Deployment and Governance Using COBIT 4.1: A Practical Approach	70.00	30.00
COBIT Online 4.1			
COLB*	Annual Full Subscription + Benchmarking (purchase online at *www.isaca.org/cobitonline*) ISACA members SAVE 75%	400.00	200.00 50.00
	▶ Visit *www.isaca.org/cobitonline* for additional information. ◀		
COBIT Mappings			
WCMCMM*	Mapping of CMMI for Development V1.2 With COBIT 4.0	25.00	Free
WCMISO*	Mapping of ISO/IEC 17799: 2005 With COBIT 4.0	25.00	Free
WCMIT3*	Mapping of ITIL V3 With COBIT® 4.1	25.00	Free
WCMNIST*	Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1	25.00	Free
WCMPMB*	Mapping of PMBOK to COBIT 4.0	25.00	Free
WCMSEI*	Mapping of SEI's CMM for Software to COBIT 4.0	25.00	Free
WCMTOG*	Mapping of TOGAF 8.1 With COBIT 4.0	40.00	Free
WCMFF*	Mapping FFIEC with COBIT 4.1	25.00	Free
WCM20000*	Mapping of ISO/IEC 20000 with COBIT 4.1	25.00	Free
WCMCMM2*	Mapping of CMMI for Development V1.2 with COBIT 4.1	25.00	Free

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

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

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

Code	Title	Nonmember	Member
VAL IT™			
Enterprise Value: Governance of IT Investments			
VITM*	Getting Started With Value Management	40.00	25.00
VITF2*	The Val IT Framework 2.0	90.00	45.00
VITB2*	The Business Case Guide—Using Val IT 2.0	40.00	25.00
VITAG*	Value Management Guidance for Assurance Professionals—Using Val IT 2.0	40.00	25.00
VITS2*	Complete Set	185.00	105.00
39-CRC	The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results	86.00	76.00
5-RO	A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance	105.00	95.00
RISK IT AND RISK RELATED TOPICS			
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	84.00	74.00
11-CRC8	How to Complete a Risk Assessment in 5 Days or Less	95.00	85.00
84-WRM	Information Technology Risk Management in Enterprise Environments	105.00	95.00
2-HBS	IT Risk: Turning Business Threats Into Competitive Advantage	45.00	35.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

SUPPLEMENT

Code	Title	Nonmember	Member
RISK IT AND RISK RELATED TOPICS *(cont.)*			
1-HHOP	The Operational Risk Handbook for Financial Companies	89.00	79.00
5-PL	Risk Management & Risk Assessment	105.00	95.00
55-WRCS	Risks, Controls, and Security: Concepts and Applications	129.00	119.00
RITF*	The Risk IT Framework	95.00	45.00
RITPG*	The Risk IT Practitioner Guide	115.00	55.00
AUDIT, CONTROL AND SECURITY—ESSENTIALS			
48-CRC	Access Control, Security, and Trust: A Logical Approach	100.00	90.00
1-IT9	Accounting Information Systems, 9th Edition	258.00	248.00
70-WAS	Accounting Information Systems: Controls and Processes	183.00	173.00
6-PAW	Applied Security Visualization	65.00	55.00
93-WAAS	Auditing and Assurance Services: Understanding the Integrated Audit	223.00	213.00
6-PL	Auditing IT Infrastructures	105.00	95.00
76-WSL	Build Your Own Security Lab: A Field Guide for Network Testing	60.00	50.00
43-CRC	Building an Effective Information Security Policy Architecture	90.00	80.00
31-CRC	Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI	140.00	130.00
79-WCAF	Computer Aided Fraud Prevention and Detection: A Step by Step Guide	74.00	64.00
4-IGI	Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions	110.00	100.00
51-CRC	Data Protection: Governance, Risk Management, and Compliance	82.00	72.00
50-WPM6	Effective Project Management: Traditional, Agile, Extreme, 6th Edition	70.00	60.00
1-ABES	Enterprise Security for the Executive: Setting the Tone from the Top	45.00	35.00
92-WIA	The Essential Guide to Internal Auditing, 2nd Edition	65.00	55.00
71-WCF	Essentials of Corporate Fraud	58.00	48.00
82-WACL	Fraud Analysis Techniques Using ACL	221.00	211.00
62-WFC	Fraud Casebook: Lessons from the Bad Side of Business	84.00	74.00
10-EL	GFI Network Security and PCI Compliance Power Tools	73.00	63.00
36-CRC	How to Achieve 27001 Certification: An Example of Applied Compliance Management	100.00	90.00
2-W404	How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control, 3rd Edition	100.00	90.00
7-ART	Implementing the ISO/IEC 27001 Information Security Management System Standard	105.00	95.00
2-ABA	Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists	106.00	96.00
83-WIS	Information Storage and Management: Storing, Managing, and Protecting Digital Information	70.00	60.00
4-CRC3	Information Technology Control and Audit, 3rd Edition	100.00	90.00
90-WACS	IT Audit, Control, and Security	95.00	85.00
IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud			
WITCOC*	E-book – PDF Format (purchase online only)	50.00	FREE
ITCOC*	Print Format	60.00	35.00
STDPK*	IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals	20.00	15.00
WITAF*	ITAF: A Professional Practices Framework for IT Assurance e-book—PDF (purchase online only)	45.00	FREE
15-MIT2	IT Auditing Using Controls to Protect Information Assets, 2nd Edition	80.00	70.00
IT Control Objectives for Basel II			
WITCOB*	E-book—PDF Format (purchase online only)	35.00	FREE
ITCOB*	Print Format	50.00	20.00
PSOX*	IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition	7.00	7.00
9-SYN	The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments	83.00	73.00
22-MSM	IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data	60.00	50.00
6-ITSOC	IT Strategic and Operational Controls	70.00	60.00
1-IIA	A New Auditor's Guide to Planning, Performing, and Presenting IT Audits	80.00	70.00
5-ART	Outsourcing Information Security	103.00	93.00
7-SYN9	PCI Compliance, Second Edition	70.00	60.00
1-RIA	Practical IT Auditing with current Supplement	445.00	435.00
2-SAPP	SAP Security and Risk Management, 2nd Edition	80.00	70.00
1-IGI	Securing the Information Infrastructure	110.00	100.00
5-PSM	Security Metrics: Replacing Fear, Uncertainty, and Doubt	70.00	60.00
2-WG	Standard for Auditing Computer Applications	509.00	499.00
2-BAY*	Stepping Through the InfoSec Program	45.00	35.00
AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS			
18-MAO	Applied Oracle Security: Developing Secure Database and Middleware Environments	70.00	60.00
4-DC	Audit Guidelines for DB2	80.00	70.00
1-SAPP	COBIT and the Sarbanes-Oxley Act	45.00	35.00
88-WFA	Fraud Auditing and Forensic Accounting, 4th Edition	85.00	75.00
10-ART	Identity Management: Concepts, Technologies, and Systems	110.00	100.00
Linux: Security, Audit and Control Features			
WLIN*	E-book—PDF Format (purchase online only)	30.00	15.00
PLIN*	Print Format	50.00	35.00
Managing Risk in Wireless Environment: Security, Audit and Control Issues			
WW*	E-book—PDF Format (purchase online only)	40.00	20.00
PW*	Print Format	50.00	35.00
OS390*	OS/390-z/OS Security, Audit and Control Features	70.00	55.00
29-ST4	A Practical Guide to IBM i and i5/OS Security and Compliance	89.00	79.00
1-MPPI	Protecting Industrial Control Systems from Electronic Threats	100.00	90.00
ODB9*	Security, Audit and Control Features Oracle® Database, 3rd Edition	55.00	40.00
ISOA3*	Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition	75.00	60.00
ISPS3*	Security, Audit and Control Features Oracle® PeopleSoft®, 3rd Edition	____	____
ISAP3*	Security, Audit and Control Features SAP® ERP, 3rd Edition	75.00	60.00
3-JBSS	Security Strategies in Windows Platforms and Applications	100.00	90.00
3-EL	Wireless Operational Security	95.00	85.00
NON-ENGLISH RESOURCES			
2-TCA	Administración de la Seguridad de Información	55.00	45.00
CISA Examination Reference Material			
	Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the June or December 2012 CISA exam—see page S5		
CISM Examination Reference Material			
	Study aids available in Japanese and Spanish for the June or December 2012 CISM exam—see page S5		
	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.ch*		
	COBIT 4.1 Edition, available at the following web site Chinese Simplified Edition - *www.isaca.org/getcobit* French Edition—*www.afai.fr* Hebrew Edition - *www.isaca.org.il* Hungarian Edition—*www.isaca.org/getcobit* Italian Edition - *www.aiea.it* Japanese Edition—*www.isaca.org/getcobit* Portuguese Edition—*www.isaca.org/getcobit* Russian Edition—*www.isaca-russia.ru* Spanish Edition—*www.isaca.org/getcobit*		
1-AOCF	Computación Forense: Descubriendo los Rastros Informáticos	42.00	32.00
Meycor COBIT Suite			
	Meycor CobiT es un software completo e integrado para la implementación de COBIT como una herramienta para el Buen Gobierno de la TI, Seguridad de la TI o Aseguramiento de la TI según COBIT 4.1. (see *www.isaca.org/nonenglishbooks* para descripción y precios)		
1-TCA	Principios de Auditoría y Control de Sistemas de Información	40.00	30.00
INTERNET AND RELATED SECURITY TOPICS			
19-M24	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	60.00	50.00
45-CRC	Cloud Computing: Implementation, Management, and Security	90.00	80.00
9-EL	Computer and Information Security Handbook	130.00	120.00
11-EL	Cyber Attacks: Protecting National Infrastructure	70.00	60.00
1-CAP3	Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 3rd Edition	48.00	38.00
2-SCC	Cybercrimes: A Multidisciplinary Analysis	199.00	189.00
34-CRC	Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition	90.00	80.00
4-MGH3	Gray Hat Hacking: The Ethical Hakers Handbook, 3rd Edition	70.00	60.00
1-MHF	Hacking Exposed Computer Forensics Secrets and Solutions, 2nd Edition	60.00	50.00
2-MCG6	Hacking Exposed: Network Security Secrets & Solutions, 6th Edition	60.00	50.00
23-MHE	Hacking Exposed Web Applications, 3rd Edition	60.00	50.00
17-MHE2	Hacking Exposed Wireless: Wireless Security Secrets & Solutions, 2nd Edition	60.00	50.00
49-CRC	Honeypots: A New Paradigm to Information Security	150.00	140.00
29ST-3	The Little Black Book of Computer Security, 2nd Edition	35.00	25.00
21-MMS	Mobile Application Security	60.00	50.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00
10-MOC2	Network Security: The Complete Reference, 2nd Edition	80.00	70.00
59-WNS	Network Security Fundamentals	82.00	72.00
1-GL	NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning	60.00	50.00
1-WCNR	No Root for You: A Series of Tutorials, Rants and Raves, and Other Random Nuances Therein	33.00	23.00
56-WPC	Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft	106.00	96.00
1-HA	Scrappy Information Security: The Easy Way to Keep the Cyber Wolves at Bay	30.00	20.00
30-CRC	Securing Converged IP Networks	100.00	90.00
24-MSIEM	Security Information and Event Management (SIEM) Implementation	75.00	65.00
1-OSM	Security Monitoring	55.00	45.00
2-JBSF	System Forensics, Investigation, and Response	112.00	102.00
6-EL	XSS Exploits—Cross Site Scripting Attacks and Defense	73.00	63.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

Code	Title	Nonmember	Member
	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
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	60.00	50.00
6-SYN	Business Continuity and Disaster Recovery Planning for IT Professionals	70.00	60.00
BMIS*	The Business Model for Information Security	60.00	45.00
41-CRC	Business Resumption Planning, 2nd Edition	108.00	98.00
54-WCIO2	CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition	75.00	65.00
WCCS*	Creating a Culture of Security (e-book)	50.00	FREE
32-CRC	Crisis Management Planning and Execution	90.00	80.00
37-CRC	Digital Privacy: Theory, Technologies, and Practices	90.00	80.00
2-IGI	Emerging Topics and Technologies in Information Systems	205.00	195.00
89-WEG	Empowering Green Initiatives with IT: A Strategy and Implementation Guide	60.00	50.00
9-ART	Enterprise Information Security and Privacy	109.00	99.00
1-CMP	Enterprise Security Architecture: A Business-Driven Approach	97.00	87.00
60-WESO	Essentials of Sarbanes-Oxley	45.00	35.00
23-WIT	The Executive's Guide to Information Technology, 2nd Edition	110.00	100.00
10-VH	Foundations of IT Service Management Based on ITIL® V3	66.00	56.00
3-VH	Frameworks for IT Management	66.00	56.00
85-WF101	Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition	65.00	55.00
64-WGRC	Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices	173.00	163.00
42-CRC	The Green and Virtual Data Center	90.00	80.00
7-ITGR	Green IT in Practice, 2nd Edition	60.00	50.00
20-MHE	Hacking Exposed Malware and Rootkits: Malware & Rootkits Secrets & Solutions	60.00	50.00
67-WHF	Human Factors in Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation	62.00	52.00
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
46-CRC	Implementing the Project Management Balanced Scorecard	90.00	80.00
10-ITISQ	Implementing Service Quality based on ISO/IEC 20000	35.00	25.00
28-CRC	Information Security: Design, Implementation, Measurement and Compliance	110.00	100.00
2-ITG*	Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition	7.00	7.00
Information Security Governance: Guidance for Information Security Managers			
3-ITG*	Information Security Governance: Guidance for Information Security Managers	50.00	25.00
W3ITG*	E-book—PDF Format (purchase online only)	45.00	FREE
WSH*	Information Security Harmonisation: Classification of Global Guidance (E-book—PDF format purchase online only)	40.00	FREE
1-BS12	Information Security Policies Made Easy, Version 12	805.00	795.00
2-PS3	Information Security Roles & Responsibilities Made Easy, Version V3	505.00	495.00
50-CRC	Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement	90.00	80.00
3-IGI	Information Technology Governance and Service Management: Frameworks and Adaptations	205.00	195.00
80-WITM8	Information Technology for Management: Improving Strategic and Operational Performance, 8th Edition	212.00	202.00
81-WIC	Internal Controls Policies and Procedures	95.00	85.00
5-VH	ISO/IEC 20000: A Pocket Guide	33.00	23.00
12-VH	IT Financial Management	66.00	56.00
3-ITGD	IT Governance: Guidelines for Directors	90.00	80.00
4-ITIG	IT Governance: A Pocket Guide	26.00	16.00
5-AS12	IT Governance: Policies & Procedures, 2012 Edition	255.00	245.00
WGPM*	IT Governance and Process Maturity (E-Book—purchase online only)	30.00	Free
8-ITHP	IT Governance to Drive High Performance: Lessons from Accenture	25.00	15.00
5-ITOC	IT Outsourcing Contracts: A Legal and Practical Guide	41.00	31.00
11-VH	IT Outsourcing: Part 1 Contracting the Partner	42.00	32.00
25-MIPM	IT Project Management: On Track from Start to Finish, 3rd Edition	60.00	50.00
91-WKPI	Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs, 2nd Edition	60.00	50.00
40-CRC	Leading IT Projects: The IT Manager's Guide	96.00	86.00
26-MDM	Master Data Management and Data Governance, 2nd Edition	70.00	60.00
9-VH	MOF—Microsoft Operations Framework V4.0: A Pocket Guide	33.00	23.00
MIC*	Monitoring Internal Control Systems and IT	70.00	55.00
2-ITO	Outsourcing IT: A Governance Guide	82.00	72.00
3-JR	A Practical Guide to Reducing IT Costs	55.00	45.00
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
5-SYN	Sarbanes-Oxley IT Compliance Using Open Source Tools, 2nd Edition	73.00	63.00
Security Awareness: Best Practices to Secure Your Enterprise			
WSA*	E-book—PDF Format (purchase online only)	35.00	20.00
PSA*	Print Format	50.00	35.00
75-WSO	The Sarbanes-Oxley Section 404 Implementation Toolkit: Practice Aids for Managers and Auditors, 2nd Edition	105.00	95.00
13-VH	The Service Catalog	66.00	56.00
58-WSOA	Service Oriented Architecture: A Planning and Implementation Guide for Business and Technology	70.00	60.00
73-WSOA	Service Oriented Architecture Field Guide for Executives	60.00	50.00
9-ITSIA	Swanson on Internal Auditing: Raising the Bar	60.00	50.00
77-WTS	Technology Scorecards: Aligning IT Investments with With Business Performance	60.00	50.00
4-ITG*	Unlocking Value: An Executive Primer on the Critical Role of IT Governance	7.00	7.00
2-ITPI	Visible OPS Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps	32.00	22.00
44-CRC	Vulnerability Management	90.00	80.00
87-WWC	World Class IT: Why Businesses Succeed When IT Triumphs	48.00	38.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

FOUR EASY WAYS TO PLACE AN ORDER:

Order online at *www.isaca.org/bookstore*

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

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

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.

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

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.

DELIVERY

Orders normally ship within 2-3 business days upon receipt of payment. Once shipped, delivery time can vary between 2-7 business days.

CUSTOMS

Customers are responsible for any custom duties/taxes/VAT charges levied by the country of destination. See *www.isaca.org/shipping* for further information.

SUPPLEMENT

ISACA®
Trust in, and value from, information systems

Customer Order Form

Order Online at *www.isaca.org/bookstore*

OFFICE USE ONLY

Vol. 1-12

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

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

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

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%	
California (CA), New Jersey (NJ), Tennessee (TN)—7%	
Illinois (IL)—9%	
For all orders please include shipping and handling charge—see chart below.	
TOTAL	

Payment Information—Prepayment Required

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

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

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

Credit Card # _____

Exp. Date _____

Print Cardholder Name _____

Signature of Cardholder _____

Shipping & Handling Rates for Orders

All orders outside the US are shipped Federal Express Priority.

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

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

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

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

What Does Your Future Hold? Find Out Next Summer.

An Exclusive Leadership Forum for Business and Information Technology Professionals

ISACA's World Congress

INSIGHTS 2012

25-27 June 2012 | San Francisco, CA

A unique opportunity to collaborate with fellow thought leaders on strategies for the effective integration of business and technology.

Limited seats available, to learn more visit:

www.isaca.org/2012insights-Journal

ISACA®

Trust in, and value from, information systems

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

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

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

Identities. Access. Information. Compliance.

A smarter, more secure solution.

That's the power of know.

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

we can

ca technologies