ISACA® Journal

VOLUME 3, 2013

Big Data

Featured articles:

What Is Big Data and What Does It Have to Do With IT Audit?

Considerations for Ensuring Security of Research Data in a Federally Regulated Environment

IT Security Responsibilities Change When Moving to the Cloud

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

A NEW ERA

EuroCACS/ISRM CONFERENCE 16-18 September London, England

A NEW EDGE

Make plans today to attend EuroCACS/ISRM 2013 featuring world-class networking, customised learning opportunities and special guest speakers David Lacey and Amar Singh.

David Lacey will lead a panel discussion entitled Look into the Future for Information Security – Trends, Technologies and Threats.

David Lacey has over 25 years experience directing information security for leading organisations such as Shell, Royal Mail and the British Foreign Office. He is an independent researcher, writer and consultant, and the author of "Managing the Human Factor for Information Security", "Managing Security in Outsourced and Offshored Environments" and "Business Continuity Management for Small and Medium Sized Companies". David is an honorary fellow of the Jericho Forum, a member of IOActive's Strategic Advisory Board, and a member of the Infosecurity Europe "Hall of Fame".

Opening keynote speaker, Amar Singh, will give his insights on the future of cloud computing.

Amar Singh is breaking the mould of the typical CISO and is making a mark in the global InfoSec community as a leading, innovative, and benchmark-setting Information Security Executive. He brings a unique fusion of pragmatism, practicality, with a healthy dose of proportionate paranoia to his work and is commanding the information security and assurance space with his inspiring approach to Information Security Governance, Risk and Compliance.

euro cacs℠ INFORMATION SECURITY AND RISK MANAGEMENT CONFERENCE

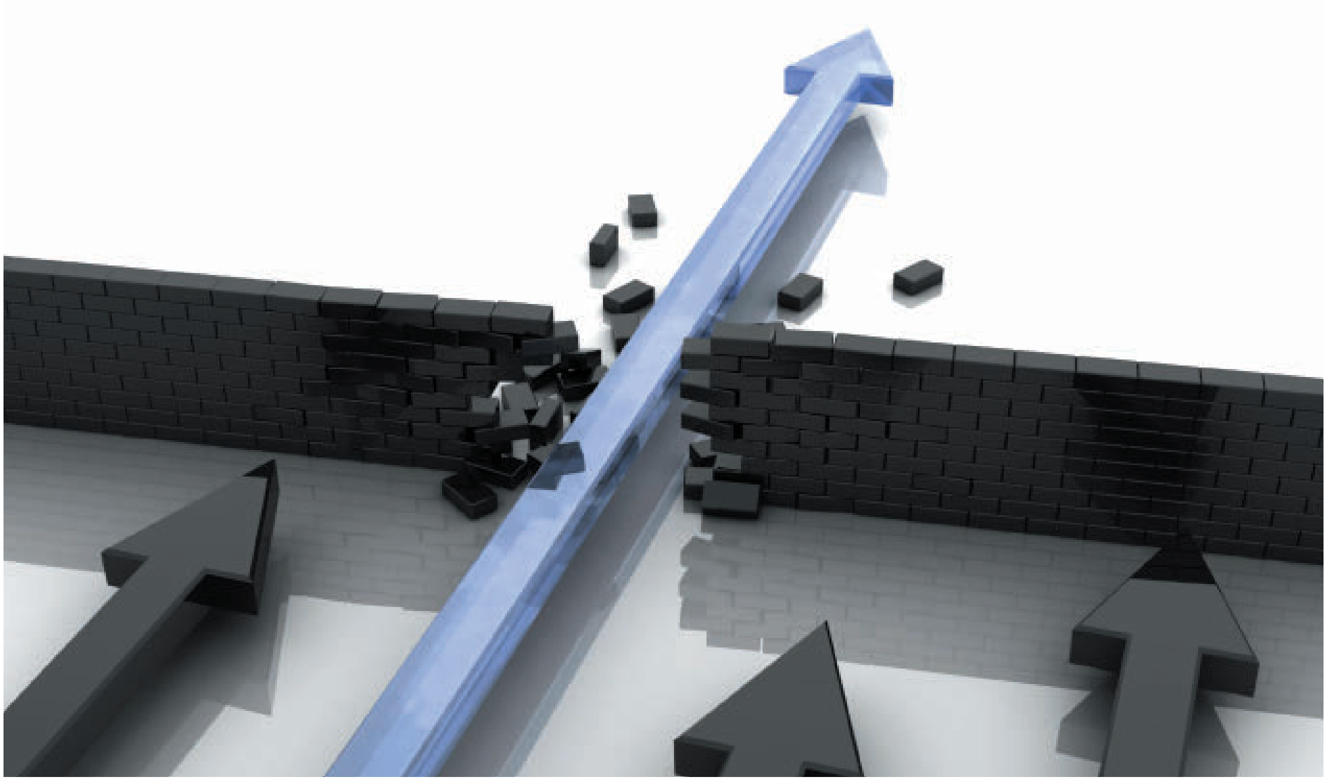
Co-located in one of the world's great destinations, ISACA's EuroCACS/ISRM Conference offers global attendees career growth opportunities including:

- Unique learning experiences across more than 40 sessions on security, risk and assurance
- Fresh content delivered in a variety of styles ranging from interactive discussion and hands-on participation to engaging case studies from many industries
- The chance to sharpen your skills while earning up to 39 CPEs
- Networking opportunities with like-minded professionals from top global organisations

ISACA®

Trust in, and value from, information systems

Register on or before 22 July 2013 at isaca.org/Euro2013 and save US $240!



Volume 3, 2013

ISACA® Journal

Columns

Features

Plus

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

Read more from these *Journal* authors…

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

Journal Online

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

Online Features

The following articles will be available to ISACA members online on 3 June 2013.

An Introduction to Auditing HP NonStop Servers—Review of User Access
David Ramirez, CISA, CISM, CISSP, BS 7799 LA, MCSE, QSA, and Nikos Zarras, CISA, MBCS

Dealing With Computer Fraud
Filip Van Hallewijn, CISA, CISM, AMBCI

Phishing Should Not be Treated the Same as Common Spam
Norman M. Sadeh, Ph.D.,

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

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.*

Barbarians at the Ramparts

On the last day of 2012, the *New York Times* printed a rather disturbing article. The first sentence is sufficient to explain why it created such angst. "The antivirus industry has a dirty little secret: Its products are often not very good at stopping viruses." The gist of the rest of the piece is that there has been a massive growth in the incidence of malware, from one million new strains in 2000 to 49 million in 2010. Worse yet, the virus writers of the past were mostly devilish amateurs, the so-called "script kiddies," while today the "bad guys…[are] siphoning out a company's trade secrets, erasing data or emptying a consumer's bank account."[1]

This is, obviously, unhappy news for those of us who are *concerned* about information security. Everyone is concerned, of course, but we information security professionals are supposed to *do something* about it. The evidence presented in this article raises problems in a number of ways. First, most companies have made a sizable investment in malware protection; it is difficult to read and harder to explain that the return on investment (ROI) is diminishing and may have expired. Unlike an old car that can be traded in for a new model, the antimalware producers have not developed a single solution that can replace the old one. Moreover, it is still necessary to pay maintenance fees for existing products because the prior threat of defeatable viruses has not gone away.

Second and more serious, those with information to protect—especially information that has monetary value—may be exposed to threats for which there are presently no effective countermeasures. The media often use situations such as this to write screed that I call "Civilization as We Know It Is Coming to an End." There is, however, some justification of limited optimism. The history of information technology is replete with crises like this one. Before this, there were hackers, viruses, Year 2000 and international espionage; society has survived them all, and there is reason to believe information technology will survive this period as well.

WALLS AND LADDERS

Ever since humankind built walls around its fortresses and towns, attackers have built ladders to climb over the walls. Sometimes the walls have been high enough; sometimes the ladders overtopped them. Evidently, the ladder builders have the advantage for now, but I am confident that the wall builders will soon catch up. Indeed the same *New York Times* article quoted at the beginning of this column discussed various novel approaches to improving malware protection. These include behavior-based blocking and continuous monitoring of access to servers, databases and files for suspicious activity.[2] I make no pretense of being able to describe their underlying technologies and there is no guarantee as yet that they will be effective, but it is good to know that security software vendors are rising to the challenge of the cyber ladder builders.

Just because higher walls will soon be built, there is no excuse for complacency on the battlements. In the face of the inadequacies of certain tools, security professionals need to apply other existing protective measures more aggressively and perhaps in unanticipated ways.

INCREASED VIGILANCE

The first step is to accept the fact that the barbarians are planning to come over the walls and to be on perpetual lookout for their arrival. There is no need for paranoia, but there are people in the world with evil intentions for the information in organizations' databases. Therefore, attention to monitoring systems, such as intrusion detection and virus filters, must be redoubled.

One tendency on the part of some managers I have dealt with over the years must be halted. That is, I have been told that evidence of a failed attack is unimportant because, after all, it *failed*. Those who espouse such a position need to understand that in many cases, unsuccessful penetration attempts are a prelude to the one that actually gets through and leaves no trace. The logs produced by security tools should be scrutinized for patterns of timing, source location, repetition and any other identifying characteristics that may indicate that a breach has taken place.

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:

In particular, the usual inclination to assume that a system problem is benign until proven otherwise should be reversed. That is not to say that every system hiccup should be treated as an attack, but rather that the possibility of an attack should be kept in mind—right up front—when something unexpected happens. Increased vigilance is a small, inexpensive price to pay for enhanced security during difficult times.

CERT

Every organization at risk needs technicians trained to respond if a breach is identified, or even suspected. Known generically as a computer emergency response team (CERT), such a team is primed to take immediate and effective action should there be a security breach or other cause of extended system disruption.

Today, there are CERTs at various levels: within organizations, at research institutions,[3] regionally and nationally. Given the threats faced by all organizations reliant on information systems, the development of an internal CERT and linkage with local and national teams is applied common sense. There is simply no justification for not being prepared.

DEFENSE IN DEPTH

If, as the *New York Times* article alleges, the attackers are overwhelming the defenses provided by current antimalware tools, it may be prudent to apply multiple layers of protection. This is hardly a new concept (in fact, none of the techniques suggested in this article are new), but sometimes desperate times call for tried-and-true measures. For example, if there is reason to fear the failure of one antivirus filter, use two, or three or enough that there is some confidence that if one is beaten, another will prevent the successful penetration of a virus.

Bar all the gates: Have a virus filter on perimeter routers, on servers and on personal computers. Of course, there may still be an attack that circumvents all barriers, but there is some reason to hope that attackers will seek easier prey if they find several walls to climb over at a particular location.

CLASSIFICATION

Information classification by itself will not prevent attacks, but it might lead to a program in which the most valuable resources—critical and sensitive databases and other information resources—receive the most stringent protective measures. These might include placement in tightly controlled data centers with limited physical access,[4] encryption (as a way to reduce the value of sensitive information to a penetrator) and even removal of these files from online access.

Any malfunction involving the most sensitive information should be treated as a hostile action until proven otherwise. While, in the past, those experiencing a virus or other malware attack were often the unfortunate recipients of random vandalism, targeted computer attacks are increasingly prevalent.[5] Sadly, it is now more rational to consider that anything that negatively affects a crucial resource is a hostile action.

There is a need for close cooperation between the developers of improved security tools and the potential buyers of such safeguards. The robustness of mutual vendor-customer self-interest has been a goad to progress in the past and I believe will again raise the walls higher. (I will return to this topic in a future column.)

ENDNOTES

[1] Perlroth, Nicole; "Outmaneuvered in Their Own Game, Antivirus Makers Struggle to Adapt," *The New York Times*, 31 December 2012

[2] *Ibid.*

[3] To my knowledge, the first CERT (and the origin of the term) was at Carnegie Mellon University's Software Engineering Institute.

[4] To a shocking extent, successful attacks are being perpetrated by people with authorized access. See Silowash, George, *et al.*; *Common Sense Guide to Mitigating Insider Threats, 4th Edition*, Software Engineering Institute, December 2012.

[5] Articles about recent attacks on US banks—Engleman, Eric; "Major Banks Under Renewed Cyber Attack Targeting Websites," *Bloomberg*, 20 December 2012—and the same *New York Times* article quoted previously are anecdotal evidence of a clear trend toward targeted attacks.

The Arrival (Finally) of PCI Cloud Guidance

Andrew Hay is the chief evangelist for CloudPassage, a cloud server security provider, where he serves as the lead advocate for its Software as a Service (SaaS) server security product portfolio. Find Hay tweeting at *@andrewsmhay.*

In February, the PCI Security Standards Council (PCI SSC)'s Special Interest Group (SIG) for Cloud[1] released its much-anticipated guidance for securing Software, Platform and Infrastructure as a Service (SaaS, PaaS and IaaS) cloud servers. Though many in the security and cloud industries claim that the guidance lacks enforcement capabilities, is at least three years behind the technology curve or is too prescriptive in nature, the information supplement should still serve as a valuable source of information for those looking to make their cloud servers compliant with the Payment Card Industry Data Security Standard (PCI DSS).

The guidance, *PCI DSS Cloud Computing Guidelines Information Supplement*,[2] addresses a number of questions frequently asked by clients looking to move to the cloud, in addition to questions by PCI Qualified Security Assessors (QSAs), approved scanning vendors (ASVs) and internal security auditors (ISAs) looking to align customers' cloud projects with the standard.

One of the most commonly asked questions of the PCI SSC was a point of clarification around PCI DSS responsibility delineation between the cloud service provider (CSP) and the client organization. Knowing *who* is responsible for *what* with regard to the cloud PCI DSS was addressed at length within the information supplement.

The security and compliance responsibility of an end user's cloud server instance depends entirely on the cloud architecture model being used. As shown in **figure 1**, if clients are using a SaaS application, they may be responsible only for the interface and resultant data. Conversely, if their server is running on an IaaS cloud architecture, their responsibility broadens to include the application, solutions stack, operating system, virtual machine instance and even the virtual network infrastructure.

The Cloud SIG guidance clearly states that just parking data on a PCI-compliant CSP does not automatically make an organization PCI-compliant. Even where a CSP may be validated for certain PCI DSS requirements, this validation does not automatically transfer to its clients' environments. For example, a CSP's validation may have included use of up-to-date antivirus software on the CSP's systems. This validation, however, would likely not transfer to the individual client cloud service instance—especially if the client is hosting its

Figure 1—Assigning Control Between the CSP and the Client Across Different Service Models

Cloud Type/Layer	IaaS	PaaS	SaaS
Data	🟩	🟩	🟩
Interfaces (APIs, GUIs)	🟩	🟩	🟩
Applications	🟩	🟩	🟦
Solution stack (programming languages)	🟩	🟩	🟦
Operating systems (OS)	🟩	🟦	🟦
Virtual machines	🟩	🟦	🟦
Virtual network infrastructure	🟩	🟦	🟦
Hypervisors	🟦	🟦	🟦
Processing/memory	🟦	🟦	🟦
Data storage (hard drives, removable disks, backups, etc.)	🟦	🟦	🟦
Network interfaces and devices, communicaitons infrastructure	🟦	🟦	🟦
Physical facilities/data centers	🟦	🟦	🟦

🟩 Client

🟦 Cloud service provider

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:

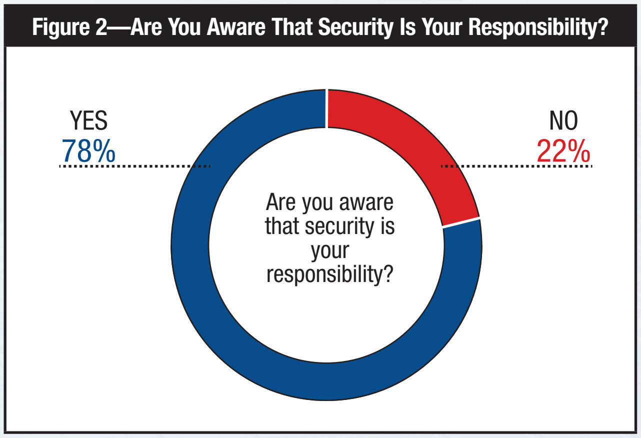
instance on a shared IaaS cloud architecture. The client must still maintain compliance for all of its own systems by ensuring technical controls are installed and updated on all client-side systems used to connect into the cloud environment.

Security or compliance professionals might think this guidance should be common-sense knowledge. Unfortunately, not everyone understands the delineation of security responsibility in cloud environments. In a recent survey, 22 percent of respondents believed that their CSP was responsible for the security of customer cloud server instances (**figure 2**).[3] This is perhaps due to a misunderstanding of the different cloud architecture models or CSP security capabilities, muddled CSP marketing, or some combination thereof.

As a general rule, the more aspects of a client's operations that the CSP manages, the more responsibility the CSP has for maintaining PCI DSS controls. However, the Cloud SIG notes that "outsourcing maintenance of controls is not the same as outsourcing responsibility for the data overall. Cloud customers should not make assumptions about any service, and should clearly spell out in contracts, memorandums of understanding, and/or (service level agreements [SLAs]) exactly which party is responsible for securing which system components and processes."[4]

Figure 3 depicts how PCI DSS responsibilities may be shared between clients and CSPs.

Figure 2—Are You Aware That Security Is Your Responsibility?



The Cloud SIG made sure to highlight that the concept of shared or joint responsibility can be a particularly tricky path to navigate:

> *Where the CSP maintains responsibility for PCI DSS controls, the client is still responsible for monitoring the CSP's ongoing compliance for all applicable requirements. CSPs should be able to provide their clients with ongoing assurance that requirements are being met, and where the CSP is managing requirements on behalf of the client, they should have mechanisms in place to provide the customer with the applicable records.*[5]

Figure 3—Sharing PCI DSS Responsibilities Between Clients and CSPs

PCI DSS Requirement	IaaS	PaaS	SaaS
Install and maintain a firewall configuration to protect cardholder data.	⬜	⬜	🟦
Do not use vendor-supplied defaults for systems passwords and other security parameters.	⬜	⬜	🟦
Protect stored cardholder data.	⬜	⬜	🟦
Encrypt transmission of cardholder data accross open, public networks.	🟩	⬜	🟦
Use and regularly update antivirus software or programs.	🟩	⬜	🟦
Develop and maintain secure systems and applications.	⬜	⬜	🟦
Restrict access to cardholder data by business need to know.	⬜	⬜	⬜
Assign a unique ID to each person with computer access.	⬜	⬜	⬜
Restrict physical access to cardholder data.	🟦	🟦	🟦
Track and monitor all access to network resources and cardholder data.	⬜	⬜	🟦
Regularly test security systems and processes.	⬜	⬜	🟦
Maintain a policy that addresses information security for all personnel.	⬜	⬜	⬜
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	🟦	🟦	🟦

🟩 Client 🟦 Cloud service provider ⬜ Both client and cloud service provider

As with all hosted services in scope for PCI DSS, the client organization should request sufficient evidence and assurance from its CSP that all in-scope processes and components under the CSP's control are PCI DSS-compliant. This verification may be completed by the client's assessor (e.g., a QSA or ISA) as part of the client's PCI DSS assessment. If the CSP has already undergone a PCI DSS assessment that was performed by another assessor, the client's assessor will need to verify that the CSP's assessment covered all services provided to the client and all applicable requirements were found to be in place for the environments and systems in scope.

According to the Cloud SIG, the recommended practice for clients with PCI DSS considerations is to work with CSPs whose services have been independently validated as being PCI DSS-compliant. CSPs that have undergone PCI DSS validation should be able to provide their clients with the following:

1. Proof of compliance documentation (such as the attestation of compliance [AOC] and applicable sections from the report on compliance [ROC]), including date of compliance assessment
2. Documented evidence of system components and services that were included in the PCI DSS assessment
3. Documented evidence of system components and services that were excluded from the PCI DSS assessment, as applicable to the service
4. Appropriate contract language, if applicable

CSPs should provide their clients with evidence that clearly identifies what was included in the scope of their PCI DSS assessment, the specific PCI DSS requirements against which the environment was assessed and the date of the assessment. All aspects of the cloud service *not* covered by the CSP's PCI DSS assessment should also be identified and documented, as these will need to be validated by either the client or the CSP in order for a client's assessment to be completed. The client must have a detailed understanding of any security requirements that are not covered by the provider and are therefore the client's responsibility to implement, manage and validate as part of its own PCI DSS compliance assessment.

Considerations for the client may include:

- How long has the CSP been PCI DSS-compliant? When was the last validation?
- What specific services and PCI DSS requirements were included in the validation?
- What specific facilities and system components were included in the validation?
- Are there any system components that the CSP relies on for delivery of the service that were not included in the PCI DSS validation?
- How does the CSP ensure that clients using the PCI DSS-compliant service cannot introduce noncompliant components to the environment or bypass any PCI DSS controls?

So, does this mean that the PCI Cloud SIG is saying that customers can only use PCI-compliant CSPs? The guidance does not come right out and state that in such pointed words. It does, however, mention the complications involved with trying to become PCI-compliant in noncompliant cloud architectures—effectively presenting a use-at-your-own-risk approach.

As clients, enterprises are free to choose whichever CSP they wish, just as they should be free to move their servers, applications and data among CSPs. They should note, however, that if they are not using a certified PCI-compliant CSP, they would likely run into issues achieving PCI certification themselves. According to the Cloud SIG, "CSPs that have not undergone a PCI DSS compliance assessment will need to be included in their client's assessment. The CSP will need to agree to provide the client's assessor with access to their environment in order for the client to complete their assessment."[6]

The client's assessor may require onsite access and detailed information from the CSP, including but not limited to:

- Access to systems, facilities and appropriate personnel for onsite reviews, interviews and physical walk-throughs

- Policies and procedures, process documentation, configuration standards, training records, and incident response plans
- Evidence (such as configurations, screen shots and process reviews) to show that all applicable PCI DSS requirements are being met for the in-scope system components
- Appropriate contract language, if applicable

Therefore, if an organization needs to be compliant, the scope of its assessment would need to include its CSP's infrastructure and processes as well as its own. And therein lies the rub. The PCI SIG guidance says that an enterprise can operate its cloud servers within the bounds of the PCI DSS in a noncompliant cloud architecture provided that it, as the individual CSP client, is comfortable (or even capable of) certifying its CSP's environment. The environment, which would include the physical architecture, software architecture and process, might also extend to other customers' cloud server instances if proper segmentation is not defined among tenants.

It is exponentially easier and more cost-effective to move into a PCI-compliant CSP than one that has not yet certified its part of the shared-responsibility model. To put it another way, if the PCI DSS compliance of a CSP is the first 26 miles of a marathon, the compliance of the organization's cloud servers is but the last 385 yards.

ENDNOTES

[1] PCI Security Standards Council, *www.pcisecuritystandards.org/get_involved/special_interest_groups.php*

[2] Cloud SIG, *PCI DSS Cloud Computing Guidelines Information Supplement*, PCI Security Standards Council, *www.pcisecuritystandards.org/security_standards/documents.php*

[3] CloudPassage, 2012 Cloud Security Survey, *www.cloudpassage.com/resource-center/get/security-and-the-cloud-2012*

[4] *Op cit*, Cloud SIG

[5] *Ibid.*

[6] *Ibid.*

IS Audit Basics

Auditing the IT Auditors

Tommie Singleton, CISA, CGEIT, CPA, is the director of Consulting for Carr Riggs & Ingram, a large regional public accounting firm. His duties involve forensic accounting, business valuation, IT assurance and service organization control engagements. Singleton is responsible for recruiting, training, research, support and quality control for those services and the staff that perform them. He is also a former academic, having taught at several universities from 1991 to 2012. Singleton has published numerous articles, coauthored books and made many presentations on IT auditing and fraud.

Every time an IT auditor engages in an IT audit/assurance project, at least one person reviews the work. The audit profession in general has developed structures and processes to make sure audits and similar projects are subject to an appropriate degree of review before being released to the sponsor. That process often involves multiple layers of review. The more risk associated with the project, the stricter the review process becomes and the more layers the structure contains.

The review process is designed to make sure the final product is appropriate given the original request, the results of tests and procedures, and technical literature and guidance on the subject matter. Tenure is important for a quality review to occur, and naturally requires a level of skill and knowledge to perform. The bottom line is that someone who is a subject matter expert (SME) in terms of the type of IT audit being performed will be the reviewer. Thus, for a Payment Card Industry (PCI) audit, the reviewer is likely to be certified Payment Card Industry Data Security Standard (PCI DSS), have years of experience, and be knowledgeable of technical literature and guidance on PCI audits. For a financial audit, the reviewer is likely to be a partner who is knowledgeable about IT, knows the client, knows the technical literature and guidance, and has years of experience.

Everyone involved in the project wants a quality review done internally prior to being released.

The questions addressed herein are: What should an IT auditor new to the profession expect in terms of the review process? What types of things are reviewers concerned about? What things would cause a reviewer to send the project back to the IT audit team for changes? How can the IT auditor make sure the review process goes smoothly? What does a reviewer's checklist look like?

SCOPE AND RISK

The first thing to understand about the review process is that the structure and process are highly correlated with risk. That is, the more risk associated with an IT audit project, the higher the level of scrutiny in the review process and the higher the likelihood of multiple layers of review. Therefore, if a project has a lot of risk associated with it for one reason or another, the IT auditor knows up front that the project will be reviewed more closely and probably by more professionals than otherwise.

Sometimes the type of entity drives that same intense review. Audits of financial institutions, larger entities (e.g., publicly traded companies) or entities highly dependent on IT are often considered in need of a higher level of review.

A level of importance based on other issues may also lead to a higher level of review. For instance, an internal audit of the entity's perimeter for a high-profile organization could be seen as vitally important in today's environment and, thus, may lead to a higher level of review.

Generally speaking, even entry-level IT auditors have a sense of this elevated need for review and recognize a project that is likely to take on that process. If risk is relatively high, more caution is needed in tests and procedures, documentation and work papers, and communications and reporting.

RELEVANT AREAS FOR IT IN A REVIEW

A review obviously covers many aspects of the project/audit other than those that are IT-related. The general (non-IT) aspects include planning, technical proficiency of the team members, sufficient independence, methodology and using the work of others, among others. The areas in a review that can be related to IT are described in the following sections.

Technical Training and Proficiency

IT members of an audit or project are treated the same as others in terms of assessing an adequate level of technical abilities and proficiency sufficient for a particular project. One of the differences is the number of subsets of IT that exist and the need to have experts in them from time to time.

FORUM

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:

For instance, a medium-sized company could be employing e-commerce via a web site, using a service organization to take care of payments (subject to PCI compliance and federal and state laws), using cloud services and involving a host of other IT-related influencers. These present the need for several specialty areas of IT that could arise for this single entity.

A second issue is the need to keep skills and abilities adequate and up to date. It goes without saying that once a person chooses to be in the IT audit profession (or any other IT profession), the person is committed to life-long learning. IT changes so rapidly that a person's skills and abilities can become obsolete in a few years. Thus, one aspect of assessing risk for the IT function in an entity is the level of training and professional education people obtain each year, both on the corporate and individual levels. The same is true for IT auditors.

Controls: ICFR

Controls are always a part of an IT audit or assurance project, but they can be different sets of controls depending on the nature of the project and the audit objectives. Thus, each of the controls aspects that follow may or may not apply to a specific IT audit (i.e., when applicable, use them).

When the audit project involves financial reporting, the internal controls over financial reporting (ICFR) are a critical component of what the reviewer(s) want to examine. Thus, the IT auditor must take care in a financial audit to identify the relevant IT controls for ICFR and make sure to gain a proper understanding of applications, transactions and infrastructure that impact the financials.

The reviewer's checklist[1] for this item should generally look something like **figure 1**. In some manner, the items in **figure 1** should be mapped to authoritative guidance and work papers.[2] This ensures compliance with standards and a sufficient scope of checklist items and facilitates the review process.

Controls: Entity Level

Another aspect of internal controls that affects the IT auditor is entity-level controls (ELC). These are controls at the higher levels of the entity that can impact the objective(s) of the IT audit or project. These would include board-related controls (e.g., IT governance), executive-related controls (e.g., managing the IT function by the CIO) and other broad controls relevant for the entity.

The reviewer's checklist for ELC should generally look something like **figure 2**. Once again, the items usually are mapped to authoritative guidance and work papers. Often, and probably usually, an analysis of the ELC would require a walk-through to see if these controls have been designed properly and are implemented. Testing of these controls may become necessary later in the IT audit theoretically, but are sometimes done simultaneously with the up-front identification and analysis.

Figure 1—Sample Reviewer's Checklist for ICFR

Did the IT audit team gain an understanding of:

- The applications that support significant processes and major classes of transactions (e.g., does software support the deposits process)?
- How transactions flow within the application (i.e., initiated, authorized, recorded, processed, reported)?
- The underlying infrastructure (e.g., host server, network) supporting the applications identified?

Did the IT audit team assess the control environment, risk assessment and monitoring activities?

Audit Documentation:
Does the audit documentation include:

- An understanding of the IT environment documented and retained in the planning section of the work papers?
- Did the IT audit team document the control environment, risk assessment and monitoring activities?

Figure 2—Sample Reviewer's Checklist for ELC

Did the IT audit team perform an assessment of the client's IT control environment?

Audit Documentation:
Does the audit documentation contain the completed entity-level questionnaire and supporting information including performance of walk-throughs?

Controls: IT General Controls

IT general controls (ITGCs) have been one of the hot topics in IT and controls over the last few years. ITGCs have an effect on financial audits, all internal IT audits, all external IT audits and IT governance.

One of the things IT auditors need as a foundation is a good understanding of what constitutes an ITGC, how they are measured, what their risks are, and how to identify controls and assess their effectiveness. A great beginning is to read the *IT Audit Framework (ITAF)* from ISACA, section 3630, Auditing ITGCs.[3]

Figure 3—Various Authoritative Lists of ITGCs

ISACA's ITAF	PCAOB's AS5	AICPA's IT Audit White Paper
• Introduction to ITGC • Information resource planning • IT service delivery • Information systems operations • IT human resources • Outsourced and third-party activities • Information security management • Systems development life cycle (SDLC) • Business continuity planning (BCP) and disaster recovery planning (DRP) • Database management and controls • Systems software support • Network management and controls • Hardware support • Operating system management and controls • Physical and environmental control • Enterprise portals • Identification and authentication	• Security and access • Computer operations • System development and changes	• IT environment/IT function • Access controls • Change management • BCP and DRP • Outsourcing/service organization controls

Figure 4—Sample Reviewer's Checklist for ITGC

Did the IT audit team perform the ITGCs review? Did the review include the following attributes:

- Identification of risk and related control objectives?
- Identification of controls in place and the assessment of design effectiveness?
- Walk-throughs of IT process maps and existing controls?
- Identification of tests to evaluate the controls identified?
- Clearly documented results of the tests performed and the assessment of operating effectiveness?
- Work papers that support the assessment?
- Identification of control deficiencies and analysis of whether the deficiency elevates to significant or material weakness?
- Follow-up on the control deficiencies with management throughout the year, including testing of deficiencies remediated during the audit year?
- Year-end testing procedures?

Audit Documentation:
Is the audit documentation:

- Prepared in sufficient detail to provide a clear understanding of its purpose, source and conclusions reached?
- Prepared in sufficient detail to provide a clear understanding of nature, timing, extent and results of procedures performed, evidence obtained and conclusions reached?
- Clear in identifying the type of test (e.g., walk-through, inspection)?
- Clear in identifying, for example, the audit sample selected from a population, the source of the sample size?
- Appropriately organized to provide a clear link to the significant findings or issues?
- Able to determine who performed the work, the date the work was completed, the supervisor who reviewed the work and the date of the review?

ITAF describes 17 different areas of ITGC. The Public Company Accounting Oversight Board (PCAOB) describes three. The American Institute of Certified Public Accountants (AICPA) has five. **Figure 3** provides these lists. It is fairly easy to map these three taxonomies to each other; thus, there is basically a consensus as to the ITGCs. The difference is in the details of the items.

IT auditors need to understand that a significant weakness in an ITGC not only affects the ITGC, but also everything it affects. An ITGC is considered to be an entity-level control by the PCAOB, and thus it affects almost everything in the IT function and much, if not all, of the information systems, applications and technologies. It is for this reason that the PCAOB and AICPA guidance states that if the ITGC has significant deficiencies, the auditor cannot rely on application controls, which in reality reside beneath the ITGCs.

The reviewer's checklist for ITGCs would generally look something like **figure 4**. It is based on authoritative guidance and work papers.

Controls: Application

Application controls are, by definition, automated controls, or hybrid controls,[4] which make sure transactions are properly initiated, authorized, recorded, processed and reported. The more the control objective is driven by manual controls being melded, the higher the failure rate of the control. As IT professionals know, a fully automated control does the same thing over and over again. Once it has been tested, and as long as integrated technologies are unchanged, it will keep producing the same results as designed.

The IT auditor needs to know when it is appropriate to include application controls, which controls are relevant, how to test the control, how to assess its level of reliability and assurance provided, and how to fit all of that with the overall audit plan and program. The reviewer will be looking for that kind of information.

The reviewer's checklist for ITGCs would generally look something like **figure 5**.

Figure 5—Sample Reviewer's Checklist for Application Controls

- Did the audit engagement team and the IT audit team agree to specific application software automated controls that are identified as key controls to be the responsibility of the IT audit team to test?
- Did the IT audit team perform appropriate tests of ITGCs over in-scope application software (i.e., the application software identified to contain key automated controls, as described previously)?
- Did the IT audit team perform testing to verify the design and operating effectiveness of the identified application software automated controls, including the use of appropriate sample sizes, as agreed to with the audit engagement team?
- Did the IT audit team work with the audit engagement team to complete the aggregation analysis of any identified ITGC deficiencies?

Work Papers/Documentation

All auditors understand that the audit tests and procedures, and other aspects of the audit program, must be documented. The body of work papers, in particular, becomes the body of evidence to support the audit report and findings.

In addition, work papers become a key factor in the review process. The reviewer usually has not been privy to the daily information being gathered and handled during the audit process. Therefore, the reviewer is dependent on a body of information to pick up and fully understand, for example, what was done, the results, whether a sufficient body of tests and procedures was done, and whether the proper conclusions were drawn from the body of evidence. In fact, it is not uncommon in the first review for the reviewer, who is generally one level above the team leader internally, to have a question or need something else done to the evidence or need something else done for the audit program. In such a case, this is done with some form of written instructions (i.e., notes). When this happens, the process is pushed back to the team leader to clear up whatever the reviewer requested—usually referred to as "clearing notes" in a financial audit. It then goes back to the same reviewer. The efficiency and effectiveness of this process, including the loop, are highly dependent on the work papers' quality, completeness and clarity (for reader's understanding).

Report

Lastly, there is a report. The report is definitely subject to review. The report must be in conformity with the entity's methodology and any technical requirements. It is probably the most important document to get reviewed.

PROCESS

Some of the process has been explained, but it will flow something like the following:

- Team leader reviews the documentation, work papers and report before sending it up the review chain.
- Someone above the team leader reviews the audit. If problems or issues are found, the package is returned to the team leader, who addresses them.
- Often, the review then goes to yet another person up the review chain—or parallel to it—for a second review.

- Should the nature of the audit (e.g., risk) or entity require it, a third review might occur.
- Even when the internal part is complete, sometimes there is an external entity that reviews the audit and the review process.

CONCLUSION

If the review process is done properly, the resulting product has sufficient quality to withstand scrutiny and analysis by the sponsor and other users, which means it is a quality audit. Therefore, it is valuable for the IT auditor to understand what constitutes a proper review, how that review process is carried out and how to make sure that the process is as trouble-free as possible.

Review is often multilayered—the team leader (e.g., manager) reviews for the team, someone else reviews the team leader (partner or director of IT audit) and additional layers may be needed for special occasions. But each layer is generally looking for the same things: proper scope throughout, proper work papers/documentation, whether the body of work papers support conclusions, and whether the report is written properly (grammar/spelling, enough narrative but not too much), addresses the original audit objectives effectively and is technically correct.

Perhaps the best guidance for the topic of this article is ITAF.[5] It contains information on the subjects herein and more. In particular, it can make the review process more efficient and effective since the IT auditors doing the work are empowered to properly scope the audit, develop adequate evidence, address the proper controls and draw the proper conclusions.

To help make the process go smoothly and to avoid "loop backs" to clear up issues from the reviewer, IT auditors need to be diligent in performing their duties. In particular, it is important to self-check the audit when they believe they are done, asking:

- Were all of the audit objectives addressed?
- Were the tests and procedures robust enough given the risk involved?
- Were all the relevant laws and regulations considered?
- Is the body of evidence sufficient to support the conclusions and findings?
- Do the work papers tie back to the audit objectives and conclusions properly?

While most newer (to the profession) IT auditors may need some time and experience to adequately address the guidance provided here, they need to at least understand who audits the auditors, how that process works, and how to make that process efficient and effective.

ENDNOTES

[1] The checklists herein are based on checklists that might be used in a financial audit. Thus, they would be somewhat different for an internal IT audit for application controls, infrastructure audits, etc., but the principles should be similar.

[2] All checklists have those two same factors: mapped to authoritative literature in some manner (e.g., reviewer mentally scanned the relevant literature requirements) and mapped to workpapers, usually physically on the form.

[3] ISACA, IT Assurance Framework (ITAF), *www.isaca.org/itaf*

[4] Hybrid refers to a combination of manual and automated controls to perform the control objective. This type of control is referred to as IT-dependent by the PCAOB and others.

[5] *Op cit*, ISACA

Why Do Corporate Frauds Occur?

Vasant Raval, CISA, DBA, is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interests include information security and corporate governance. Opinions expressed in this column are his own, and not those of Creighton University. He can be reached at *vraval@creighton.edu.*

Recently, 125 students at Harvard University were accused of cheating on the final examination in a course titled "Introduction to Congress."[1] College education should lead to moral development. However, it seems the bond between college experience and character development has weakened considerably. With some exceptions, the mind-set of institutions and their stakeholders seems to have drifted toward a narrower, more materialistic focus. Today, the careerist mind dominates the scene; the moral mind is no longer attractive.

Cheating, of course, is a type of indiscretion and suggests the degradation of moral fabric as much as other indiscretions such as financial fraud. Within the broad range of exhibited indiscretions, we may include malicious attacks, social engineering, cyberattacks and a multitude of violations of trust that humans can craft. Regardless of the outward shape of such occurrences, the underlying propensity to act as such is constant and unvarying. Any type of indiscretion, including fraudulent financial reporting, can be argued as a root-level problem of human behavior. At the very core of the human constitution, something in the nature of a being causes the compromise. There may not be an easy fix for it. However, a clear explanation of acts of fraud lies in answers that put human nature at the center of the fraud paradigm.

The US Securities and Exchange Commission's enforcement actions vividly portray that between 1998 and 2007, the chief executive officer (CEO) and chief financial officer (CFO) were named in 89 percent of the cases of fraudulent financial reporting.[2] This number is so high that one could simply follow the 80:20 rule and pursue the question of why a single, albeit most powerful, executive would resort to financial fraud, often against his own long-term interests. While we habitually associate the financial reporting of fraud to the company involved, it seems that a key to the pattern of fraud is a single person in most cases, if not all.

In searching for answers, one should first look at the intentional (nonbasic) actions of a person. Fundamentally, any volitional human behavior is a result of the interaction between nature and nurture, or as some might say, between organism and environment.[3] The two belong to different disciplines, moral philosophy and social science, and yet, neither one by itself is sufficient to offer an explanation of the act—in our case, an act of fraud. Representing the person's choice, an actual act is a result of the organism acting within the context of the environment—the situation—at the time. In the following discussion, the first dimension—human nature—is expressed in the form of disposition of the person, and the second dimension—the environment in which the act takes place—is denoted primarily in the form of temptations to which the executive becomes attached.[4]

EXECUTIVE DISPOSITION

People's natures drive their tendencies. Fundamentally, our choices are an expression of our inner state or disposition. The disposition of a person drives the choices he/she makes, whether these choices have to do with physical, mental, moral or spiritual aspects of his/her life. Since a fraud borders on immorality of the actor, we are primarily interested in the person's disposition in terms of moral development. Using Kohlberg's stages of moral development,[5] one could argue that low moral development is exhibited in self-centric behavior and high moral development is found in less selfish (or predominantly other-centric) behavior. In essence, dispositional properties of a person drive the desire to perform an act. The proneness to act in a certain way comes from one's disposition; it is the nature of the person that drives choices at all levels in life.

Aristotle once said that a genuinely virtuous action proceeds from "firm and unchangeable character" rather than from transient motives. At the corporate executive level, the constitution that drives one's choices has vast impact. For a

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:

self-centric executive, transient motives may dominate the choices, while a selfless executive would adhere to choices that agree with his/her integrity regardless of the temptations that surface along the way. The CEO's moral stage of development influences the tone at the top that cannot be neutral to, or against, his/her disposition. Thus, one could argue that CEOs who commit fraud are of a different disposition than those who do not. It is all a matter of desire driven by one's nature.

We need to be careful in differentiating between a disposition and an occurrence. Disposition exists all the time, while an occurrence is an episode expressing the disposition. A rubber band is stretchable, it is the rubber band's disposition, but that does not mean the rubber band is always in a state of being stretched. A glass pane is breakable, it is the disposition of the glass pane; however, it shatters only upon impact of a thrown object. The shattering of glass is an occurrence while the property of being breakable is its disposition. In the context of executive fraud, one might translate this as: Some executives may be more prone to commit indiscretion, but may not necessarily have been involved in an occurrence of fraud.

ATTACHMENT TO TEMPTATIONS

The nature of an individual does not exhibit behavioral tendencies in a vacuum. There has to be the context, the environment in which the act is rooted. The environment offers a trait-eliciting condition, a prerequisite to commit fraud. Before indulging in a fraudulent act, the executive's assessment of the environment should lead to the belief that such an act is feasible. In essence, the desire and corresponding motivation stemming from one's disposition meet the belief that the act can be "pulled off" without consequences (or with affordable consequences). Desire, belief and the link between the two jointly trigger the act. Desire provides the motivation and belief renders an assurance of the means-end relationship (i.e., "If I do this, I will get that.").

It is questionable that opportunities by themselves cause fraud. If that was the case, both self-centric and less selfish executives would be drawn to them equally. Even in the face of many opportunities, selfless executives would not take advantage of the circumstances even when they ascertain that the act is feasible and the side effects, if any, can be controlled. It is not the opportunities, but rather temptations that act like forceful magnets that suck selfish executives into the act.[6] Temptations emerge as stimuli that attract the person to seek the unpossessed object of attachment. Once a temptation surfaces, the subject evaluates the feasibility of yielding to the temptation. The belief that it is feasible would, in turn, reinforce the conviction that the temptation on hand can be indulged in; motivation is fueled by the belief and the act of fraud occurs.

Myrseth and Fishback observe that a temptation considered in isolation ("just this time only, never again") facilitates the adoption of a narrow frame of reference that leads to indulgence. On the other hand, those who consider a wide frame of reference (a longer-term consideration of pooled consequences of such opportunities over time) avoid indulgence in the immediate future.[7] An executive who frames tempting opportunities as isolated or *special* will in all likelihood go down the path of the fraud cycle.

While temptations exist for all, there seems to be a difference in their treatment by selfish and selfless executives. The former are more vulnerable to putting personal interests above everything else. On the other hand, the latter can exercise self-control by structuring circumstances to increase the likelihood that the temptation will not be acted upon. Thus, virtuous executives could resist temptation; for them, the attachment to temptation, and therefore propensity to succumb to it, is weak. Consequently, they can walk away from temptation. To quote McDowell, "considerations favoring behavior contrary to virtue are 'silenced' in the virtuous person; although she may experience inducement to vice, she will not count them as reasons for action."[8]

> "Information technology could play a significant role in establishing means-end efficiency of a potential fraud."

INFORMATION TECHNOLOGY AS MEANS

Most discussions of information ethics fall in the category of environment and not the human disposition. This is logical as technology does not shape the moral grounding of an actor of fraud; it operates only as a part of the circumstances. By itself, technology can help explain how the fraud happened, but can contribute little to why it happened. From the forensic analysis of a technology-based fraud, investigators would most likely be able to infer how the fraud happened, but could not derive insights on why the person indulged in the act.

This is not to say that information technology does not play a role in frauds; indeed, it does. Depending on the situation, information technology could play a significant role in establishing means-end efficiency of a potential fraud. As an enabler of crimes, technology always poses considerable risk. Even when the technology was rather rudimentary compared to today's standards, executives used technology to establish the means to attain the end. The 1970's case of Equity Funding[9] clearly illustrates this. At Equity Funding, the executives created an obscure file that auditors couldn't access and stored all fictitious insurance policy records in it. The company's growth and a false sense of prosperity were manipulated, leading to market capitalization growth and investor enthusiasm.

> "One cannot control the means of indulgence… only the core understanding of why humans indulge in such acts will offer viable solutions to minimize cases of fraud."

In contrast to the Equity Funding case, the contexts are different today and yet the story is the same. This is evident in cases concerning cybersecurity, spamming, identity theft, social engineering and money mules to exploit innocent people. At a higher level in management, you see this in the development of financial services products (e.g., complex derivatives), fast-track computer trading and a mosaic of scams all leveraging information technology to achieve means-end efficiency.

Technology is here to stay. For information technology, change is constant. New products, applications, platforms, services and business models emerge all the time. One cannot control the means of indulgence. In the final analysis, only the core understanding of why humans indulge in such acts will offer viable solutions to minimize cases of fraud.

ENDNOTES

[1] Some behaviors, such as lying, appear to be more common than we think. Andi McNeal in the *Journal of Accountancy* (August 2012, p. 32-37), notes that Robert Feldman observed strangers who had just met while they engaged in small talk with the intention of becoming acquainted. The results indicate that, on average, people tell three lies during a 10-minute conversation, a finding Feldman has reached consistently in repeated studies (p. 36).

[2] Beasley, M.S.; J.V. Carcello; D.R. Hermanson; T.L. Neal; *Fraudulent Financial Reporting: 1998-2007, An Analysis of US Public Companies*, Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2010

[3] Bem, Daryl J.; David C. Funder; "Predicting More of the People More of the Time: The Search for Cross-situational Consistencies in Behavior," *Psychological Review*

[4] For an in-depth discussion, refer to "Human Disposition and the Fraud Cycle," *International Journal of Applied Behavioral Economics*, 2(1), January-March 2013, p. 1-16

[5] Kohlberg, L.; "Moral Stages and Moralization: The Cognitive Developmental Approach," in L. Kohlberg (Ed.), *The Psychology of Moral Development: The Nature and Validity of Moral Stages*, Harper & Row, USA, 1984, p. 170-205

[6] Raval, V.; "The Disposition-based Fraud Cycle," *International Journal of Applied Behavioral Economics*, 2(2), 2013

[7] Myrseth, K.O.R.; A. Fishbach, "Self-Control: A Function of Knowing When and How to Exercise Restraint," *Current Directions in Psychological Science* 18(4), 2009, p. 247-252

[8] McDowell, J.; "Are Moral Requirements Hypothetical Imperatives?," *Aristotelian Society Supplementary*, 53, p. 13-29

[9] For a discussion on the case, refer to *www.davehancox.com/hancox---sulem---public-speaking/publications/equity-funding (accessed Feb. 25, 2013).*

Five Questions With…

Walter Smiechewicz, CPA

Walter Smiechewicz is a managing director in PricewaterhouseCoopers (PwC)'s Los Angeles, California, USA, office. In the risk assurance practice, he specializes in the disciplines of governance, risk and internal audit. He is responsible for driving the internal audit; governance, risk and compliance (GRC); and enterprise risk management (ERM) consulting services for the financial services sector. He oversees these services in PwC's Western Region and leverages his industry expertise to help companies identify and assess risk and devise cost-effective mitigation strategies consistent with their business objectives.

Smiechewicz's previous experience includes senior-level roles in regional and national entities as chief risk officer (CRO), senior managing director of enterprise risk assessment and chief audit executive. He began his career as a certified public accountant with Deloitte & Touche.

In his professional career, Smiechewicz has worked with the C-suite and boards of directors leading efforts in the areas of governance and interactions with national regulatory bodies. An author and frequent guest speaker, he has led the design, implementation and management of ERM, GRC, internal audit, loan review, fraud investigations, and compliance and Sarbanes-Oxley protocols.

Smiechewicz has been an active volunteer with United Rescue Mission and its Hope Garden Facility for Women & Children. He has served on the nonprofit boards of Gateway-Longview, Girl Scouts, the University of Buffalo's Internal Audit Advisory Board and several not-for-profits in India.

He and his wife reside in Thousand Oaks, California, USA. In his spare time, he enjoys reading military history, particularly with a view to learning the leadership lessons one can derive from such history. He is currently researching and working on an article covering governance lessons that can be learned from Sun Tzu's *The Art of War*. He also enjoys his newer hobby as an amateur photographer.

Q What do you see as the biggest risk factors being addressed by IT audit professionals? How can businesses protect themselves?

A I see data accuracy and data security as two principal areas that must be without ambiguity as they are the basis for sound and secure transactions. These two areas require continuing and constant attention, especially in light of the disruptive abilities of motivated groups prepared and capable of launching cyberattacks.

The other less-discussed risk is the failure to use IT to your strategic advantage. With the rapid advancements in technology and its pervasive use by consumers, updated and leading-edge systems will provide a competitive advantage in the market. Ease of use through well-designed user experiences will encourage consumer satisfaction and loyalty. Those who do not see technology, no matter what business they are in, as a needed core competency and strategic advantage will see the risk realized by loss of market share.

Q How do you see the role of governance of enterprise IT (GEIT) changing in the long term?

A First, controls will largely be electronic and GEIT will be the fulcrum in all aspects of governance in any corporation. Anyone who continues to rely on manual controls will not be able to survive the cost and slow pace those controls, by their very nature, place on a company.

Longer-term shifts may be even more significant. The wide dependence on technology for all social transactions will continue to increase until it is thoroughly integrated into all aspects of living. Our wallets will become a thing of the past as all transactions will probably be executed through near field communication (NFC) and our smartphone. No more credit cards, loyalty numbers, health care cards, driver's licenses and boarding passes. In time, handheld devices will be what is necessary for any transaction, no matter the degree or complexity. The technology required to manage and secure this vast collection of data and provide fail-safes to ensure against disruption, as well as customer inconvenience, will be critical in positioning companies for success in the market.

> "Internet of things (IoT) will be the next wave of change."

Internet of things (IoT) will be the next wave of change. China appears to have marked this out as a new frontier and seems to be at the front end of investing in IoT. The Internet as we know it may change dramatically as information is shared between things and pushed to you based on who you are and what you do.

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:

All of these advantages will continue to place technology at the center of our social and economic connections. Technology, no matter what your business, will be a large part of defining your product and commercial success. One way of looking at this is that all companies will be technology companies that happen to sell metals or clothing or professional services.

Q **As someone who implemented the US Sarbanes-Oxley Act requirements, now more than 10 years since its inception, how do you see it as having changed business and the work of audit and risk professionals?**

A Sarbanes-Oxley, by design, was weighted toward financial disclosure controls. And although a challenge—both in time and cost—to implement, it helped to improve transparency. What it did not really clarify is the still occluded process of understanding an entity's strategy and the concomitant risk-appetite-to-risk-capacity equation that investors want to readily understand when making investment decisions. An entity's strategy and risk-appetite-to-risk-capacity discussion is a large-ticket item within ERM, about which we find that C-suite and boards are asking for assistance.

Q **Over your career, you have expanded beyond an initial focus on internal audit to a risk management and governance focus. Did you find this to be a natural progression? Do you have any advice for those considering a similar transition?**

A I have been very fortunate to have had the opportunity to move seamlessly between both worlds and have enjoyed the different sets of professional knowledge and challenges they each present. The expanded focus I have been able to have has enhanced my abilities and benefited my clients on both sides. On the internal audit side, I have a clear view of the larger risk factors, having been a CRO. And on the risk side, I do not lose sight of the importance and need for effective as well as efficient control structures.

While it has provided me a unique vantage point and lens from which to view issues, I would not say it would be a natural progression as a general rule, but rather something that I actively pursued to expand my skills and ultimately my career. If an individual's skill set comprises deep strength in internal audit and broad knowledge of risk combined with the intangibles related to executive management and successful board-level interaction, as well as industry recognition, then it could be a good fit for him/her.

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

A The biggest professional challenges I have faced have arisen from a risk assessment that showed a measureable mismatch among the strategy, risk appetite and risk capacity within an organization. I have seen in the industry where the appetite for risk outdistances the entity's risk capacity. This presents a dilemma in that the risk assessment work is fundamentally sound, but the mismatch may still exist. It is similar to overloading a seagoing vessel. The vessel may be well maintained, the crew may be qualified and trained, and the market may appear to want the product, but the unfortunate decision was made to overburden the vessel or take too risky of a course to market. Risk professionals are charged with pointing this out before the vessel leaves the port. It can be a career challenge as the vessel is still run aground because of too large a risk appetite or faulty navigation.

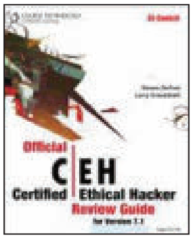
Lessons learned from this are to continue to do what you were hired to do, crystallize your message early and keep making that message known in a professional manner, understanding that even after you have diligently done your duty, the strategic direction taken may not be what you felt was most prudent.

Book Review

Steven J. DeFino, ECT, CTT+, SCNP, CISSP, ITIL, and Larry Greenblatt, CISM, CEH, ECSA, CISSP

Reviewed by Dauda Sule, CISA, marketing manager at Audit Associates Ltd., a consultancy firm that specializes in designing and organizing training programs pertaining to auditing, fraud detection and prevention, information security and assurance, and anti-money laundering. Sule previously worked in the Nigerian banking industry and was a systems security and assurance supervisor at Gtech Computers, a computer and allied services company.

Official Certified Ethical Hacker Review Guide, Version 7.1



Although the *Official Certified Ethical Hacker Review Guide, Version 7.1* is targeted toward individuals who wish to attain the Certified Ethical Hacker (CEH) certification, it could benefit anyone in the IT assurance, security and audit fields. Individuals with certifications such as Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP) and other information security assurance and risk management professionals will find this guide convenient in their work. While increasing their knowledge, it can also help these professionals ensure that their networks and systems are strengthened against hacking attacks and it provides an introductory guideline to performing penetration tests.

The guide is presented in an easy-to-follow, engaging language and includes practical examples in each chapter for the reader to try. The guide begins by introducing the concept of ethical hacking and then gradually builds on the process—how information is gathered on the target using passive techniques; the enumeration stage, which involves determining what can be obtained from a target; the actual system hacking; and introduction of malware, social engineering, denial of service, web servers, wireless networks, cryptography and more.

Since the guide is primarily meant to assist in preparation for the CEH exam, it includes 20 practice exam questions and answers for each chapter. In addition, there are extra resources included with the book: access to a web site with cheat sheets for practice memorization and drill skills; an access code to install and register CertBlaster test preparation resources, which simulate the CEH certification exam; and access to Cengage's information security community web site.

The guide is a must-have for anyone taking the CEH exam. Additionally, it can serve as a guide for anyone interested in starting a career in ethical hacking and penetration testing.

EDITOR'S NOTE

The *Official Certified Ethical Hacker Review Guide, Version 7.1* is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Kaya Kazmirci, CISA, CISM, CISSP, offers IT governance-related training and consulting services. He was previously the internal audit director in Istanbul, Turkey, for Avea, a mobile telecommunications operator. Kazmirci has more than 30 years of experience in information technology and business, with extensive experience in restructuring the IT function and implementing audit methodologies in large banks and telecommunication operators. Kazmirci's experiences include extensive reviews of financial management systems including banking, billing and charging, accounting and enterprise resource planning (SAP & Oracle) systems, and IT organizations. He is well versed in generally accepted IT standards and frameworks, such as COBIT, ISO 27001, WebTrust and SysTrust.

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:

Migrating From COBIT 4.1 to COBIT 5

Upgrading the Turkish Banking System

During the 1990s, numerous crises occurred in the Turkish banking sector (including several high-profile bank failures) that led to the development of a rigorous set of standards by the Turkish Banking Regulation and Supervision Agency (BRSA). All Turkish banks are required to become compliant with these standards. The first of these standards, *Banking Internal Audit and Risk Management Systems Communique*, related to technology infrastructure and was published in 2001. Subsequent related publications detailed the high-level approach that the first banking technology standard described, and mandated COBIT® implementation and compliance in all Turkish banks.

These standards[1] clearly state that COBIT compliance should be based on the most recent COBIT version. Therefore, on a biyearly basis, during the audit of 48 operating Turkish banks, all external auditors must complete COBIT-based IT audits and have a Certified Information Systems Auditor (CISA®), as well as a financial auditor, sign the related audit report. The resulting maturity assessments and audit results dramatically increased the Turkish banking industry's IT awareness as well as its IT control understanding. As a result, banking industry leaders learned of many control weaknesses, especially during those first audits, and implemented many technology and related control improvements.

Since all Turkish banks are required to use the current version of COBIT for statutory audits, the release of COBIT® 5 in 2012 initiated a reading frenzy for all who work in or around the Turkish banking sector.

The Turkish Banking Association (TBA) recently commented on the COBIT® 4.1 migration to COBIT 5 and its relevant impact on banking operations.[2] The TBA team[3] that completed the work on which this article is based recommends that each member bank form a work group with the members drawn from the bank's inspection board, operational process management and internal systems management departments. These work groups should each conduct a detailed review of COBIT 5 and then share their findings with each other (under TBA auspices), external auditors and the BRSA. The review's goal should be to outline a COBIT 5 implementation road map as well as to clearly define any improvement areas.

The consensus among the TBA team is that upgrading to COBIT 5 will have a value-added impact on both internal control systems and general banking operations. Areas that will require detailed planning and assessment prior to successfully migrating to COBIT 5 include:

1. **Organizational scope**—COBIT 5 is premised on an end-to-end approach to control. Optimally, IT operates in concert with all areas of the bank to provide seamless service, control and governance. While COBIT 4.1 was primarily implemented in the Turkish banking industry's technical purview, COBIT 5 implementation will require enhanced operational, audit and governance coordination and integration. Bank internal/external audit, inspection boards as well as industry, tax, antitrust and treasury regulators will need to clearly align with the BRSA standard and create transparent real-time governance coordination with stakeholders.
2. **Audit approach**—DSS06 *Manage business process controls* includes (within its scope) all banking activities. Traditionally, a bank inspection board's financial experts have audited banking operations and services, and bank IT auditors have conducted technology audits. COBIT 5 requires a coordinated approach that includes combined financial and technology teams focusing on specific operational processes and then reporting in a coordinated fashion to leadership.
3. **Assurance guidance**—Bank inspection boards will need to read the *COBIT® 5 for Assurance* publication for guidance during audit planning (scheduled for release in second quarter 2013).

4. **Assessing new and changed processes**—COBIT 5 includes several new processes and one new domain, as well as several processes that have been significantly revised. As existing experience with these processes is limited, the TBA team plans to utilize 2014 to assess and plan implementation as well as to rectify any potential conflicts with existing operations and/or approaches. The banking sector is presently assessing the new processes and developing a prioritized implementation plan.
5. **Process assessment model**—Changes in the COBIT Process Assessment Model (PAM) could lead to processes having lower maturity scores in COBIT 5 capability assessments. For example, a COBIT 4.1 control objective that attained a maturity score of two (repeatable) may not have sufficient documentation to achieve even a zero (if the process does not achieve its stated goals) in COBIT 5. COBIT 5 requires a minimum of work product (inputs and outputs), base practice and process outcome to be defined for a capability score of one. In contrast, a COBIT 4.1-based maturity assessment could result in the same score without any documentation.[4]
6. **Timing**—The process for migrating to COBIT 5 in an enterprise with an existing COBIT 4.1 implementation will require communication and consensus among all stakeholders, which should include, at a minimum, banks, external auditors and the BRSA. Achieving this consensus and developing a common implementation plan will take hard work on behalf of all related parties. How much time this development will take and when the work results will be accepted and implemented is under discussion. The BRSA has announced that, while COBIT 5's implementation in 2014 is possible, the related changes in operational scope, method and approach will be significant compared to COBIT 4.1. The BRSA further stated that it would continue to review the matter and make a broader announcement at a later date.[5]

CONCLUSION

Turkish Banks and external auditors appear to have significant work remaining to detail a COBIT 4.1 to COBIT 5 migration road map. This road map should include a clear description of COBIT 5 including organizational scope and responsibility (i.e., which departments will be responsible for implementing and auditing specific COBIT 5 processes and domains), a description of how the new and revised processes and domains are to be implemented and audited, and a detailed understanding of the COBIT 5 PAM's required documentation. Once this road map is complete, the Turkish Banking Industry can plan and schedule its upgrade to COBIT 5. The BRSA has announced that the earliest possible time frame for this migration is 2014; however, based on industry developments, a later implementation date is also possible.

ACKNOWLEDGMENTS

The author would like to thank the following experts for their invaluable support in crafting this article: Necdet Almaç, Murat Lostar, Mustafa Gülmüs, Emre Özbek, Izzet Gökhan Özbilgin, Ph.D., Aslı Dogrusöz, Emre Besli, Funda Çetintas, Betül Öz, Serdar Güzel, Barıs Bagcı, Cem Ergül and Barıs Yalçın.

ENDNOTES

[1] See Turkish Banking Regulation and Supervision Agency, "BRSA Regulation on Bank Information Systems and Banking Processes Audit to Be Performed by External Auditors," published in *The Turkish Official Gazette* dated, 13 January 2010, Nr. 27461, *www.bddk.gov.tr/WebSitesi/english/Legislation/8800regulationonbankingprocesses.pdf*. The Information Systems Audit Regulation, "Information System Audit," 24th article's second item specifies COBIT-based bank audits. The same document's "Definitions and Abbreviations," fourth article, first item, subitem f, defines COBIT as the most recent standard published by ISACA.

[2] Many members of the review team were also ISACA Istanbul Chapter COBIT 5 work group members who shared their work.

[3] Please see acknowledgments for a list of team members.

[4] COBIT 4.1 PAM was released in September 2011 and COBIT 5 PAM was released in the first quarter of 2013.

[5] BRSA, Letter to TBA regarding COBIT 5 use in IT and process audits, 4 January 2013

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

Rohit Bakhshi is a product manager with Hortonworks. Prior to joining Hortonworks, Bakhshi was an emerging technologies consultant at Accenture where he worked with Fortune 500 companies to incorporate big data technologies within their enterprise architecture.

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:

What Is Big Data and What Does It Have to Do With IT Audit?

For many years, IT auditors have been able to rely on comparatively elementary data analysis tools to perform analyses to draw conclusions. With the recent explosion in the volume of data generated for business purposes (e.g., purchase transactions, network device logs, security appliance alerts), current tools may now not be sufficient. By necessity, big data uses data sets that are so large that it becomes difficult to process them using readily available database management tools or traditional data processing applications. The paradigm shift introduced by big data requires a transformation in the way that such information is handled and analyzed, moving away from deriving intelligence from structured data to discerning insights from large volumes of unstructured data.

There is a lot of hype and confusion regarding big data and how it can help businesses. It feels as if each new and existing technology is pushing the meme of "all your data belong to us." It is difficult to determine the effects of this wave of innovation occurring across the big data landscape of Structured Query Language (SQL), Not Only SQL (NoSQL), NewSQL, enterprise data warehouses (EDWs), massively parallel processing (MPP) database management systems (DBMS), data marts and Apache Hadoop (to name just a few). But enterprises and the market in general can use a healthy dose of clarity on just how to use and interconnect these various technologies in ways that benefit business.

Big data not only encompasses the classic world of transactions, but also includes the new world of interactions and observations. This new world brings with it a wide range of multistructured data sources that are forcing a new way of looking at things.

Much of the work involved in conducting IT audits entails inspection of data generated from systems, devices and other applications. These data include configuration, transactional and raw data from systems or applications that are downloaded and then validated, reformatted and tested against predefined criteria.

With the sheer volume of data available for analysis, how do auditors ensure that they are drawing valid conclusions? What tools do they have available to help them? According to a report from Computer Sciences Corporation (CSC), there will be a 4,300 percent annual increase in data generation by 2020.[1] Currently, a one terabyte (Tb) external drive costs around US $80. It is very common for even medium-sized enterprises to generate one Tb of data within a short period of time. Using Excel or even Access to analyze this volume of data may prove to be inadequate. More powerful enterprise tools may be cost-prohibitive for many audit firms to purchase and support. In addition, the training time and costs may also prove to be excessive.

Transactions generated as a result of common business events, such as purchases, payments, inventory changes or shipments, represent the most common types of data. Also, IT departments increasingly record events related to security, availability, modifications and approvals in order to retain accountability and for audit purposes. IT departments also record more system-related events to enable more effective support with smaller staffs. Firewalls and security appliances log thousands of events on a daily basis. Given the sheer volumes of data, these security-related events cannot be manually analyzed as they were in the past. Marketing teams may record events such as customer interactions with applications, and larger companies also record interactions between IT users and databases.

There has been significant growth in the volume of data generated by devices and by smartphones and other portable devices. End users and consumers of information generate data using multiple devices, and these devices record an increasing number of events. The landscape has evolved from an Internet of PCs to an *Internet of things*. These things include PCs, tablets, phones, appliances and any supporting infrastructure that underpins this entire ecosystem.

Few of these new types of data were utilized or even considered in the past.

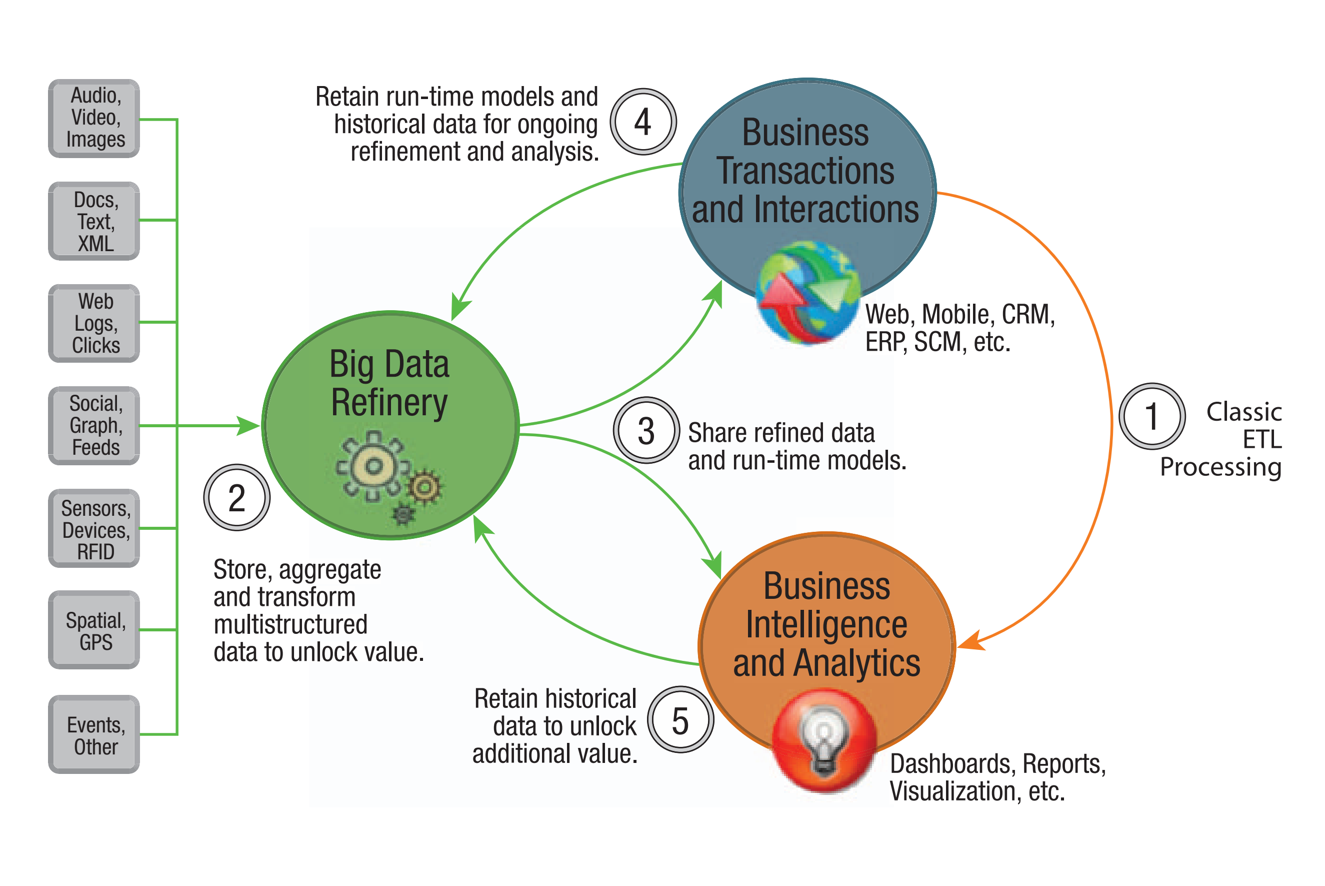
PAST AND PRESENT

Enterprise IT has been connecting systems via classic extract, transform, load (ETL) processing (as illustrated in step 1 of **figure 1**) for many years to deliver structured and repeatable analysis. In step 1, the business determines the questions to ask and IT collects and structures the data needed to answer those questions.

The big data refinery, as highlighted in step 2, is a new system capable of storing, aggregating and transforming a wide range of multistructured raw data sources into usable formats that help fuel new insights for the business. The big data refinery provides a cost-effective platform for unlocking the potential value within data and discovering the business questions worth answering with the data. A popular example of big data refining is processing blogs, clickstreams, social interactions, social feeds, and other user- or system-generated data sources into more accurate assessments of customer churn or more effective creation of personalized offers.

There are numerous ways for auditors to utilize the big data refinery. One instance is analysis of logs generated by firewalls or other security appliances. Firewalls and security appliances commonly generate thousands of alerts per day. It is unlikely that a group of individuals would be able to manually review these alerts and form meaningful associations and conclusions from this volume of data. Auditors could collaborate with IT to determine predefined thresholds to flag certain types of events and could even formulate countermeasures and actions

Figure 1—Maximizing the Value of Data


Audio, Video, Images
Docs, Text, XML
Web Logs, Clicks
Social, Graph, Feeds
Sensors, Devices, RFID
Spatial, GPS
Events, Other
Retain run-time models and historical data for ongoing refinement and analysis.
4
Business Transactions and Interactions
Web, Mobile, CRM, ERP, SCM, etc.
Big Data Refinery
2
Store, aggregate and transform multistructured data to unlock value.
3
Share refined data and run-time models.
1
Classic ETL Processing
Business Intelligence and Analytics
Retain historical data to unlock additional value.
5
Dashboards, Reports, Visualization, etc.

Source: Hortonworks, *http://hortonworks.com/blog/big-data-refinery-fuels-next-generation-data-architecture/*

to respond to such events. A centralized logging facility to capture all security events could also be utilized to relate certain types of events and assist in drawing conclusions to determine appropriate follow-up actions.

Another potential use for the big data refinery is in fraud analysis of large volumes of transactional data. Using predefined criteria determined in collaboration with other departments, the big data refinery could flag specific transactions out of a large population of data to investigate for potential instances of fraud.

The big data refinery platform provides fertile ground for new types of tools and data processing workloads to emerge in support of rich, multilevel data refinement solutions.

With that as a backdrop, step 3 of **figure 1** takes the model further by showing how the big data refinery interacts with the systems powering *business transactions and interactions* and *business intelligence and analytics*. Complex analytics and calculations of key parameters can be performed in the refinery and flow downstream to fuel run-time models powering business applications, with the goal of more accurately targeting customers with the best and most relevant offers, for example.

Since the big data refinery is great at retaining large volumes of data for long periods of time, the model is completed with the feedback loops illustrated in steps 4 and 5 of **figure 1**. Retaining the past 10 years of historical Black Friday[2] retail data, for example, can benefit the business, especially if it is blended with other data sources such as 10 years of weather data accessed from a third-party data provider. The point here is that the opportunities for creating value from multistructured data sources available inside and outside the enterprise are virtually endless with a platform that can perform analysis in a cost-effective manner and at an appropriate scale.

A next-generation data architecture is emerging that connects the classic systems powering business transactions and interactions and business intelligence and analytics with products such as Apache Hadoop. Hadoop or other alternate products may be used to create a big data refinery capable of storing, aggregating and transforming multistructured raw data sources into usable formats that help fuel new insights for any industry or business vertical.

One key differentiator for enterprises is the ability to quickly yield and act promptly upon key insights gained from seemingly disparate sources of data. Companies that are able to maximize the value from all of their data (e.g., transactions, interactions, observations) and external sources of data put themselves in a position to drive more business, enhance productivity, or discover new and lucrative business opportunities.

Emerging techniques allow auditors to draw key conclusions from a wide range and large population of data sources (internal and external). These conclusions or insights may reflect changes to the overall risk profile, new risk factors to the enterprise and specific internal risk factors such as material misstatement to financial reporting, fraud risk and security risk.

ENDNOTES

[1] Computer Sciences Corporation (CSC), 2012

[2] The day after the US Thanksgiving Day holiday, a major shopping day in the US

Jacqueline Medina, CIPP-IT, is affiliated with Booz Allen Hamilton, Virginia, USA.

Ryan Morrell, CISSP, is affiliated with Booz Allen Hamilton, Virginia, USA.

Dennis Pickett, CISSP, is affiliated with Westat, Rockville, Maryland, USA.

John Lumpkin is affiliated with the Eunice Kennedy Shriver National Institute of Child Health and Human Development, Maryland, USA.

Timothy McCain, CISM, is affiliated with University of Colorado-Colorado School of Public Health (USA).

Dina Drankus Pekelnicky is affiliated with University of Wisconsin (USA).

Alex Bengoa, MCSE, is affiliated with Tulane University (New Orleans, Louisiana, USA).

David Songco is affiliated with the Eunice Kennedy Shriver National Institute of Child Health and Human Development, Maryland, USA.

Considerations for Ensuring Security of Research Data in a Federally Regulated Environment

This article examines the challenges of implementing US federal information security requirements during the pilot (or vanguard) stage of a data-intensive study, and provides recommendations for others embarking on ventures of similar scope. Research data were collected by researchers at locations, or study centers (SCs), distributed throughout the US and were aggregated in a central repository to allow for analysis over the life of the study. Data were subject to federal security requirements during collection, evaluation, storage and transfer. This effort required coordination by numerous researchers, IT personnel and study administration at dispersed locations, utilizing differing hardware and software technologies.

The National Children's Study (NCS or "the study")[1] is the largest, most data-intensive study of children's health ever planned in the US. It will follow 100,000 children from conception to 21 years of age. The study will collect and track samples and data points from the children and their mothers and/or fathers for analysis by numerous qualified researchers. This requires an information management system (IMS) that is powerful, flexible and secure over time. The following analysis of the IMS models used by the study is undertaken from an organization perspective and, therefore, includes personnel, financial and logistical ramifications.

The NCS is a prospective, longitudinal study of the effects of environment and genetics on child health, growth and development in the US. Mandated by the Children's Health Act of 2000,[2] it is led by the Eunice Kennedy Shriver National Institute of Child Health and Human Development (NICHD) with a consortium of other federal agencies. Within the National Institutes of Health (NIH), NICHD provides resources and oversight and administers the funds for the study. Each SC also provides personnel, space and expertise. One principal investigator (PI) oversees the study at each SC, and is accountable for all research and IT needs.

REQUIREMENTS FOR A FEDERAL IMS

In addition to the obvious challenges of size, complexity and scope, this was the first cohort study of this size and duration required to comply with federal information security regulations (see US Information Security Regulations sidebar). The key regulations (Federal Information Security Management Act [FISMA][3] and US Health Insurance Portability and Accountability Act [HIPAA][4]) and their corresponding guidelines (e.g., National Institute of Standards and Technology [NIST] documents) provide an overarching umbrella that ensures stringent controls to protect the confidentiality, integrity and availability of sensitive information. FISMA requires that a federal risk executive representing enterprise management evaluates, mitigates or approves outstanding risk before a system "goes live." Although the NCS itself is not a HIPAA-covered entity, nearly every group with which the system will interact (hospital and university research groups) is. Therefore, the strategic decision was made to voluntarily maintain HIPAA compliance.

Risk assessment and management is the purview of a federal risk executive[5] who holds ultimate responsibility for risk-related decisions. This function is served by NICHD's chief information officer (CIO), the individual responsible for appropriate use and protection of information and IT. The CIO strives to enable the research mission of the study with a user-friendly IMS while ensuring the protection of information belonging to individual subjects and to the study.[6]

Leadership's security strategy is to ensure that controls are flexible and comprehensive enough to meet the changing needs of the study over time and to respond to the changing IT threat landscape and security implementation requirements.[7] Key challenges based on the study's variables, particularly growing user demand and operational requirements, are:

- Enforcing security controls on field equipment managed by third parties
- Establishing an identity and access management model to ensure trust in a multitude of dispersed organizations
- Implementing controls into the information life cycle management process that would be effective regardless of the type of device
- Ensuring adherence to baseline operational security controls at remote locations
- Implementing functional and secure procedures for handling hard-copy and electronic protected health information (PHI) and personally identifiable information (PII)
- Securely incorporating increasingly mobile platforms
- Ensuring chains of evidence and nonrepudiation policies throughout the IMS
- Constantly reevaluating risk and assessing efficacy of controls

Due to the involvement of human subjects, all aspects of the NCS are conducted in accordance with the design and specific provisions detailed in the Institutional Review Board (IRB) approved protocol, which includes provisions concerning human protections afforded by the informed consent process.[8] The NCS is committed to preserving the privacy of its participants and confidentiality of its data and, as a result, adopted an evolving security framework that ensures responsible data stewardship and is in line with federal requirements. The IMS was planned and implemented with these considerations. Ultimately, the NCS is able to provide a novel, flexible, comprehensive and accessible IMS.

FIRST IN CLASS

The study requires a secure, functional and flexible environment within a federally funded consortium of public and private institutions for a scientific endeavor of unprecedented scale, and boasts unique information security and privacy achievements. The varied restrictions and institutional risk tolerance of the different types of entities involved requires cooperation and compromise to create solutions that meet research needs and still mitigate risk to the study's data.

US INFORMATION SECURITY REGULATIONS

Federal agencies have a responsibility to ensure the appropriate use and protection of federal information and information systems as codified in the Federal Information Security Management Act of 2002 (FISMA). FISMA requires agencies to establish, document and implement agencywide programs to provide adequate information security and privacy safeguards that are "…commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information." (OMB Circular A-130)

To meet this mandate, agencies apply cost-effective technical and nontechnical controls to ensure systems and applications used by the agency, including those provided or managed by another agency, contractor or other source, operate effectively and provide appropriate confidentiality, integrity and availability of its information and information systems. Agency privacy officials, chief information officers (CIOs) and the Inspectors General conduct annual FISMA reviews of the agency's program.

Health plans, health care clearinghouses and covered health care providers (referred to as "covered entities") are responsible for ensuring the appropriate use, protection and disclosure of protected health information (PHI) as mandated by the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rules. The HIPAA Security Rule, similar to FISMA, requires effective risk management to adequately and effectively protect information in electronic form, specifically electronic PHI (e-PHI). Covered entities apply technical and nontechnical controls to provide appropriate confidentiality, integrity and availability of e-PHI.

HIPAA compliance efforts can be integrated with those for FISMA and the privacy provisions of the US E-Government Act of 2002 to broaden and enhance an agency's information security and privacy program.

The NCS was designed in stages, with a pilot to examine the feasibility, acceptability and cost of recruitment and operations, and a forthcoming main study to focus on exposure response. The vanguard stage allowed for optimization of several aspects of the study's operations and strategies. Common understanding and regular, clear communication with centralized oversight were critical in keeping so many varied SCs focused on the same goal with different paths. Study leaders and representatives of functional teams participated in weekly conference calls with PIs and composed formal guidance as necessary.

Collaboration among the many stakeholders evolved quickly as need forced creative solutions to problems. Communication channels and forums were established to provide consistent and reliable coordination. Scientists established consortium groups, listservs and virtual conferences to facilitate discussion among individuals or entities with similar issues. Strong interdependencies were created toward a mature functional and secure environment, as well as for successful data collection and interpretation. Stakeholders worked closely together to form unique solutions to security requirements, demonstrating that risk mitigation could be undertaken in different forms depending on need.

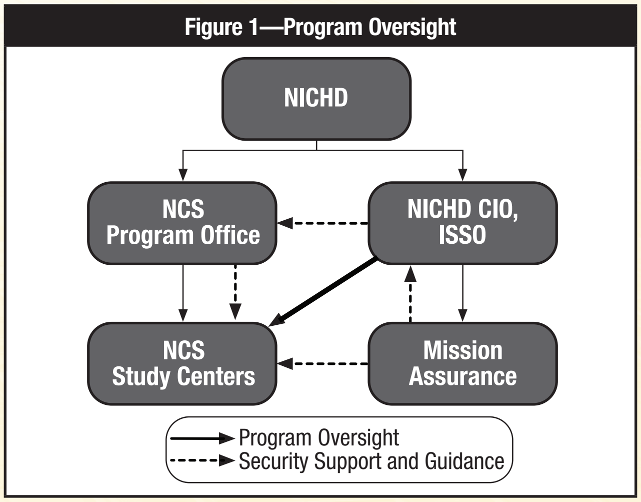
To address the size, complexity and evolving nature of the NCS, the program office (responsible for much of the planning, operations and logistics of the study) and the office of the CIO leveraged several functional teams with specific roles, responsibilities, tools and processes. The teams helped fill knowledge gaps, which varied widely among SCs. An information assurance team (mission assurance) was created to assist with security compliance, controls planning and implementation, documentation, and troubleshooting. A data access team was established to create and regulate data-use agreements mandated by system security policy and plans and necessitated by the interactions inherent in the model. A data analysis team functioned to ensure quality and integrity of data, especially with respect to data transmissions, and a federated institutional review board was put in place to ensure that human subjects were protected according to law. The program office, office of the CIO and mission assurance worked closely with each other and the SCs for continuous improvement and monitoring of security needs (**figure 1**).

This extended team was able to facilitate SC implementation by providing guidance on the compliance process customized for each SC's environment; however, this represented a large investment by the study.

EFFECTS OF FEDERAL REGULATIONS ON THE EVOLUTION OF THE IMS

Federal legislation and guidelines impacted individual SCs and the NCS as a whole. SCs perceived both benefits and challenges. In many cases, the perception depended on the organizational risk tolerance and capacity to address the regulations.

Figure 1—Program Oversight



Implementing federally mandated controls offered an opportunity to reexamine institutions' commitments to data security and the confidentiality of participant data. By aligning operations with the applicable regulations, researchers and institutions were able to operate within a defined security program framework and became more effective data stewards. This allowed for better management, assessment and identification of risk, which led to improved security, effective risk mitigation and, ultimately, better protection of study assets (e.g., equipment, data, staff, study mission).

Study leadership realized a long-term risk with the use of proprietary platforms that might not remain current and could not be modified, risking dependence on platforms that could not be secured and did not provide the capabilities needed. Likewise, they recognized that systems and system components may need to be reused or adapted for new uses and, therefore, emphasized interoperable, modular architecture so that any component of a data system could accurately and efficiently communicate with other data systems while adhering to international data standards.

While there were benefits, federal regulations presented many challenges to the NCS. Since SCs were derived from existing research institutions, NCS staff often worked on multiple projects and had to draw boundaries to maintain sensitive study data in isolation. Since systems had to be certified at an acceptable level of risk by a risk executive before data could be stored, transported or manipulated, many SCs were faced with setting aggressive timelines for risk mitigation, hindering their ability to assess, analyze, plan and budget appropriately. Failure to meet timelines often jeopardized project success and delayed the collection, submission and analysis of study data. These frustrations impeded local engagement of participants and collaboration with other SCs.

By detailing new and unfamiliar requirements for SCs and their staff, federal regulations caused staff push-back and frustration in some cases, including reluctance to do more than the minimum required to achieve and maintain compliance. This required PIs to maintain a higher level of responsibility and oversight of compliance than expected. Depending on the SCs' organizational features and familiarity with federal regulations, they may have perceived challenges as minimal or extensive.

CENTRALIZED MODEL

The study began with seven SCs, located throughout the US, using a centralized coordinating center that was responsible for oversight of information management and security. The program office and coordinating center developed protocols, guidelines and security specifications for the infrastructure of the data center, and the coordinating center distributed standardized equipment. With this centralized guidance and support, all SCs utilized the same processes (**figure 2**). While SCs were responsible for local (primarily physical and environmental) security, the majority of requirements and equipment were centrally developed and maintained, allowing SCs to focus on recruitment and data collection. Data were collected at the SCs and sent to the coordinating center.

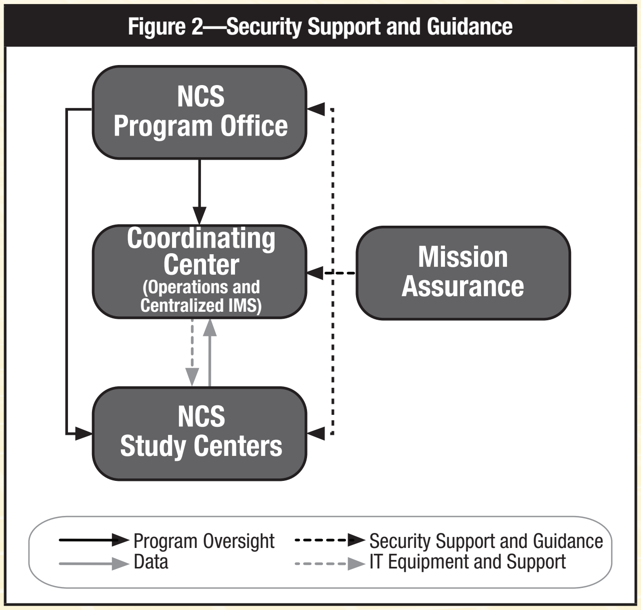
Several benefits were recognized with a centralized model:

- Knowledgeable support was consistent, allowing SCs to become acclimated to regulations quickly and with little local resource investment.
- A central team leveraged lessons learned to take advantage of economies of scale.
- Centralized storage facilitated reliable access and consistent security for data.
- Control implementation was standardized across sites, and all stakeholders understood the status of the others.

Some challenges were created by minimal local management and control:

- Equipment, such as laptops, sent to SCs from the coordinating center was restricted to NCS use, necessitating that staff working on multiple projects use multiple laptops.
- Security restrictions added to local overhead and cost.
- SCs lacked opportunity to develop a comprehensive understanding and local capacity to fully manage regulations, both for the NCS and for future projects.

Figure 2—Security Support and Guidance



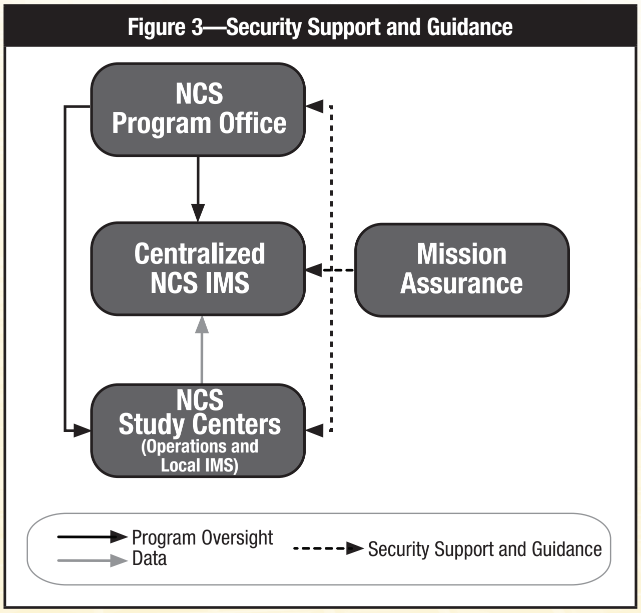
FACILITATED DECENTRALIZED MODEL

As the NCS grew to 40 locations throughout the US, it migrated to a facilitated decentralized model. The study provided standardized specifications on how to collect and transmit data, and the geographically distributed SCs implemented a variety of local, modular informatics solutions for case management and data acquisition.[9] They were responsible for coordinating their own security and leveraged local expertise for flexible, tailored information management, while the NCS provided centralized assistance and guidance.[10] SCs submitted data to a central archive and maintained a local copy (**figure 3**).

This model had some obvious and some unforeseen benefits:

- SCs had greater flexibility and control in implementing solutions to requirements in a way that met local needs.[11]
- Compliance with federal regulations aligned well with institutions' regulatory governance around other types of sensitive data, allowing institutions to bolster their local regulatory governance programs.

Figure 3—Security Support and Guidance



- The extended community recognized additional benefits, such as increased reporting on phishing and other media threats after training or discussions of security topics resulted in increased stakeholder awareness.
- PIs perceived more control and ownership over data, and were more involved in the compliance process.
- SCs built local capacity and knowledge, positioning them to better compete for additional federally funded studies with similar requirements or related technical evaluation criteria.[12]
- Personnel became compliance leaders at their institutions, leveraging lessons learned and collaboration for a better understanding of applicability and process implementation.[13]
- SCs were able to heavily leverage existing space, knowledge or capabilities from other departments within the hospital or university.[14]

Drawbacks were varied, and required readily available, centralized expertise:

- A greater acceptance of risk was required in this model, which drove a greater need for risk management at both the SC and program-office levels, incurred greater cost, and affected schedules negatively.
- Variety in available skills, knowledge and experience at SCs led to different implementation of controls and to varied levels of security, risk and data accessibility across sites.
- Some SCs were not fully aware of requirements and not well prepared to implement solutions. Some did not see the value of regulations or were frustrated by the complexity and costs, and hoped to minimize compliance efforts.
- IMS customization required a minimum level of knowledge and experience locally. Controls presented time and resource challenges to entities that were not familiar with requirements.
- Additional complexity for SCs with multiple locations, sometimes with differing contract periods, was created by the sharing of a single, local system.
- The compliance process was slow—years for some SCs. Delays in achieving compliance had a ripple effect on collecting, submitting and analyzing data, as well as on collaborating across SCs.
- Researchers with little information security knowledge were sometimes pulled from their core competencies to focus on compliance.
- SCs struggled with determining local needs and budget.
- Many controls, such as multifactor user authentication credentials and systems, were expensive and labor-intensive to implement.

SCs varied in how they handled achievement of federal compliance, but one common practice that served sites well can be considered. Among the University of Colorado (USA), University of Wisconsin (USA) and Tulane University (Louisiana, USA) SCs, a single position was created that oversaw all IMS, IT, data and security compliance work. Centralized oversight allowed for the creation of an overarching IT program that met the overlapping needs of data quality, IMS functionality, hardware and network needs, and compliance requirements. At Colorado and Tulane, these positions were assigned to IT managers within the institution, while Wisconsin created a new position external to the IT department.

LESSONS LEARNED

In a study of this size and with this many stakeholders, some lessons were hard-earned and future studies may benefit from knowing what worked within this diverse group.

- Information security had to be about mitigating risk while facilitating the mission, not about enforcing rigid controls without consideration for downstream effects.
- Management buy-in was critical throughout to develop and modify policy and to provide access to supplementary funding and resources.
- An active community with PIs, IT personnel and enterprise management worked together with centralized oversight and expertise, and was successful in developing creative solutions.
- The application of controls required proper scoping of the IMS environment, or boundary, within which to secure sensitive information.
- Controls, such as the IMS and security program, needed to be extensible to stand up to the addition of components.
- A surprising number of controls were addressed through administration; even more were addressed with a smaller technology footprint than expected due to overlap in family coverage for control applicability. Understanding the essence of the requirement was the foundation for achieving and maintaining compliance with federal and organization-specific mandates.
- In this large consortium, many stakeholders were not technically savvy and required special considerations to ensure continued investment. Communication and targeted messaging were crucial to this process.
- Policy and procedures had to be developed alongside stakeholders and disseminated thoroughly, with contract and procurement authorities educated before their services were required, and more time than normal allocated for developing or modifying contracts.
- Researchers and other stakeholders recognized peripheral benefits after compliance was achieved and the IMS and related systems went live.[15]
- In many cases, existing infrastructure, controls and experience with the process created resources that could be leveraged for subsequent solicitation responses. Reduced overhead and time investments were recognized in the planning of future studies.
- Oversight personnel had to be able to pull in resources for appropriate expertise or surge support.

CONSIDERATIONS FOR THE DECISION-MAKING PROCESS

The decision to meet (or to pursue projects that require meeting) federal information security requirements is a major decision that should be undertaken at the enterprise level after thorough risk/benefit analysis, as with any major institutional investment. Costs can be high. In the model described here, with a data center collecting data from SCs, compliance with federal requirements cost approximately US $200,000 per year centrally, and US $50,000–150,000 per year per SC. SCs with IT departments dedicated one to two full-time personnel; others hired staff to fulfill this role. Many without dedicated IT staff hired contractors for US $50,000–100,000.

Other considerations include:

- For many federally funded studies, all security controls must be implemented or the unmitigated risk accepted by the risk executive prior to use of the IMS for data storage. Researchers should work with IT personnel to understand their existing infrastructure, resources available, necessary steps and timeline before applying for a grant or contract requiring federal compliance.
- The institutional effects of security compliance should be considered. For instance, a secure system that may be leveraged by a department or institution may be considered a long-term investment. The consideration for unforeseen funding and personnel needs can be seen in the context of organizational risk management.
- Compliance is not a one-time event and cannot be delegated to the IT department. It must include management and business stakeholders from inception to identify components to include for long-term operations. Not including all stakeholders early can lead to scope creep as additional interconnections, data flows, system interactions, accessibility, personnel and infrastructure gaps are identified later.

> “Compliance is not a one-time event and cannot be delegated to the IT department.”

- A local gap analysis using the NIST guides should be conducted early by an objective entity (security consultant or risk management expert) to assess the IT security posture. This can help identify areas where remediation is required and give a good foundation for compliance documentation.
- An open-source model should be considered. NCS leadership believes it provides a greater long-term strategic advantage due to its flexibility in deployment and extensibility with other technologies.

- FISMA considerations on open-source products should be given thought with respect to vulnerability assessment and patching. Nonproprietary products may be more sustainable in the long run, but may require a higher level of effort for initial customization and for long-term upkeep. It is important when conducting a risk assessment on any open-source technologies to consider the support community's track record of addressing the risk.
- The PI and IT personnel should choose an IMS model (i.e., centralized, facilitated decentralized, other) that suits their needs, but must also weigh benefits and risk. Making the correct decision for all stakeholders up front will save time and money and will facilitate research and data stewardship.
- Latitude to engage sponsoring agencies and contractors should be provided, and service level agreements (SLAs) with decentralized branches of the organization must have the necessary provisions for raw data access and interconnections for remote activities.

RECOMMENDATIONS AND NEXT STEPS

Entry into research that requires federal IMS oversight should not be undertaken lightly, as it creates burdens to IT and security governance programs as well as to scientific personnel. However, requirements are far from insurmountable and do confer benefits to researchers and to their institutions.

All available resources should be leveraged for optimal and efficient results. A thorough gap analysis should be conducted and consider institutional hardware, space, personnel, knowledge and existing security controls before committing to federal mandates. Real benefits are seen when projects can leverage existing resources, producing economies of scale. Aligning with a known entity around existing regulations (international, federal, organizational) makes them simpler to understand, enforce and disseminate. If resources allow, knowledgeable consultants should be leveraged to help get started, educate staff, answer questions and assist with stakeholder buy-in.

It is important to invest all stakeholders as key partners, share all information freely, and communicate clearly and frequently. A thorough understanding of risk and threats should be maintained, and decisions on how to implement controls should be approached in a collaborative manner. Effective implementation of many controls requires specific knowledge and behavior by stakeholders, and a belief in and understanding of benefits ensures cooperation. For optimal benefits, forums, training and other group activities should be created to leverage the problem-solving skills of the greater group and to keep different functional groups communicating. Security personnel should take time to understand the needs of the researchers in order to accurately weigh risk against mission need. Centralized expertise must be available to leverage lessons learned, provide templates and standard operating procedures, and keep all parties headed in the correct direction.

An organization should not attempt to begin the business and research processes until it has established a sustainable level of compliance and mitigated risk that would not be acceptable in a federally regulated environment.

ACKNOWLEDGMENTS

This manuscript was developed by a writing team identified by the National Children's Study (NCS) Publications Committee for the purpose of timely sharing of centrally collected NCS data. It is thus a primary NCS publication. This project has been funded with federal funds from the US National Institutes of Health, Department of Health and Human Services, administered by the Eunice Kennedy Shriver National Institute of Child Health and Human Development under contract nos. HHSN2752010000072U, HHSN275200800018C, HHSN275201100014C, HHSN275200503396C and HHSN275200800010C.

REFERENCES

National Institute of Standards and Technology (NIST), *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53 revision 3, USA, 2009, *http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf*

NIST, *Managing Information Security Risk (Organization, Mission, and Information System View)*, SP 800-39, USA, 2011, *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf*

NIST, *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems*, February 2004

NIST, *Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems*, March 2006

Bolten, Joshua; Office of Management and Budget Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, The White House, 26 September 2003, USA, *www.whitehouse.gov/omb/memoranda/m03-22.html*

Evans, Karen; Office of Management and Budget Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, The White House, 12 July 2006, USA, *www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf*

The White House, Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, revised 28 November 2000, USA, *www.whitehouse.gov/omb/circulars_a130_a130trans4/*

ENDNOTES

[1] The National Children's Study, *www.nationalchildrensstudy.gov/Pages/default.aspx*

[2] 106th Congress, Public Law 106-310, *www.gpo.gov/fdsys/pkg/PLAW-106publ310/html/PLAW-106publ310.htm*

[3] Congress, Federal Information Security Management Act (FISMA), P.L. 107-347, title III, USA, December 2002

[4] Congress, Health Insurance Portability and Accountability Act, P.L. 104-191, USA, August 1996

[5] National Institute of Standards and Technology (NIST), US Department of Commerce, *Guide for Applying the Risk Management Framework to Federal Information Systems*, SP 800-37, Revision 1, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

[6] The National Children's Study, "Connecting the Dots: How Computer Innovation Supports the National Children's Study," December 2009, *www.nationalchildrensstudy.gov/newsandevents/eupdates/Pages/e-update-12-2009.aspx#dots*

[7] Modi, Tara; "FISMA 2010: What It Means for IT Security Professionals," *ISACA Journal*, vol. 5, 2010, USA

[8] Institutional Review Board (IRB), 45 CFR & 46, parts A through D

[9] Hirschfeld, Steven; David Songco; Barnett S. Kramer; Alan E. Guttmacher; "National Children's Study: Status in 2010," The National Children's Study, 2011, 78(1), p. 119–125

[10] Hirschfeld, Steven; Barnett Kramer; Alan Guttmacher; "Current Status of the National Children's Study," *Epidemiology*, vol. 21, no. 5, September 2010, USA, p. 605-606

[11] As an example, Tulane University (New Orleans, Louisiana, USA) adapted single sign-on for researchers across its platforms, which was not possible within the centralized model.

[12] University of Wisconsin (Madison, Wisconsin, USA), University of Colorado-Colorado School of Public Health (Aurora, Colorado, USA) and Tulane University experienced the building of institutional knowledge and expertise under the facilitated decentralized model, making the SCs' IT leaders campus resources for FISMA projects.

[13] One active and resourceful group was the Governance in Information Systems and Security in Technology Consortium, a collaboration led by University of Colorado and Tulane University SC personnel. The consortium brought together IT leaders from SCs for biweekly security discussions and allowed real-time problem solving within the community focused on achieving federal compliance through guidance from the mission assurance team and program office and through lessons learned from other SCs. The group focused on concrete examples in interpreting security controls and how they were applied in specific environments.

[14] In the case of the University of Wisconsin, the existing clinical translational science awards office on campus was familiar with federal regulations and shared existing personnel and knowledge. Their server rooms had physical controls in place that the SC was able to leverage. In addition, staff members were available year-round to assist with needs for surge support and to provide expertise; thus, challenges to SC IT staff resources were somewhat diminished.

[15] As evidenced by the Colorado, Wisconsin and Tulane SCs, establishing a FISMA-compliant system within a private enterprise created additional funding opportunities for all PIs on campus.

IT Security Responsibilities Change When Moving to the Cloud

Larry G. Wlosinski, CISA, CISM, CRISC, CAP, CDP, CISSP, ITIL, is a professional IT security consultant at Earth Resources Technology Inc. and has more than 37 years of experience in IT security. Wlosinski's security experience includes policy and procedure writing, planning, information assurance, continuous monitoring, security and risk assessments, incident response, network and data security, contingency planning, and security awareness and training. He is also a past president of the Niagara Frontier Chapter of the Data Processing Management Association (DPMA). Wlosinski has spoken on cloud security at federal and professional conferences and has conducted many classes on various IT security topics.

How will an organization's information security staff be affected if the organization's computer systems are moved to a cloud environment? What about the change in responsibilities within the organization and the expectations of the cloud service provider (CSP)?

While the three common cloud delivery models[1]—Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)—are pretty well known and described in literature, the latest service being defined by the Cloud Security Alliance (CSA) is Security as a Service (SecaaS).[2] SecaaS "provides third-party facilitated security assurance, incident management, compliance attestation, and identity and access oversight. SecaaS is the delegation of detection, remediation, and governance of security infrastructure to a trusted third party with the proper tools and expertise."[3] SecaaS covers 10 security domains that include products and/or services, which are available from many vendors, to manage security concerns with an organization's cloud provider.

For PaaS, the organization and the provider share the responsibility for the application and the virtual management environment; the CSP provides and manages the control of the server, data storage and network services. For IaaS, the organization is responsible for the application and the responsibility of the virtual management environment is shared with the provider. For SecaaS, the vendor or designated contractors provide the products and/or services that support the cloud environment.

The cloud environment participants fall into the following categories:

- **Consumer/end user**—Owner of the data (person or enterprise)
- **Cloud service provider**—An organization that makes the service available
- **Cloud service requestor**—The enterprise's technical staff (e.g., architect, developer, business manager, IT manager)
- **Cloud SecaaS provider**—The vendor (e.g., an independent assessor[4]) that provides the product and/or IT security service in lieu of the enterprise's employees
- **Auditor**—Independent IT security assessor
- **Service broker**—An enterprise (examples of service brokerages include Intel and McAfee) that offers intermediation, monitoring, transformation/portability, governance, provisioning and integration services, and negotiates relationships among various CSPs and consumers
- **Carrier**—Telephone (or data communication) line intermediary between provider and consumer

CLOUD PARTICIPANT RESPONSIBILITY BREAKDOWN

The breakdown of responsibilities can fluctuate considerably based on the size variations of organizations (from small to large). The following is a baseline breakdown of responsibilities that may be implemented, to some degree, in organizations that have utilized one or more of the cloud delivery models.

The end user (or requesting enterprise) is responsible for:

- Security awareness of everyone involved with implementing, operating and maintaining the system
- Access agreements, such as contracts, service level agreements (SLAs) or other joint agreements
- Malicious code protection, such as antivirus software and continuous monitoring of the network and application

The IT security responsibilities of the CSP include:

- Application partitioning and information remnants in the infrastructure
- Security function isolation and resource priority of the platform
- Boundary protection of the application

- Regular audit and continuous monitoring to analyze, repair, verify, track and capture malicious activity
- Monitoring for unauthorized configuration changes
- Utilizing monitoring tools to maintain a secure information systems (IS) environment
- Backup and recovery to assess that contingency planning occurs and testing is performed
- Environmental controls for the customer and the provider
- Physical access for the customer and the provider

IT security controls managed by the end user or CSP (depending on the service model) include:

- Account management
- Account enforcement
- User identification and authentication
- Device identification and authentication
- Authenticator management
- Cryptographic key establishment and management

Shared responsibilities of the end user and CSP include:

- Access control to the data, system and server environment
- Data and media protection of all storage devices
- Maintenance (configuration management)
- Incident response participation and reporting
- Personnel security (including background checks)
- Contingency planning for the user organization and the CSP locations

The architect of the end user is responsible for:

- Information flow enforcement
- Acquisition of network services to the SecaaS and CSP
- IS documentation

From a cloud model perspective, there are two types of application developers, meaning the writer and tester of the program code. For a SaaS application, the developer is the vendor that offers the system/application. For PaaS and IaaS systems/applications, the developer is the user organization. For both types of developers, the following responsibilities apply:

- Security training of, for example, the programmers, administrators, help desk and users
- Life-cycle support for updating current applications and installing new ones
- System configuration (for the developer who turns the system over to production) and the hosting environment
- Security testing of the applicable controls[5]
- Flaw remediation of source code (this is the responsibility of the organization that wrote the application)

- Baseline configuration. The baseline is the responsibility of the developing organization (for SaaS, it is the vendor; for IaaS and PaaS, it is the end user).
- Configuration change management. This responsibility is separated from the security staff as part of security control, known as segregation of duties.
- Access restrictions for change. This control applies to user accounts and system administration; application of this control depends on the cloud delivery model.

The end user's business manager is responsible for:

- Risk assessment and updates, which may be performed by in-house staff or by an organization that provides the service, such as the Federal Risk and Authorization Management Program (FedRAMP)
- Allocation of resources (e.g., staff, funding)

The end users' IT manager is responsible for:

- Access control policies and procedures
- Account management
- Audit review, analysis and reporting
- Security awareness and training policy
- Security assessment and authorization policy and procedures
- IS connections
- Configuration management policy and procedures
- Contingency planning policy, procedures and plans
- Identification and authentication policy and procedures
- Incident response policy and procedures
- Security planning policy and procedures
- Third-party personnel security
- System and communications protection policy and procedures
- System and services acquisition policy and procedures
- External IS services

The third-party auditor is responsible for:

- Security assessment
- Security certification

- Security accreditation

The service broker is responsible for:

- Relationship negotiation
- Managing the use, performance and delivery of services

The carrier (telecommunication or data line provider) is responsible for:

- Denial-of-service (DoS) protection
- Transmission integrity
- Transmission confidentiality
- Trusted path

SECAAS IT SECURITY DOMAINS

The SecaaS vendor can be responsible for one or more of the 10 IT security domains according to the interconnection agreement. The 10 IT security domains for SecaaS as defined by the CSA are:

1. **Identity and access management**—This includes authentication, identity management, single sign-on, provisioning/deprovisioning, centralized directory services, privileged user management, access management, authorization management, access policy management, and audit and reporting.
2. **Data loss prevention (DLP)**—This includes data sovereignty; setting and enforcing policy; legal/regulatory requirements; geographic, architectural, storage, end-point and encryption considerations; and forensics.
3. **Web security**—This includes the existing infrastructure, proxy configuration, antivirus, antispyware, compliance, social network/blog access, URL filtering, queries, alerts and the audit trail.
4. **Email security**—This includes data security and protection, regulatory compliance, data residency, unauthorized disclosure, malware, spam protection, encryption, records retention/data destruction, system management and logging, and mobile devices.
5. **Security assessment**—This includes legality and nondisclosure agreements; standards; architecture; inventory; baseline configurations; process flow; logging; continuous monitoring; common requirements; data access; tools; accuracy and coverage; provider infrastructure; secure communication, reporting and sharing of results; and penetration testing.
6. **Intrusion management**—This includes intrusion detection and response; intrusion management; service level agreements; governance, regulatory and compliance issues; and financial, technical, security and architectural issues.
7. **Security information event management (SIEM)**—This includes log data management, risk management, regulatory and compliance requirements, incidents and events, SLAs, information sharing, and inputs and outputs.
8. **Encryption**—This includes data availability, key management, securing the client, policy and enforcement, data integrity, data at rest, data in transit, data in use, and data destruction.
9. **Business continuity and disaster recovery planning**—This includes the SLA; jurisdiction of the data; data protection/encryption; separation of duties; access controls; metadata retention, separation and protection; resilience; licensing; and failover automation.

Figure 1—SecaaS Security Posture

Category	Domain	Protective	Preventive	Detective	Reactive
1	Identity and access management	X	X		
2	Data loss prevention		X		
3	Web security	X		X	X
4	Email security	X		X	X
5	Security assessment			X	
6	Intrusion management	X		X	X
7	Security information and event management			X	
8	Encryption	X			
9	Business continuity and disaster recovery planning	X		X	
10	Network security	X		X	X

Figure 2—Mapping of SecaaS Domains and Cloud Delivery Models

Category	Domain	SaaS	PaaS	IaaS
1	Identity and access management	X	X	
2	Data loss prevention	X	X	
3	Web security	X	X	
4	Email security	X		
5	Security assessment	X	X	X
6	Intrusion management	X	X	X
7	Security information and event management	X	X	
8	Encryption	X	X	X
9	Business continuity and disaster recovery planning	X	X	
10	Network security	X	X	X

10. **Network security**—This includes the network model, network access controls, content inspection and control, distributed DoS protection, virtual private network (VPN) and Multiprotocol Label Switching (MPLS) connectivity, forensic support, traffic capture, and resources.

Figure 1 presents the security posture (i.e., protective, preventive, detective, reactive) for each SecaaS domain.

Figure 2 is a mapping of the SecaaS domains to the cloud delivery models.

More detailed information on the CSA SecaaS domains can be found on the CSA web site,[6] where one can also find sample vendors, by domain, that can provide support in the way of software, hardware and/or staff to satisfy an organization's needs. To effectively utilize these services, the organization needs to implement contractual relationships, adjust its security architecture and reevaluate staff assignments to determine who is tasked with performing the job functions and security responsibilities described here.

CONCLUSION

Enterprises working in or planning a transition to computer systems working in the cloud should consider the job function responsibilities of their technical staff and evaluate their skills and weaknesses. In some cases, it may be beneficial to change job descriptions, and in some cases, it may be necessary to provide them the training they need to function effectively. Remember that the enterprise's administrators and programmers were trained to develop the new environment because of the changes in software, systems and appliances; therefore, the operational staff can also benefit from learning any new skills associated with moving to the cloud environment.

ENDNOTES

[1] Jansen, Wayne; Timothy Grance; *Guidelines on Security and Privacy in Public Cloud Computing*, NIST Special Publication 800-144, National Institute of Standards and Technology, December 2011, *http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf*

[2] Cloud Security Alliance (CSA), *Security Guidance for Critical Areas of Cloud Computing Version 3.0*, 14 November 2011, *https://cloudsecurityalliance.org/research/security-guidance/*

[3] *Ibid.*

[4] An example of an independent assessor is the Federal Risk Authorization Management Program (FedRAMP), a US federal government organization that supports federal agency efforts in certification and accreditation of cloud systems hosted at vendor locations.

[5] Sample responsibility designations can be obtained from the FedRAMP *(www.gsa.gov/portal/category/102371)* and the CSA *(https://cloudsecurityalliance.org)* web sites.

[6] *https://cloudsecurityalliance.org/research/secaas/#_downloads*

Santhosh Patil is a principal in Infogix Inc.'s Strategic Services practice. Patil assists industry-leading enterprises in assessing information risk, aligning business problems with strategic planning, advisory and technology solutions. Previously, Patil has worked in consulting positions across several industries including health care, property and casualty insurance, trading and risk management, investment banking, and hedge funds.

Information Controls and Monitoring Framework for Health Care Organizations

Charting the Path to Bring Efficiency in Business Operations and Reduce Administrative Costs in Support of Health Care Reforms

Health care spending is a key component of any industrialized nation's economy. In many countries, not including the US, basic health care affordability is ensured through universal insurance or taxpayer funding. Health care spending in the US is by far greater than any other developed nation in the world. Thus, US health care organizations must find ways to reduce administrative costs, increase efficiency of operations and ultimately make quality health care affordable to all insured, in a radically altered playing field due to ongoing health care reform and regulations. With the accelerating use of real-time data exchanges and increasing complexity of health insurance and information exchanges, the need for validating and tracking key information is critical to manage information risk and ensure compliance with regulations that meet many of the US Affordable Care Act (ACA)[1] provisions.

Organizations across the health care value chain, including payers, providers and a myriad number of intermediaries, recognize the urgent need to manage cost and improve performance in their core business operations to cope with an expanding array of regulatory and standard requirements such as the International Classification of Diseases (ICD) 10,[2] the US Health Information Technology for Economic and Clinical Health (HITECH) Act[3] and the National Association of Insurance Commissioners Model Audit Rule (NAIC-MAR).[4] More specifically, the ACA requires health care payer organizations to establish procedures to simplify administrative operations and reduce costs without compromising the service level. This involves adopting a single set of standards and operating rules between health providers for claims processing, eligibility verification, electronic fund transfers for payments, enrollment and disenrollment. Health insurance firms will also need to deal with a tax on revenues and a cap on profitability in the small group and individual markets. Health care organizations that are not able to document compliance may be fined up to US $1 per covered member per day, which can quickly turn into millions of dollars in penalties, specifically for large health insurers.

KEY BUSINESS DRIVERS AND IMPLICATIONS

As health insurance organizations plan to overhaul their processes and systems in order to deliver on the mandated requirements and meet the deadlines imposed, they are bound to face significant challenges:

- **Transition to ICD-10:** While some countries in the world are in the process of adopting ICD-11 (11th revision of ICD, available in 2015), the US health care system is surging toward adoption of ICD-10 by late 2014. Operational implications may arise out of reengineering the current systems within the claims systems, payment processing and health information analytics.
- **Transition from batch to real-time systems:** Gateways to health information are moving into distributed real-time systems resulting in a greater need for tracking information flows.
- **Replacement of market forces with new audit and compliance requirements:** In order to be compliant with regulations set by NAIC-MAR/Sarbanes-Oxley, sufficient documentation will be necessary for insurance organizations to audit operations of historical claims, payments and enrollments.
- **Integration of health insurance exchanges:**[5] Starting in 2014, individuals and some employer groups in the US will be able to buy health insurance in marketplaces called health insurance exchanges. A new set of enrollments in small group and individual segments will require business-to-business reconciliation and

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:

balancing of enrollments and subsidies across exchanges, trading partners and payers.

- **Impacts of electronic health records (EHR):**[6] Widespread usage of electronic health information can adversely affect the integrity of member claim information.
- **Policy-level changes aimed at universal coverage and Medicaid expansion:** An increase in enrollments will result in new data validation, verification and measurement requirements.

INFORMATION CONTROLS FRAMEWORK FOR HEALTH CARE ORGANIZATIONS

With changes in health care organizations happening on a massive scale in the US, there is a strong need to effectively manage information exchanges across their operations. Organizations should establish strategies to perform information systems (IS) control and audit to overcome the challenges facing the industry. The Enterprise Operational Information Management Framework is one such controls framework that encompasses a standardized approach to deploy information management controls, monitoring and measurement capabilities across business operations of a payer organization. Some of the salient features of the framework are illustrated in **figure 1**.

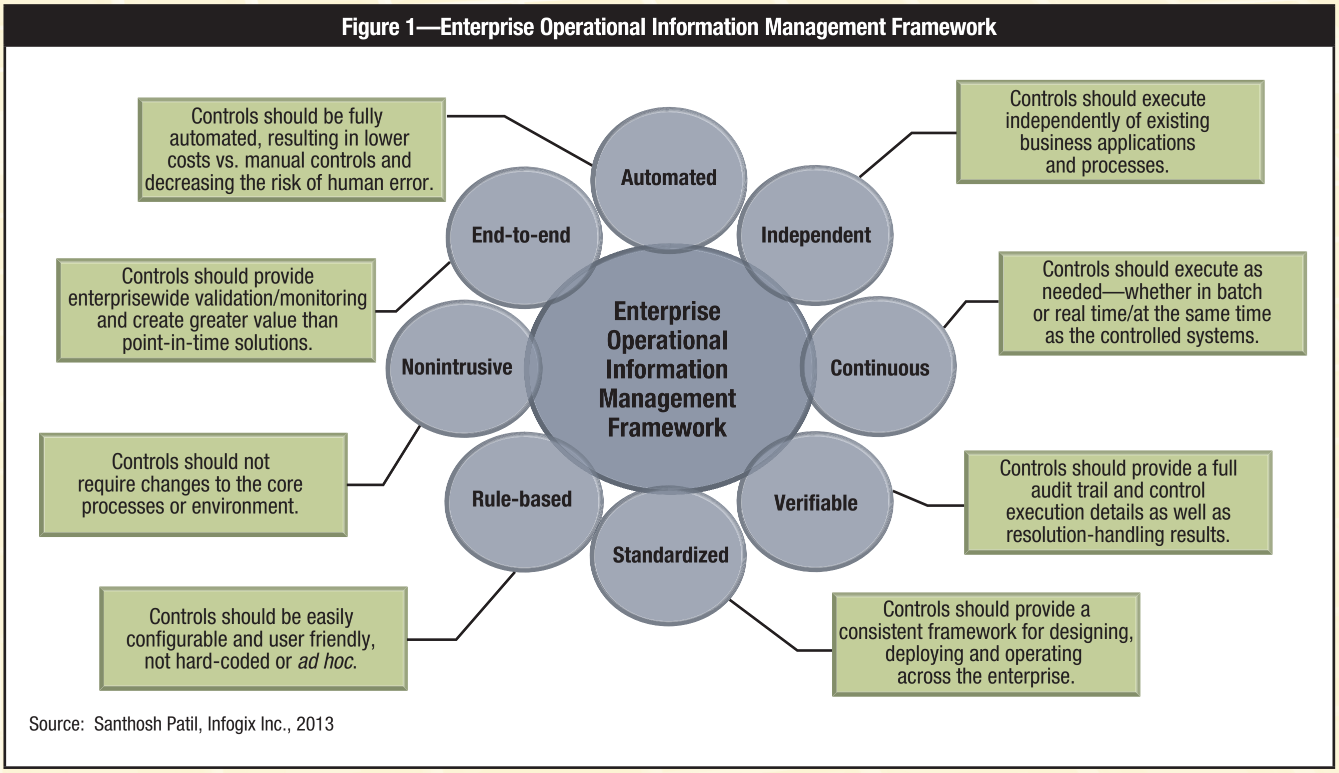
ACHIEVING OPERATIONAL EXCELLENCE THROUGH INFORMATION CONTROLS

While US health care organizations are making drastic changes, it is critical to have effective information controls in place to achieve operational efficiency and reduce costs. The following are some critical insurance processes in which health care organizations across the world could benefit from automated information controls.

Sales and Enrollments

Starting in 2014, the establishment of health insurance exchanges by certain US state and federal agencies is expected to expand insurance coverage and increase affordability to many individuals and employer groups in the US. Many payer organizations are in the midst of building new processes and systems with the goal of integrating with exchanges and other channels to allow enrollment of a new set of members, as illustrated in **figure 2**. Robust validation and monitoring are necessary to ensure this process. Automated validation

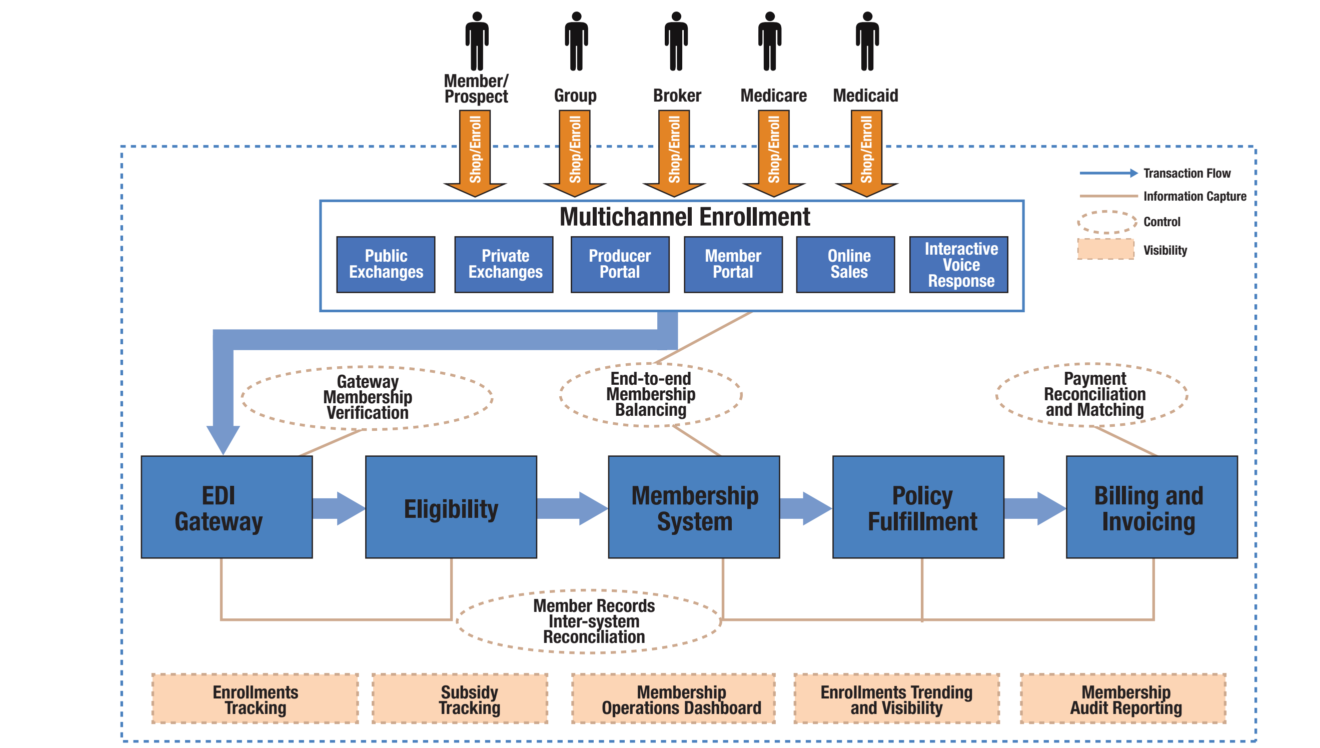
Figure 1—Enterprise Operational Information Management Framework



Enterprise Operational Information Management Framework
Automated
Independent
Continuous
Verifiable
Standardized
Rule-based
Nonintrusive
End-to-end
Controls should be fully automated, resulting in lower costs vs. manual controls and decreasing the risk of human error.
Controls should execute independently of existing business applications and processes.
Controls should provide enterprisewide validation/monitoring and create greater value than point-in-time solutions.
Controls should execute as needed—whether in batch or real time/at the same time as the controlled systems.
Controls should not require changes to the core processes or environment.
Controls should provide a full audit trail and control execution details as well as resolution-handling results.
Controls should be easily configurable and user friendly, not hard-coded or *ad hoc*.
Controls should provide a consistent framework for designing, deploying and operating across the enterprise.

Source: Santhosh Patil, Infogix Inc., 2013

Figure 2—Sales and Enrollments



Source: Santhosh Patil, Infogix Inc., 2013

can ensure that total member records match between the exchange and payer gateway. The enrollments via exchanges will have additional complexity with US federal subsidies that are applied based on subscribers' income levels. Insurers will need to track down subsidy amounts for each member through the exchange. Trending will need to be performed on disenrollment data and termed members tracked. Additional trending on profile information changes of members and frequency of updates, for example, to detect patterns of fraud and abuse will be important in this newly competitive environment. As such, organizations that monitor and measure sales and enrollment data will have the ability to rapidly adapt to consumer needs and competition.

Audit, Compliance and Finance Processes

US health care reforms have added more audit and compliance reporting requirements to an already heavily regulated industry. Internal audit is also mandating transaction-level reconciliation to prevent errors and financial losses that may result from changes in systems and processes. The ability to perform premium reconciliation with financial and membership systems aligns with this mandate. Payer organizations should develop formal structures to document financial risk and controls for monitoring and reporting purposes. In parallel, automation of manual processes and the reduction of dependencies on IT will help generate consistent and accurate audit information for regulators. To comply with NAIC-MAR, sufficient documentation to audit historical claim information indicating final disposition of all critical transactions is critical.

EDI Operations Management

Electronic data interchange (EDI) is the exchange of business information in standard electronic formats. The EDI standards are developed and maintained by the Accredited Standards Committee (ASC) X12.[7] The X12 standards are designed to work across industry and company boundaries. Health care organizations use specific X12 standards (e.g., 837, 835, 834,820, 270, 271) to electronically exchange health-related information among their trading partners. As shown in **figure 3**, health organizations typically use an EDI gateway system in which such electronic transactions are validated and consumed before they are directed to their respective processing system (i.e., claim adjudication, enrollment, eligibility, billing, payment).

Although additional validations are necessary, end-to-end reconciliation and balancing are the most critical functions for ensuring the integrity of EDI transactions.

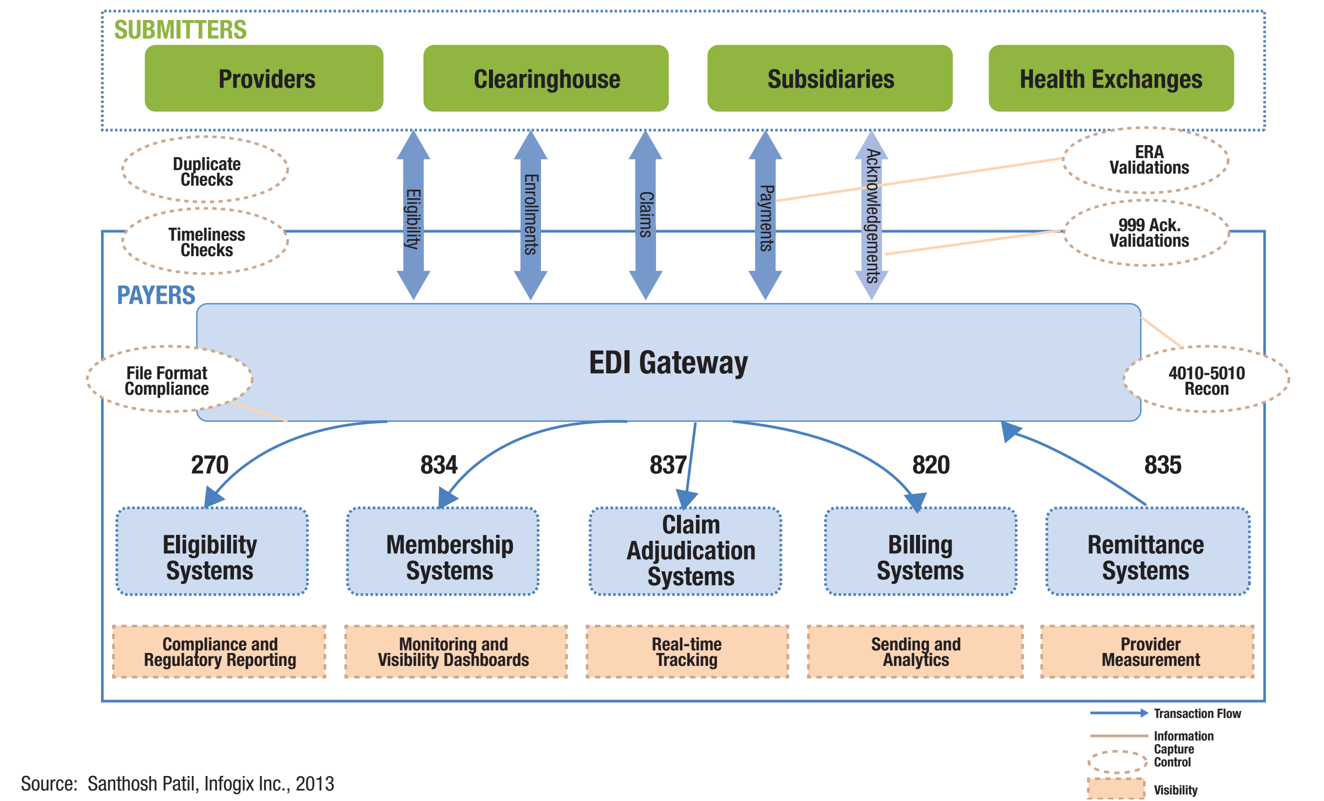
The ability to monitor EDI transactions is a second critical function. These same capabilities can be used to monitor the reasonability of received transactions, and will lead to the ability to trend on EDI data to identify operational issues and improve SLAs.

The final critical function recommended for EDI transaction integrity is the ability to utilize accurate EDI data for decision-making purposes. A transaction status report is beneficial in that it provides details of all errors that are defined between trading partners and payer gateway.

Claims Processing

Claims preadjudication is the forefront of the claims adjudication process that receives claim transactions submitted by the claims EDI gateway. The claims are validated, transformed and translated before being submitted for adjudication, as illustrated in **figure 4**. The requirements for validating and monitoring these processes include tracking all claims by claim number, for example, as they move from the EDI gateway through adjudication and payment processes. The focus here is tracking for timeliness and completeness. This same tracking validation can be used to track the life cycle during the preadjudication and adjudication steps. Tracking and validating these data allow health payer organizations to

Figure 3—EDI Gateway



Source: Santhosh Patil, Infogix Inc., 2013

monitor and report on the volume of claims in suspense by provider and procedure type. Operational improvement can be reached by aging and trending the claims processing life cycle to identify bottlenecks and improve SLAs.

CONCLUSION

With health care reform imposing new regulations and standards on the health care industry, organizations must look to increase operational efficiency and cut costs wherever possible, while still maintaining a consistent level of service.

As a result, health care organizations are looking at utilizing a standardized operational controls framework. These operational controls and monitoring solutions can be applied within organizations across the globe to automate validations, proactively detect errors and provide real-time monitoring into, for example, the EDI gateway, claims preprocessing, audit, compliance and finance processes.

It is recommended that organizations gain executive sponsorship and continually review operational controls and analytics to ensure continual improvement and maximal ROI from their solution.

ENDNOTES

[1] Congress, *Affordable Care Act Law*, USA, 2010, *www.healthcare.gov/law/full/index.html*

[2] ICD-10 Coding Compliance, *www.cms.gov/Medicare/Coding/ICD10/index.html*

[3] Congress, HITECH Act, USA, 2009, *http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__regulations_and_guidance/1496*

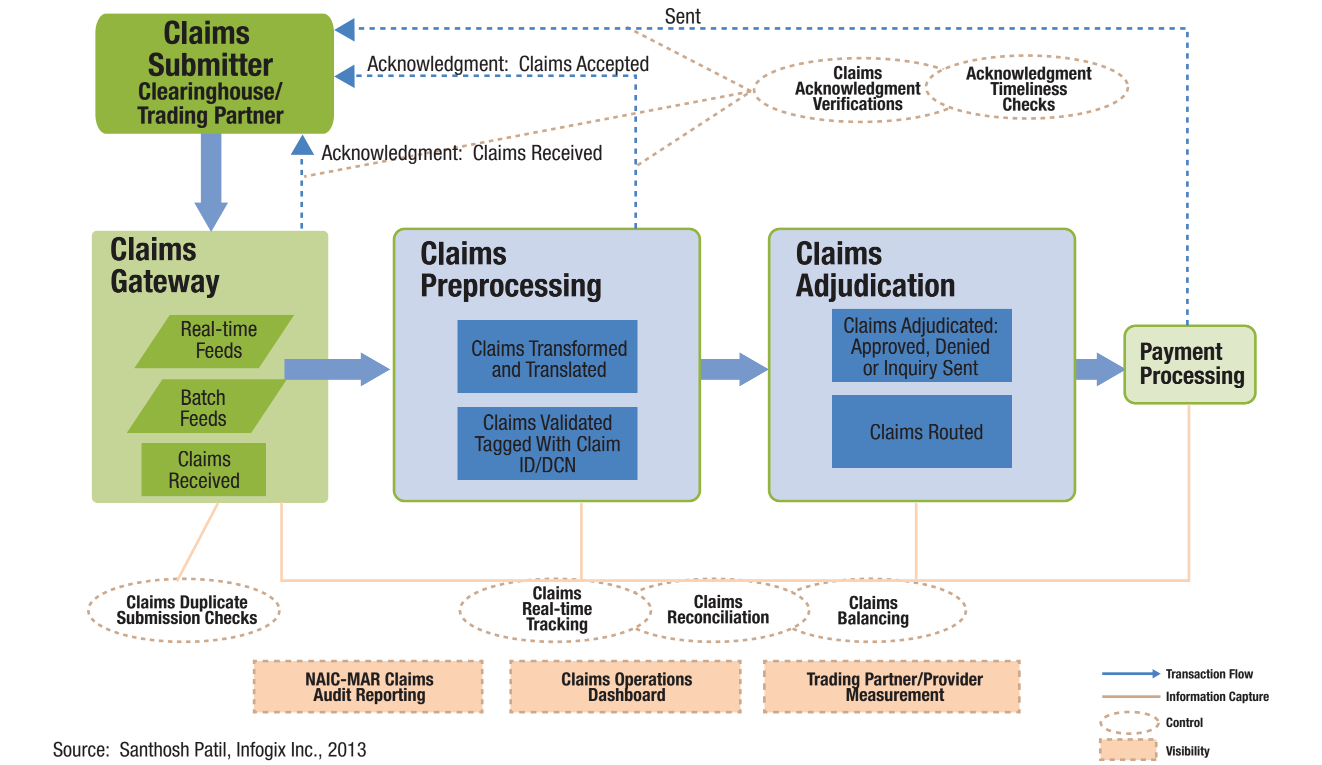
[4] National Association of Insurance Commissioners, *Implementing the Affordable Care Act's Insurance Reforms*, *www.naic.org/documents/committees_conliaison_1208_consumer_recs_aca.pdf*

[5] HealthCare.gov, "Creating a New Competitive Marketplace: Affordable Insurance Exchanges," 23 May 2011, *www.healthcare.gov/news/factsheets/2011/05/exchanges05232011a.html*

[6] HIMSS, Electronic Health Records (EHR), *www.himss.org/ASP/topics_ehr.asp*

[7] National Institute of Standards and Technology, *Electronic Data Interchange (EDI)*, USA, 29 April 1996, *www.itl.nist.gov/fipspubs/fip161-2.htm*

Figure 4—Claims Adjudication


Claims Submitter
Clearinghouse/ Trading Partner
Sent
Acknowledgment: Claims Accepted
Acknowledgment: Claims Received
Claims Acknowledgment Verifications
Acknowledgment Timeliness Checks
Claims Gateway
Real-time Feeds
Batch Feeds
Claims Received
Claims Preprocessing
Claims Transformed and Translated
Claims Validated Tagged With Claim ID/DCN
Claims Adjudication
Claims Adjudicated: Approved, Denied or Inquiry Sent
Claims Routed
Payment Processing
Claims Duplicate Submission Checks
Claims Real-time Tracking
Claims Reconciliation
Claims Balancing
NAIC-MAR Claims Audit Reporting
Claims Operations Dashboard
Trading Partner/Provider Measurement
Transaction Flow
Information Capture
Control
Visibility

Source: Santhosh Patil, Infogix Inc., 2013

Multiagent Model for System User Access Rights Audit

Christopher A. Moturi is the head of School of Computing and Informatics at the University of Nairobi (Kenya) and has more than 20 years of experience teaching and researching on databases and information systems audit.

Fredrick O. Bitta, CISA, is an IT auditor with the Central Bank of Kenya and has more than seven years of experience in T24, SAP and Oracle postimplementation review as well as database and operating systems audit. Previously, he was an IS auditor with National Oil Corp. of Kenya and Firestone EA Ltd.

Information systems (IS) security implementations put a lot of emphasis on external attacks while largely ignoring threats from within the organization. Statistics from the Computer Emergency Readiness Team (CERT) and industry security analysts show that about 80 percent of all malicious activities come from current or former employees.[1] Insider threats have become so critical that organizations have incorporated periodic user access rights audits in their information security policies to be carried out by systems auditors. The potential for fraud exists if system users have excess access rights to IS resources that are not appropriately segregated in line with the specific user's daily roles and responsibilities. Thus, more than ever, one of the prime concerns in any audit for management is the logical access to computer systems and data.[2]

IS auditors need to consistently audit system users' access to applications while cross-referencing the same with related user roles and responsibilities to ensure compliance. A mismatch should be reported and investigated in a timely manner. The need to continuously review what authorized system users access in the information system by an independent party is a key undertaking not only in risk management, but also in ensuring compliance with the organization's information security policy requirements. There is a lack of suitable tools to cross-reference what users actually access in the system within their roles and responsibilities in the organization.

The proposed multiagent model provides a platform for auditing consistency in user access rights with the ability to cross-reference what system users have accessed in the Oracle database application against their defined roles and responsibilities. The model incorporates highest-level access control policies and related procedures or business rules as defined by management, defined user roles and responsibilities, application database logs of active users, and their responsibilities. An audit report can be generated based on the analysis of conflicts between these parameters and fraud indicators isolated for further computer forensics investigation. An existing tool, Continuous Controls Monitoring Certification Manager, was used as a conceptual model for this study.

EXISTING ACCESS RIGHTS AUDITING TOOLS

Auditors can harness a new generation of tools to provide assurance on compliance with access privileges and permissions.[3] Several identity audit (IdA) application tools exist in the market today. The purpose of IdA applications is to help organizations identify differences between user permissions and user access activity. IdA applications generally operate by loading lists of user rights from repositories such as Windows Server Active Directory, importing and aggregating user access data from systems and application activity logs into a centralized data store, and using pattern-matching algorithms to correlate user identities across various logs to compare user access activity to user rights.

Examples of IdA tools include:

- **Permissions Analyzer for Active Directory**—This is a tool that enables systems administrators to get a complete hierarchical view of the effective permissions and access rights for a specific file folder (network file system) or shared drive and easily see what permissions a user has for an object.
- **Novell Identity Audit Applications**—This tool aggregates event data from a variety of Novell Identity and Access Management solutions and provides predefined reports that help demonstrate compliance, identify potential security issues and ensure the system is working as designed. Real-time alerts allow detection of critical events as soon as they occur, providing administrators with needed insight into user activity.[4]
- **Quest Access Manager**—This tool controls user and group access to resources throughout the Windows enterprise and network-attached

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:

storage devices in order to meet security and compliance requirements, to control operational costs and to optimize infrastructure performance. It intelligently suggests who should own which data resources, bringing accountability and visibility from a single console into resources that are actively used.[5]

- **Continuous Controls Monitoring Certification Manager**—Approva's Certification Manager automates the end-to-end process for reviewing user access rights across ERP systems and other business applications. Comprehensive, easy-to-understand summaries are routed to approving reviewers so they can accept or revoke access rights for their employees. Audit trails provide evidence for external audits.[6]

The key features of the assessed access rights audit tools are as follows: Permissions Analyzer provides a hierarchical view of all permission on the Microsoft New Technology File System (NTFS) or shared drive and is specific to networks and not applications. Novell Identity Audit Application is platform-specific, has real-time alerts, and offers searching and reporting on security, system and application events. Quest Access Manager is Windows-based and platform-specific. Continuous Controls Monitoring Certification Manager is not based on actual user activity, is designed for assigning rights to new system users, supports segregation of duties, and is both application- and network-based. It is of significance to note that none of the four existing IdA applications report on actual user access activity and policy exceptions as they do not track user activity at all and, thus, they lack that critical information. When considering any access control system, one considers three abstractions of control: access control policies, access control models and access control mechanisms.[7] Policies are high-level requirements that specify how access is managed and who, under what circumstances, may access what information. While access control policies may be application-specific and, thus, taken into consideration by the application vendor, policies are just as likely to pertain to user actions within the context of an organizational unit or across organizational boundaries.

MULTIAGENT CONCEPT AND APPROACH

Multiagent is an organization of coordinated autonomous agents that interact to achieve common goals. An agent is a component of software or hardware that is capable of acting exactingly to accomplish tasks on behalf of its users. Agents exhibit the following characteristics: autonomy, reactiveness, proactiveness, sociability, veracity, benevolence, rationality, adaptation, and distinct personality, behavior, name and role. Multiagents are open source and, thus, are able to operate in multiple platforms continuously monitoring what a user accesses in the system and comparing that with related roles of the same user as defined in the job description. The agents also make comparisons to establish whether there is appropriate segregation of duties within a specific user's access in the system. They are guided in decision making by the three abstractions of access control systems—access control policies, access control models and access control mechanisms.

Based on the evaluation of existing access rights audit tools, the Continuous Control Monitoring Certification Manager was adopted as the conceptual model for the implementation of the multiagent model. This tool was chosen because of its relative advantages over the other three audit applications discussed earlier as it automates the end-to-end process for reviewing user access rights across enterprise resource planning (ERP) systems and other business applications. Comprehensive, easy-to-understand summaries are routed to approving reviewers so they can accept or revoke access rights for their employees. Audit trails provide evidence for external audits. The framework does not carry out cross-referencing of actual user access with their related duties and responsibilities within the organization. It also does not capture the aspect of IS policy with regard to system access. However, it does automate the aspect of reviewing user rights before granting them access to the system

Access Rights Data Analysis

The purpose of this data analysis was to establish the existence of various scenarios of both compliance and noncompliance with regard to the parameters of system access. The data analysis was aimed at determining existence of violations specific to the sampled system users for purposes of modeling in a multiagent environment. These violations varied from conflict in segregation of duties to violations in policy requirements and conflicts with user roles defined in the job descriptions. Therefore, this data analysis was significant because the outcome informed the modeling process of the various agents arising from the various system access violation scenarios analyzed.

Systematically sampled data of 48 Oracle system users from a leading oil marketer in Kenya were collected, analyzed and used in testing the model. These data consisted of a log of active users and their responsibilities extracted from an Oracle application and contained the following information: username, security group, application, responsibility within the application, and user access start and end dates. Interviews of a sample of system users for purposes of getting information on their specific roles and responsibilities within the organization were carried out. **Figure 1** shows the data that were analyzed for purposes of this research.

The analysis involved the mapping of the job descriptions with the feedback from the questionnaires. The questionnaire response rate was 81 percent. Where the two were consistent, a yes (Y) was reported, and where there was inconsistency, a no (N) was reported. Where questionnaires were not received, the comparison was made between the job description and the access log; the assumption being that the job description was reflective of what the user does. As an example of a consistent response, an operations assistant at the depot listed one of his duties in the questionnaire as order entry in Oracle and his job description also stated that he receives orders from customer and enters them in the system.

From the analysis, two cases were discovered in which the feedback from the questionnaire was completely different from the documented users' job descriptions. On further inquiry, it was established that one of the users had been promoted to a new department, but the job description had not been updated accordingly, and the second user had left the organization, but access rights had not been deactivated.

The feedback from the 37 respondents showed that there was consistency between the job descriptions and their day-to-day duties and responsibilities. Based on this, the modeling was completed for the job descriptions because they represented the users' opinion on their daily chores within the organization. For the two samples where there was no consistency between the feedback from the questionnaires and the job descriptions, modeling was done separately and, in the risk matrix, they formed part of the three high-risk areas that were to be escalated.

The outcome of the analysis was then mapped with the active users access log. The feedback was also reported as a Y for consistency and an N for violations/inconsistency. The active users log was further mapped into the IS policy, access parameters were modeled and violations were reported accordingly.

From the analysis of the 48 samples, a total of 11 violations were reported. These violations were reported in a risk matrix as low, medium or high. From the results, it was noted that whenever a violation was reported in the mapping of the job description and the active users log, the access policy was also violated.

Figure 1—Data Analyzed

Data Required	Data Source	Analysis Done
Log of active users and their active responsibilities	Oracle database application	This log was extracted from an Oracle E-Business application and contained usernames, applications and responsibilities assigned to the users, as well as start and end dates. An understanding was gained on the responsibilities assigned to various users in the application. A sample of 48 system users was used for purposes of the study—achieved through equal probability sampling technique.
System users roles and responsibilities	Human resources (HR) department and system users	Based on the sampled system users, related user job descriptions were taken from the HR department. Targeted questionnaires were sent to the sampled system users for purposes of getting feedback with regard to their roles and responsibilities in the organization. The job descriptions and feedback from questionnaires were analyzed to establish consistency.
ICT policy	ICT manager	The information security policy of the organization was analyzed to establish areas covering access to applications. Conflict in segregation of duties within the sampled system users was determined through qualitative analysis.

Development of the Multiagent Model

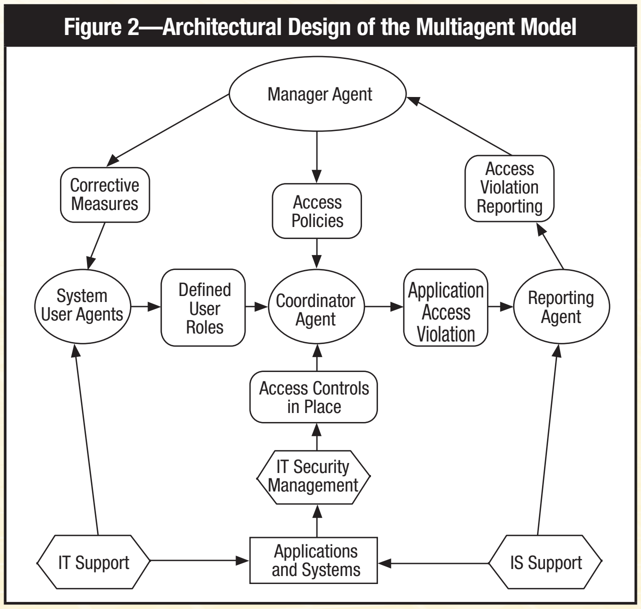
The development of the model was guided by the Tropos agent-oriented software-engineering methodology. Actors, goals, tasks, resources and social dependency between actors were established. The following agents were incorporated:

- **Actor 1: System user agent**—This agent defines user roles as mapped in the active users log from the application database and submits to the coordinator the actual responsibilities of the system user. This then enables the coordinator agent to make comparisons with the log of active users extracted from the application database to establish whether a conflict exists.
- **Actor 2: Management agent**—This agent defines and maps application access policies to the active users log from the database through the coordinator agent in order to establish the existence of conflicts. It also enables compliance by performing updates on the users' job descriptions based on access violation reports from the reporting agent. The management agent also defines new policies on access to be monitored by the coordinator agent.
- **Actor 3: Coordinator agent**—The agent establishes consistency and reports conflicts by facilitating the mapping of defined user roles from the system users' agent and the active users log from the database application for queried users. This agent reports conflicts where there is a mismatch in the mapping and consistency.
- **Actor 4: Reporting agent**—This agent reports to the management agent any violations captured by the coordinator agent.

Architectural Design

The four actors were assigned goals or subtasks of the goals as illustrated in **figure 2**.

Figure 2—Architectural Design of the Multiagent Model



Model Testing

To consistently audit what users access within a database application, three key aspects must be considered: system user roles as captured in the job description, the organization's IS policy on access to applications and the access log as extracted from the database. For purposes of establishing segregation of duties, the log of active users and their responsibilities extracted from the Oracle application were mapped for each sampled user to the user roles within the human resources management system (HRMS) module and IS policy requirements on access. Flags to access functionality were mapped within a PeopleSoft HR module and across PeopleSoft modules by user, to ensure segregation of duties. The data collected and analyzed were used in testing the model based on the logged information. Agent testing was done incrementally during software development. The testing was done at two levels: agent-level testing and society-level testing. Much focus was on agent level, which involved testing of individual agent functionality. This was achieved through an event that was triggered by another agent in order to test the functionality required.

Much of this testing required another agent to trigger an event inside the agent to be tested, such as a message from another agent. In a multiagent development environment, it is impossible or very expensive to predict agent behavior, thus the need to test each agent independently before incorporation in a society of four or more agents. Segregation of duties was also noted as a violation of policy, which was monitored by the management agent. Therefore, when developing a single agent for inclusion in the community of four agents, it was necessary to make sure that it responded correctly to the given inputs from other agents.

Testing the community of four agents involved two issues:

- How to ensure that the agents in the community work together as designed

- How to ensure that the resultant work was as expected

During the society test, the validation of the overall results of the different agents was done and the successful integration of the different agents verified. This involved checking that each agent received the correct messages from the correct agent, provided the correct responses and interacted with the environment correctly. It also involved checking that the goal of the community where the agents were interacting was being achieved.

Model Implementation

The tools used for implementation were the SQL database for storing the log of active users data and the JADE multiagent environment for running the various agents, including:

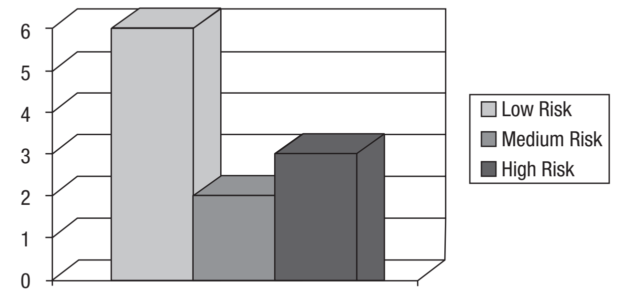
- **System user agent implementation**—This agent was implemented as an initiator of several processes including the actual access as defined in the SQL database as well as the defined user roles and responsibilities as captured from the analyis of users' job descriptions and feedback from questionnaires. The system user agent did a comparision of the actual user access against the defined roles and responsibilities when prompted by the reporting agent. The output from this agent was submitted to the management agent for purposes of establishing compliance or violation of the access policies as modeled.
- **Management agent implementation**—This agent was implemented to ensure that the applications accessed by the users are compliant with the organization's IS policy on application access, and to facilitate updates to the users' job descriptions when required to ensure reported violations are addressed. Therefore, through this agent, whenever violations were reported, the user was prompted to make updates, if they wished, to the user's job description to ensure compliance. If the users accepted this, they were allowed to incoporate some of the applications reported as violations to the user's job description so as to comply.
- **Reporting agent implementation**—With a GUI interface, the main duty of this agent was to capture input and generate an output of either violation or nonviolation and to update the user's job description in cases of reported violations to ensure compliance.
- **Coordinator agent implementation**—This agent was the coordinator of all operations within the system. It defined the sequence in which the other three agents were to be called into action. The agent ensured proper interagent communication and competition as well as coordination for purposes of realizing effective audit and reporting of user access violations.

Agents' Output on Access Violation Reporting

The output was generated in a specific format, with the username coming first, followed by the risk level, number of violations, policies violated (if any) and the particular application violated.

From the total number of 48 sampled system users, 11 reported access violations while 37 were compliant with their job descriptions and access policies of the organization. Analysis of the 11 reported violations established that, based on the risk matrix, six cases were low risk, two cases were medium risk and three cases were high risk (**figure 3**).

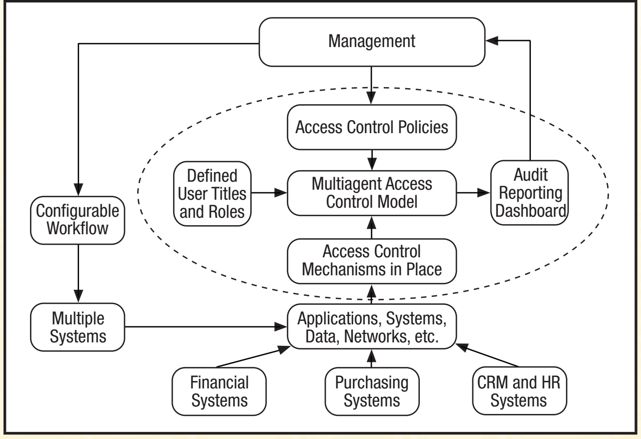
Figure 3—Case Example Access Violation Risk Matrix



PROPOSED MULTIAGENT MODEL FOR USER ACCESS RIGHTS AUDIT

Figure 4 represents the proposed model for user access rights audit based on the multiagent architectural design. The proposed model draws input from three components: the defined user roles and responsibilities, access control policies, and the actual system user access. The defined user roles were arrived at after detailed analysis of the user job descriptions and feedback from questionnaires on what user duties were within the organization. The access controls in place were representative of the active users log extracted from an Oracle application database capturing actual system user access. The access policy with regard to the application was also modeled.

Figure 4—Proposed Multiagent Model for User Access Rights Audit


Management
Access Control Policies
Defined User Titles and Roles
Multiagent Access Control Model
Audit Reporting Dashboard
Configurable Workflow
Access Control Mechanisms in Place
Multiple Systems
Applications, Systems, Data, Networks, etc.
Financial Systems
Purchasing Systems
CRM and HR Systems

When a specific user ID is queried, the application access is presented to the model. A comparison is then made between the actual access and the user roles and responsibilities as defined in the job description. The actual application access is then compared with the access policies to determine whether there exist conflicts in segregation of duties and these are reported accordingly. The reporting dashboard transmits the violations report to management who then determine if amendments need to be made to the users' job description so that they comply with the organizations requirements. When these amendments are made, a user either becomes compliant or the rights are completely revoked.

It was on this model structure that the 11 violations and 37 nonviolations were reported. The results, therefore, fit in this model. The workflow was as shown in **figure 5**, in which the multiagent control model was central to all activities. The processes included analysis of violations based on the parameters described and reporting to management for corrective action whenever violations were reported. The impact of internationally-developed data analysis and management software (IDAMS) on this model could not be quantified since there was no statistical analysis involved or correlation with the multiagent tool.

CONCLUSION

The proposed multiagent model for consistent system-user access rights audit is useful in addressing the threat from within the organization relating to application access violations. It combines the three major concerns on access to information systems—access policy, user roles as captured in the job description, and the actual user access to the system—to develop a tool that is of significance to the key stakeholders. This model can be used by IS auditors to provide independent assurance with regard to application access policies and system-user job descriptions within an organization. IS managers could proactively use the model to consistently review authorized system-user access within the application, thus ensuring compliance with the set standards. The proposed model for user access rights audit fits well in the context of most organizations because it captures all the key elements required to consistently monitor application access violations.

Further work could be done to make the model real time—by designing an interface between the tool and the organization's database application for continuous monitoring. The model could also be enhanced with an interface to other auditing software for purposes of real-time reporting and escalation of access violations to management for appropriate and timely action.

ACKNOWLEDGMENTS

The authors sincerely thank Lawrence Muchemi, Peter Wagacha, Dan Orwa and Joseph Ogutu, all from the School of Computing and Informatics, University of Nairobi, Kenya, for their contributions to this paper.

ENDNOTES

[1] Singleton, Tommie; "Mitigating IT Risks for Logical Access," *ISACA Journal*, vol. 5, 2010

[2] Schperberg, R.; "Five Questions With Robert Schperberg," *ISACA Journal*, vol. 5, 2010, *www.isaca.org/archives*

[3] Glithero, B.; "Identity Audit Applications Streamline User Access Review," *Internal Auditor*, 2010, *www.theiia.org/intAuditor/itaudit/2010-articles/identity-audit-applications-streamline-user-access-reviews/*

[4] Novell, *www.novell.com/products/audit/*

[5] Quest, *www.quest.com/access-manager*

[6] Approva Corp, *www.approva.net/products/certificationmanager*

[7] Kuhn, D. R.; F. D. Ferraiolo; R. Chandramouli; *Role-based Access Controls, 2nd Edition*, Artech House, England, 2007

Pushing Back the Rain—How to Create Trustworthy Services in the Cloud

Dan Bogdanov, Ph.D., is an information security researcher at Cybernetica (Estonia). Before starting his research career, Bogdanov worked in IT system development and consultancy. His interest in secure data processing comes from his experience in developing the data management platform of EGeen Inc., an international contract research organization (CRO) working in the area of drug development. Bogdanov is currently leading a team that is developing the Sharemind secure database system.

Aivo Kalu, Ph.D., CISA, is a security engineer at Cybernetica (Estonia) and has previously worked as the security officer for Elion Enterprises (Estonia's largest telecom, now part of TeliaSonera group) and for the Ministry of Foreign Affairs of Estonia. Kalu has experience in both creating the enterprise security architecture and auditing the baseline and compliance security.

WHO CONTROLS THE DATA IN THE CLOUD?

Cloud computing allows us to use computing infrastructure over the Internet. For example, one can rent storage and processors just as easily as one can rent a movie. Just as the movie distributor wants to prevent illegal copying of the movie, the data owner wants to prevent the cloud service provider (CSP) from copying or abusing its data. "Traditionally, the data owner has had direct or indirect control of the physical environment affecting his/her data. In the cloud, this is no longer the case."[1]

A typical CSP does not accept responsibility for preventing third-party access to sensitive data such as intellectual property, trade secrets or personally identifiable information (PII), hosted in the cloud. The cloud user must manage this risk and deploy the necessary controls for ensuring confidentiality.

KEEPING CONTROL OVER DATA

A cloud is a remote-access platform; thus, technical controls that remotely enforce a particular security policy are especially efficient. Examples of such controls include encryption and digital signatures. Encryption enforces confidentiality; digital signatures can detect if information has been modified since it was stored. Both mechanisms are static and require the user to remove the controls/protection mechanism to perform computations on the data. This means that stored encrypted and signed data are not protected from third-party access during processing.

The need for better solutions guides the development of new technologies. Secure multiparty computation (SMC) and homomorphic encryption (HE) are two new technologies that preserve cryptographic security during processing. If a cloud application uses these technologies, it can process data in the cloud without revealing the data to the CSP.

These new technologies enable applications that have previously been impossible to build due to a lack of trust in the CSP holding the data. One application of these technologies is the processing of PII with significantly better confidentiality than before. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) is scheduled to publish a standard for a privacy architecture framework (ISO/IEC 29101) that describes some ways for using SMC for PII processing.[2]

A well-studied application of SMC in the field of agriculture involves the Danish sugar company Danisco, which in 2008 began the process of requiring new contract agreements with sugar beet farmers. These manufacturing contracts contain production volumes and prices. Danisco requires this information in the contracts so that the company can plan sugar production. An auction was held to find the market-clearing price—the price at which Danisco could sign enough contracts to fulfill its need for sugar beets. However, the farmers were reluctant to report their production volumes to buyers because they feared that Danisco would use this information later to force unfavorable contract conditions. A survey held among the farmers resulted in approximately 75 percent of farmers stating that the confidentiality of the bid was either important or very important to them.[3]

Danisco began looking for better solutions because of this lack of trust. The problem was resolved with the use of an SMC auction system developed by the Alexandra Institute in Denmark. This secure auction system enforced the confidentiality of each bid in the auction and published only the market-clearing price. The sugar beet auction bids were collected over the Internet, but their software solution required representatives from Danisco and the sugar beet farmers' association to physically come together to finalize the computation.

This case showed that SMC can be used to create trustworthy cloud applications.

AN INDUSTRIAL SECTOR IN NEED OF A HEALTH REPORT

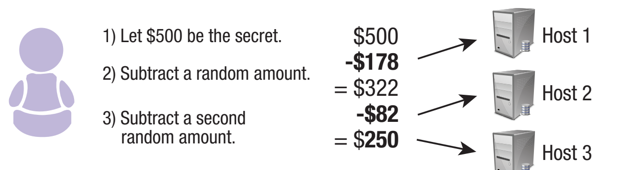
The following case study shows SMC applied using cloud computing.

The Estonian Association for Information and Communications Technology (ITL) is a trade organization that connects Estonian IT companies such as Skype, Playtech, and the local offices of IBM, Microsoft and others. These companies formed ITL to protect their interests and to promote and develop IT education in Estonia. Estonia, a European Union country, is well known for its transparent e-government solutions; this same philosophy inspired ITL to collect financial performance indicators from its members to publish reports on how well the industry sector is performing.

According to the plan, the ITL board would collect metrics from its members and compile the report. As the organization consists of competing companies, some ITL members were reluctant to give their *business health data* to their competitors, but they were interested in the promised results.

ITL proposed developing the data collection and reporting system using SMC. The proposal suggested that ITL use a special kind of SMC that is based on secret sharing. Secret sharing is used to preserve the confidentiality of the financial metrics. It is a form of anonymous encryption that splits confidential values into several pieces that individually leak no information about the original secret value (see **figure 1**).

Figure 1—Secure Storage Using Arithmetic Secret Sharing (Simplified)


1) Let $500 be the secret.
2) Subtract a random amount.
3) Subtract a second random amount.
$500
-$178
= $322
-$82
= $250
Host 1
Host 2
Host 3

The bold values are the ***shares*** of the secret value.
Each share will be stored by a dfferent host. The share looks random to the host.
Shares need to be collected in order to reconstruct the secret.

(Note that this explanation just gives the intuition and omits the mathematical details.)

Material was prepared to inform the ITL members of the planned security measures and methods to ensure the confidentiality of their inputs. While it was hard to convince companies to disclose data about their financial state, everyone was interested in the health of the industry as a whole. Thus, the guarantees of SMC convinced ITL members to participate in the reporting.

DEPLOYING SMC ON THE CLOUD

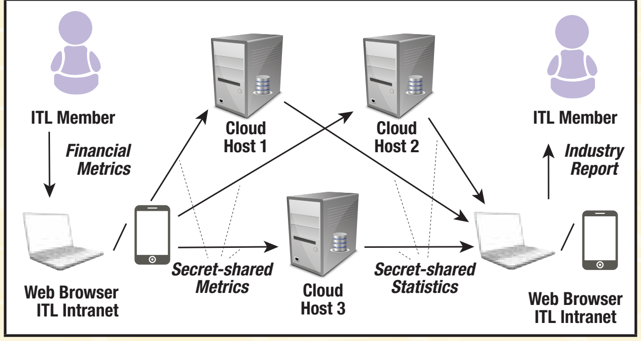
ITL chose Sharemind[4] as the SMC platform because it supported secret sharing and had the best performance among the available solutions.

The next step was the deployment of the secret-shared database. The efficient use of secret sharing requires three independent hosts for the database. Each host stores one share of each secret value. This guarantees that no single host is capable of recovering the confidential inputs from its database (see **figure 1**).

Three independent ITL members hosted the nodes of the Sharemind database. Two members used the Sharemind node on an Infrastructure as a Service (IaaS) CSP and the third member used a private server.

Sharemind developer tools provided libraries for creating the data collection and reporting applications. The resulting applications were deployed to the ITL intranet. The complete secure financial reporting system is depicted in **figure 2**.

Figure 2—Cloud Deployment of the Confidential Financial Reporting Application



The system went live in January 2011 and supplies biannual reports. A survey conducted among the ITL members showed that the new reporting system makes them feel safer about providing their financial metrics.[5]

IMPROVING CLOUD APPLICATION SECURITY BY USING SMC

Current SMC technology is most effective if the following three conditions are present:

1. The application in the cloud processes private/confidential data from several sources.
2. The data sources do not fully trust the cloud service provider with confidentiality of data stored in the cloud.
3. The data sources do not fully trust each other.

SMC can also be used for securely outsourcing information processing of a single stakeholder to the cloud. However, a private or hybrid cloud may be a more efficient solution as the encryption benefits of SMC have a higher pay-off in this situation.

When the three conditions are present, the cloud application developer should evaluate the available SMC platforms to determine if SMC can be used to improve the security of the application. An SMC platform is a good control for keeping data confidential and analyzable at the same time.

SMC also protects the user's information assets against access or seizure by the cloud service provider (CSP). Examples of such scenarios were described in a recent report by ISACA®.[6] For example, as the CSP controls the computing hardware running the cloud application, it also has access to the data residing within, including data such as customer and transaction databases. SMC can be used to protect and process databases with a greatly reduced risk of unauthorized access.

Following are the basic steps of building an SMC-enabled cloud application:

1. Identify the data donors and their confidentiality requirements to determine which data values need protection from being revealed to the CSP.
2. Develop a data model and a data flow description so that the confidential values are clearly marked.
3. Implement the data model and business logic using the tools provided by the SMC platform.
4. Deploy the SMC platform and the cloud application with the CSP of choice.

Some SMC platforms use freely available developer resources for easier evaluation. For example, Sharemind,[7] SEPIA[8] and VIFF[9] provide developer tools and example source code online.

SMC applications can be deployed using the enterprise's currently existing IaaS solutions. In time, a range of SMC-based Platform as a Service (PaaS) offerings is expected to make the use of the technology even simpler.

CONCLUSION

SMC is an emerging disruptive technology for processing confidential information. As with every technology, SMC has many approaches. Different platforms provide different security guarantees. New platforms and applications continue to be introduced around the world. Recently, the US Defense Advanced Research Projects Agency (DARPA) started the Programming Computation on Encrypted Data (PROCEED)[10] program to develop new, efficient SMC methods. In Europe, there is a project with the goal of finding out how SMC can be applied in new areas.[11]

The main challenge for this new technology is its acceptance into existing risk management frameworks so that the CSPs and users can understand the risk mitigation it provides. One of the first areas where SMC is expected to have an impact is privacy; the ISO/IEC 29101 standard project on a privacy architecture framework describes SMC as a control for protecting PII. It will be up to the real innovators—the users—to take advantage of the new technology and realize its full potential.

ENDNOTES

[1] ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, white paper, USA, October 2009, *www.isaca.org*

[2] ISO/IEC 29101, *Information technology—Security techniques—Privacy architecture framework*, November 2012

[3] Bogetoft, Peter, *et al.*; "Secure Multiparty Computation Goes Live," Proceedings of the 13th International Conference of Financial Cryptography and Data Security, Springer, 2009, p. 325-343

[4] The Sharemind secure computation platform, *http://sharemind.cyber.ee/*

[5] Bogdanov, Dan, *et al.*; "Deploying Secure Multi-Party Computation for Financial Data Analysis (Short Paper)," Proceedings of the 16th International Conference on Financial Cryptography and Data Security, Springer, 2012, p. 57-64

[6] ISACA, *Security Considerations for Cloud Computing*, Cloud Computing Vision Series, ISACA, 2012, *www.isaca.org*

[7] The Sharemind Software Development Kit, *https://sharemind.cyber.ee/download-sdk*

[8] SEPIA (Security through Private Information Aggregation), *http://sepia.ee.ethz.ch*

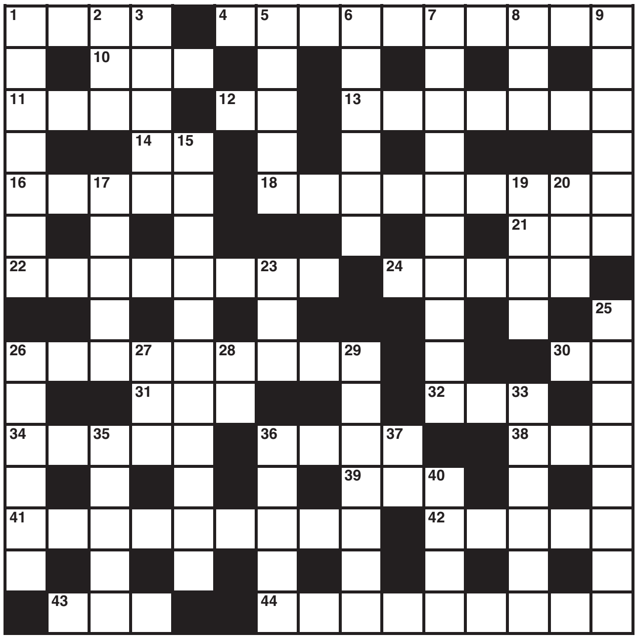
[9] Virtual Ideal Functionality Framework (VIFF), *http://viff.dk*

[10] DARPA's PROCEED program is a research effort that seeks to develop methods that allow computing with encrypted data without first decrypting it, making it more difficult for malware programmers to write viruses.

[11] Usable and Efficient Secure Multiparty Computation, *http://usable-security.eu/*

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. Team of security professionals trained to respond if a breach occurs or is suspected, abbr.
4. Way to decrease the value of sensitive information to a penetrator
10. Notable period
11. Computer linked to a network
12. Tech department
13. Prevented access
14. Word expressing surprise
16. Prepared
18. Low esteem that can result within an enterprise from a hacker penetration
21. Alert of a serious emergency
22. Relaxed, standards for example
24. Valuable item
26. Type of security software that has to be regularly updated
30. Concerning
31. Important person
32. Oracle competitor
34. Relative amounts
36. According to Aristotle, a genuinely virtuous action proceeds from "___ and unchangeable character"
38. Corporate title for the executive responsible for managing risk
39. Pledge
41. A client using a SaaS application may be responsible only for this and its resultant data
42. Supplemented
43. Certified Ethical Hacker, for short
44. Revealed

DOWN

1. Check or regulate
2. Color associated with danger
3. "Fools rush in where angels fear to ____"
5. Eminent
6. Sturdy
7. They handle the data in a computer
8. Sign a contract, e.g.
9. Reminds
15. Software applications that allow one or more virtual machines to operate directly on underlying hardware
17. Cancel a project
19. End ___
20. Sum up
23. Go off track
25. Had the financial resources to purchase
26. Quick-witted
27. "___ got it!"
28. Address type
29. Checks opinions
33. _____ Cloud Computing Guidelines Information Supplement
35. Corporate position
36. Criminal deception
37. Unchanging procedure, for short
40. Fire____, security barrier

(Answers on page 54)

CPE Quiz

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

Take the quiz online:

Quiz #148

Based on Volume 1, 2013—Governance and Management of Enterprise IT (GEIT)

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

TRUE OR FALSE

MARKS ARTICLE

1. COBIT 5 incorporates new GEIT principles.

2. The COBIT governance model is based on the Enterprise Development Maturity (EDM) model, which is also used in ISO 38500.

3. COBIT 5's governance processes include APO02 *Manage strategy* and APO12 *Manage risk*.

CARILLO ARTICLE

4. IT policies help organizations to properly articulate the organization's desired behavior, mitigate risk and contribute to achieving the organization's goals.

5. The enablers that support the implementation of GEIT include culture, ethics and behavior.

6. Writing a policy requires identifying the individuals responsible for providing an independent review.

7. Procedures are mandatory actions, explicit rules and configuration settings designed to conform to a policy.

ZOUGHBI ARTICLE

8. Many ERP investments fail to deliver due to deficient ERP investment appraisals caused by inflated expected benefits and underestimated cost and risk.

9. For business case development, step two, alignment; step three, financial benefits; and step four, nonfinancial benefits, are important.

10. Customizing an ERP system is a low-cost option due to the simplicity of the system.

11. The 10 risk factors in ERP acquisition include establishing realistic expectations.

YU ARTICLE

12. According to SkyDox, 55 percent of users use file-sharing applications and, of these, 60 percent do not report such usage.

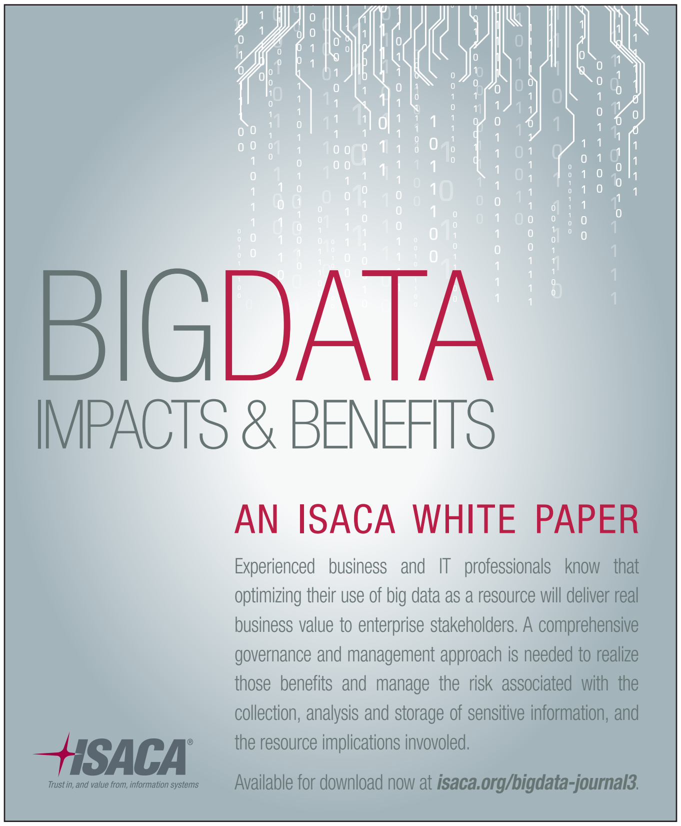
13. To control mobile devices, measures such as real-time remote locking, data wiping and device tracking may be considered.

BHATIA ARTICLE

14. Often IT governance fails due to institutionalization (e.g., changes in culture and behavior of people).

15. Hoshin Kanri is a strategic planning methodology based on Deming's PDCA Cycle.

16. IT governance implementation and institutionalization is independent of buy-in from business unit executives.



ISACA Journal
CPE Quiz
Based on Volume 1, 2013—Governance and Management of Enterprise IT (GEIT)

Quiz #148 Answer Form

(Please print or type)

Name ____

____

Address____

____

____

CISA, CISM, CGEIT or CRISC #____________________________

Quiz #148

True or False

MARKS ARTICLE

1. __________
2. __________
3. __________

CARILLO ARTICLE

4. __________
5. __________
6. __________
7. __________

ZOUGHBI ARTICLE

8. __________
9. __________
10. _________
11. _________

YU ARTICLE

12. _________
13. _________

BHATIA 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 email, fax or mail your answers for grading. Return your answers and contact information by email 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 52 for the puzzle.

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

Standards
Guidelines
Tools and Techniques

ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

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

- **Standards** define mandatory requirements for IT audit and assurance.
  They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide specific information on various methodologies, tools and templates, and provide direction on how to implement and apply the information provided in the guidelines. They take a variety of forms, such as discussion documents, templates, white papers, audit programs or books (e.g., ISACA's Technical Research Series of books: *Security, Audit and Control Features SAP® ERP, 3rd Edition*; Security, *Audit and Control Features Oracle® E-Business Suite, 3rd Edition*; *Security, Audit and Control Features Oracle® Database, 3rd Edition*; and *Security, Audit and Control Features Oracle® PeopleSoft®, 3rd Edition*).

COBIT® 5 is a business framework for the governance and management of enterprise IT. COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or public sector.

ISACA continually updates and expands the practical guidance and product family based on the COBIT framework. COBIT helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business. COBIT is available for download at *www.isaca.org/cobit.*

COBIT 5 for Assurance is currently under development and scheduled to be issued in the second quarter of 2013. It builds on COBIT 5 in that it focuses on IS audit and assurance and provides more detailed and practical guidance for IS audit and assurance professionals.

Links to current guidance are posted on the standards page, *www.isaca.org/standards*. Please note that the standards and guidelines are being updated for integration into ITAF™, *www.isaca.org/itaf*. The updated standards are scheduled to be issued in June 2013. An exposure draft of the revised guidelines is scheduled to be posted for comment on the ISACA web site in the fourth quarter of 2013.

Titles of audit and assurance standards and guidelines are as follows.

IT Audit and Assurance Standards

(to be withdrawn when the new standards are effective)

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 August2008
G15 Audit Planning Revised Effective 1 Ma1 2010
G17 Effect of Non-audit Role on the IS Auditor's Independence Effective 1 May 2010
G20 Reporting Effective 16 September 2010
G30 Competence Effective 1 June 2005
G34 Responsibility, Authority and Accountability Effective 1 March 2006
G35 Follow-up Activities Effective 1 March 2006
G42 Continuous Assurance Effective 1 May 2010

IS Audit and Assurance Standards

(scheduled to be issued in June and effective 1 September)

General

1001 Audit Charter
1002 Organisational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria

Performance

1201 Planning
1202 Risk Assessment in Audit Planning
1203 Performance and Supervision
1204 Materiality
1205 Using the Work of Other Experts
1206 Evidence
1207 Irregularity and Illegal Acts

Reporting

1401 Reporting
1402 Follow-up Activities

Code of Professional Ethics Effective 1 January 2011

Advertisers/Web Sites

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

ISACA®

Trust in, and value from, information systems

BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

Over 350 titles are available for sale through the ISACA® Bookstore.
This insert highlights the new ISACA research and peer-reviewed books.
See *www.isaca.org/bookstore* for the complete ISACA Bookstore listings.

NEW BOOKS...

www.isaca.org/newbooks

Audit, Control and Security—Specific Environments

Introduction to Healthcare Information Technology, 1st Edition
320 pages, 2013—**16-IT**
Member $73.00 | Nonmember $83.00

Wireless Network Security A Beginner's Guide
368 pages, 2012—**30-MWNS**
Member $40.00 | Nonmember $50.00

Audit, Control and Security—Essentials

IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud ⬇
WITCOCI Italian, E-Book—PDF Format (purchase online only)
Member FREE | Nonmember $50.00

Once MoreUnto the Breach: Managing Information Security in an Uncertain World
246 pages, 2012—**14-ITOM**
Member $40.00 | Nonmember $50.00

Internet and Related Security Topics IT Governance and

Information Security Governance Simplified: From the Boardroom to the Keyboard
431 pages, 2011—**54-CRC**
Member $80.00 | Nonmember $90.00

Business Management

Illustrating PRINCE2®: Project Management in Real Terms
226 pages, 2012—**15-ITIP**
Member $30.00 | Nonmember $40.00

FEATURED...

www.isaca.org/featuredbooks

Auditor's Guide for IT Auditing + Software Demo, 2nd Edition
53WAG2
Member $95.00 | Nonmember $105.00

Cyber Security Policy Guidebook
96WCSP
Member $90.00 | Nonmember $100.00

The Definitive Guide to the C+A Transformation
13ITCAT
Member $70.00 | Nonmember $80.00

Information Technology Control and Audit, 4th Edition
4CRC4
Member $90.00 | Nonmember $100.00

IT Governance:Policies & Procedures, 2013 Edition
5AS13
Member $275.00 | Nonmember $285.00

Official Certified Ethical Hacker Review Guide:For Version 7.1, 1st Ed
15-IT
Member $40.00 | Nonmember $50.00

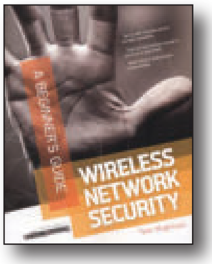
SUPPLEMENT

* Published by ISACA and ITGI

⬇ ISACA member complimentary download *www.isaca.org/downloads*

All prices are listed in US Dollars and are subject to change

NEW/FEATURED BOOKS www.isaca.org/newbooks



Wireless Network Security A Beginner's Guide

NEW

By Tyler Wrightson

Protect wireless networks against all real-world hacks by learning how hackers operate. *Wireless Network Security: A Beginner's Guide* discusses the many attack vectors that target wireless networks and clients--and explains how to identify and prevent them. Actual cases of attacks against WEP, WPA, and wireless clients and their defenses are included.

This practical resource reveals how intruders exploit vulnerabilities and gain access to wireless networks. You'll learn how to securely deploy WPA2 wireless networks, including WPA2-Enterprise using digital certificates for authentication. The book provides techniques for dealing with wireless guest access and rogue access points. Next-generation wireless networking technologies, such as lightweight access points and cloud-based wireless solutions, are also discussed. Templates, checklists, and examples give you the hands-on help you need to get started right away.

Wireless Network Security: A Beginner's Guide features:

- Lingo—Common security terms defined so that you're in the know on the job
- IMHO—Frank and relevant opinions based on the author's years of industry experience
- In Actual Practice—Exceptions to the rules of security explained in real-world contexts
- Your Plan—Customizable checklists you can use on the job now
- Into Action—Tips on how, why, and when to apply new skills and techniques at work

368 pages, 2012. **30-MWNS** Member **$40.00** Nonmember **$50.00**

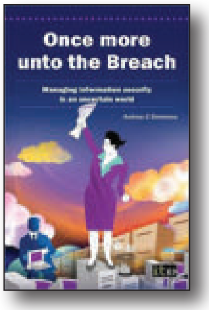
Introduction to Healthcare Information Technology, 1st Edition

NEW

By Mark Ciampa, Mark Revels

The healthcare industry is growing at a rapid pace and undergoing some of its most significant changes as the use of electronic health records increase. Designed for technologists or medical practitioners seeking to gain entry into the field of healthcare information systems, *Introduction To Healhcare Information Technology* teaches the fundamentals of healthcare IT (HIT) by using the CompTIA Healthcare IT Technician (HIT-001) exam objectives as the framework. It takes an in-depth and comprehensive view of HIT by examining healthcare regulatory requirements, the functions of a healthcare organization and its medical business operations in addition to IT hardware, software, networking, and security. *Introduction To Healhcare Information Technology* is a valuable resource for those who want to learn about HIT and who desire to enter this growing field by providing the foundation that will help prepare for the CompTIA HIT certificate exam.

320 pages, 2013. **16-IT** Member **$73.00** Nonmember **$83.00**


Once more unto the Breach
Managing information security in an uncertain world

Once More Unto the Breach: Managing Information Security in an Uncertain World

NEW

By Andrea C Simmons

Your responsibilities as an information security manager are critical. Advising on protecting the organisation's assets, security and data systems, not to mention its reputation, are in your hands. A major security breach could spell disaster.

A typical year in the life of an information security manager

In *Once More Unto the Breach*, Andrea C Simmons speaks directly to information security managers and provides an insider's view of the role, offering priceless gems from her extensive experience and knowledge. Based on a typical year in the life of an information security manager, the book examines how the general principles can be applied to all situations and discusses the lessons learnt from a real project.

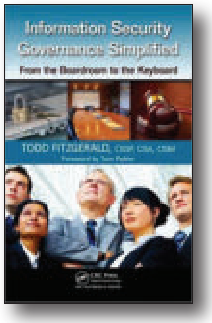
Improve your organisation's security

One of the greatest challenges faced by an information security manager is convincing colleagues of the importance of following the necessary processes and procedures. As you walk through the year with Andrea, you will make significant inroads into improving your organisation's security as you:

- think creatively in order to provide solutions to ongoing issues
- create a workable information security policy
- make friends with the right people in order to facilitate critical changes
- pinpoint weaknesses and help your colleagues to see them through your eyes
- improve physical security by helping others to take personal responsibility
- learn strategies for the effective communication of key security messages in order to maximise use of the measures in place
- appreciate how all this helps you to address the human factors and reduce your cyber risks—which are ultimately security risks
- discover why it's essential to have a camera on you at all times!

As well as a practical learning tool, *Once More Unto the Breach* is an invaluable ongoing reference guide, containing lots of practical advice to ensure that the routine tasks aren't overlooked. With many clear and comprehensive lists, this is a book that will never be out of the reach of every effective information security manager.

246 pages, 2012. **14-ITOM** Member **$40.00** Nonmember **$50.00**



Information Security Governance Simplified: From the Boardroom to the Keyboard

NEW

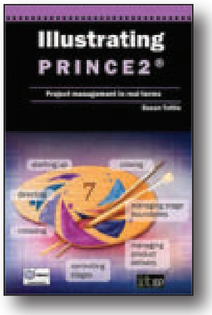
By Todd Fitzgerald

Security practitioners must be able to build cost-effective security programs while also complying with government regulations. *Information Security Governance Simplified: From the Boardroom to the Keyboard* lays out these regulations in simple terms and explains how to use control frameworks to build an air-tight information security (IS) program and governance structure.

Defining the leadership skills required by IS officers, the book examines the pros and cons of different reporting structures and highlights the various control frameworks available. It details the functions of the security department and considers the control areas, including physical, network, application, business continuity/disaster recover, and identity management.

Todd Fitzgerald explains how to establish a solid foundation for building your security program and shares time-tested insights about what works and what doesn't when building an IS program. Highlighting security considerations for managerial, technical, and operational controls, it provides helpful tips for selling your program to management. It also includes tools to help you create a workable IS charter and your own IS policies. Based on proven experience rather than theory, the book gives you the tools and real-world insight needed to secure your information while ensuring compliance with government regulations.

431 pages, 2011. **54-CRC** Member **$80.00** Nonmember **$90.00**



Illustrating PRINCE2®: Project Management in Real Terms

NEW

By Susan Tuttle

PRINCE2® is a versatile project management method that can be tailored to any project, of any size, in any environment, by any company. It is widely recognized and extensively used. This book will show you how PRINCE2® will enable you to obtain the best possible results from all your projects.

Step by step …
Written by an experienced practitioner and trainer, this step-by-step guide breaks down the PRINCE2® methodology into bite-size chunks, giving clear explanations and practical illustrations in each section. It will show you how to effectively apply the principles, themes and processes of PRINCE2® to your project.

… to effective project management
Use this book to:

- Understand what PRINCE2® actually means in real terms and real language
- Gain insight into what the PRINCE2® method offers you as a project manager
- Learn from others who have used the methodology well or badly
- Use others' experiences as your starting point for your application of PRINCE2®
- Learn better strategies for using PRINCE2® to manage the day-to-day aspects of your projects

Effectively managed projects deliver the desired results. Projects managed with the PRINCE2® framework can increase the efficiency of your business and your customers' trust in you, leading to more business and increased profits!

226 pages, 2012. **15-ITIP** Member **$30.00** Nonmember **$40.00**

EXAM REFERENCE MATERIALS

2013 CISA® EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CISA exam, order ◆

www.isaca.org/cisabooks

CISA Review Manual 2013*

CISA Review Questions, Answers & Explanations Manual 2013*

CISA Review Questions, Answers & Explanations Manual 2013 Supplement*

CISA Practice Question Database v13*

2013 CISM® EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CISM exam, order ◆

www.isaca.org/cismbooks

CISM Review Manual 2013*

CISM Review Questions, Answers & Explanations Manual 2013 Supplement*

CISM Practice Question Database v13*

2013 CGEIT EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CGEIT exam, order ◆

www.isaca.org/cgeitbooks

CGEIT Review Manual 2013*

CGEIT Review Questions, Answers & Explanations Manual 2013*

CGEIT Review Questions, Answers & Explanations Manual 2013 Supplement*

2013 CRISC EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CRISC exam, order ◆

www.isaca.org/criscbooks

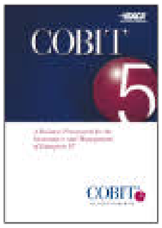
CRISC Review Manual 2013*

CRISC Review Questions, Answers & Explanations Manual 2013*

CRISC Review Questions, Answers & Explanations Manual 2013 Supplement*

COBIT 5 PUBLICATIONS

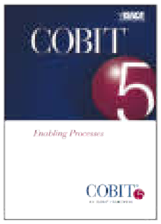
www.isaca.org/featuredbooks


COBIT 5

CB5

Member $35.00

Nonmember $50.00


COBIT 5: Enabling Processes

CB5EP

Member $35.00

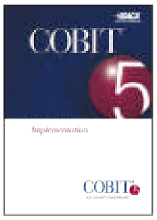
Nonmember $135.00

WCB5EP—E-BOOK

PDF FORMAT

Member FREE

Nonmember $135.00


COBIT 5 Implementation

CB5IG

Member $35.00

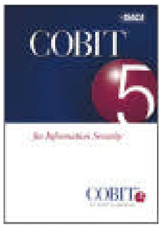
Nonmember $150.00

WCB5IG,E-BOOK

PDF FORMAT

Member FREE

Nonmember $150.00


COBIT 5 for Information Security

CB5IS

Member $35.00

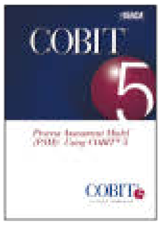
Nonmember $175.00

WCB5IS—E-BOOK

PDF FORMAT

Member $35.00

Nonmember $175.00


COBIT Process Assessment Model (PAM): Using COBIT 5

CPAM5

Member $30.00

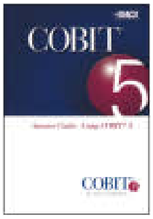
Nonmember $50.00

WCPAM5—E-BOOK

PDF FORMAT

Member FREE

Nonmember $40.00


COBIT Assessor Guide: Using COBIT 5

CAG5

Member $30.00

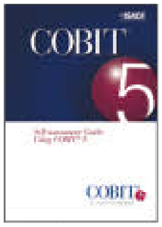
Nonmember $50.00

WCAG5—E-BOOK

PDF FORMAT

Member $30.00

Nonmember $80.00


COBIT Self-assessment Guide: Using COBIT 5

CSAG5

Member $30.00

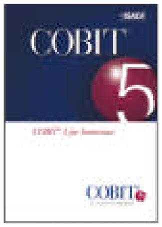
Nonmember $50.00

WCSAG5—E-BOOK

PDF FORMAT

Member $30.00

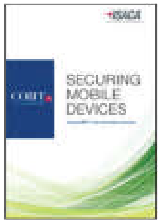
Nonmember FREE


COMING SOON

COBIT 5 for Assurance

CB5A

WCB5A—E-BOOK


Securing Mobile Devices Using COBIT 5 for Information Security

CB5SMD

Member $35.00

Nonmember $75.00

WCB5SMD—E-BOOK

PDF FORMAT

Member FREE

Nonmember $75.00

* Published by ISACA and ITGI

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

All prices are listed in US Dollars and are subject to change

2013 CISA® EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CISA exam, order ◆

Code	Title	Nonmember	Member
CISA Review Manual 2013*			
CRM-13	English Edition	$135.00	$105.00
CRM-13C	Chinese Simplified Edition	135.00	105.00
CRM-13F	French Edition	135.00	105.00
CRM-13I	Italian Edition	135.00	105.00
CRM-13J	Japanese Edition	135.00	105.00
CRM-13S	Spanish Edition	135.00	105.00
CISA Review Questions, Answers & Explanations Manual 2013*			
QAE-13	English Edition (950 Questions)	130.00	100.00
QAE-13C	Chinese Simplified Edition (950 Questions)	130.00	100.00
QAE-13I	Italian Edition (950 Questions)	130.00	100.00
QAE-13J	Japanese Edition (950 Questions)	130.00	100.00
QAE-13S	Spanish Edition (950 Questions)	130.00	100.00
CISA Review Questions, Answers & Explanations Manual 2013 Supplement*			
QAE-13ES	English Edition (100 Questions)	60.00	40.00
QAE-13CS	Chinese Simplified Edition (100 Questions)	60.00	40.00
QAE-13FS	French Edition (100 Questions)	60.00	40.00
QAE-13IS	Italian Edition (100 Questions)	60.00	40.00
QAE-13JS	Japanese Edition (100 Questions)	60.00	40.00
QAE-13SS	Spanish Edition (100 Questions)	60.00	40.00
CISA Practice Question Database v13 (1,050 Questions)*			
CDB-13	CD-ROM—English Edition	225.00	185.00
CDB-13W	Download—English Edition (no shipping charges apply to download)	225.00	185.00
CDB-13S	CD-ROM—Spanish Edition	225.00	185.00
CDB-13SW	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

2013 CISM® EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CISM exam, order ◆

Code	Title	Nonmember	Member
CISM Review Manual 2012*			
CM-12J	Japanese Edition	115.00	85.00
CISM Review Manual 2013*			
CM-13	English Edition	115.00	85.00
CM-13J	Japanese Edition	115.00	85.00
CM-13S	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 Review Questions, Answers & Explanations Manual 2013 Supplement*			
CQA-13ES	English Edition (100 Questions)	60.00	40.00
CQA-13JS	Japanese Edition (100 Questions)	60.00	40.00
CQA-13SS	Spanish Edition (100 Questions)	60.00	40.00
CISM Practice Question Database v13 (900 Questions)*			
MDB-13	CD-ROM – English Edition	160.00	120.00
MDB-13W	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

2013 CGEIT EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CGEIT exam, order ◆

Code	Title	Nonmember	Member
CGM-13*	CGEIT Review Manual 2013	115.00	85.00
CGQ-13*	CGEIT Review Questions, Answers & Explanations Manual 2013 (60 Questions)	60.00	40.00
CGQ-13ES*	CGEIT Review Questions, Answers & Explanations Manual 2013 Supplement (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

2013 CRISC EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CRISC exam, order ◆

Code	Title	Nonmember	Member
CRR-13*	CRISC Review Manual 2013	115.00	85.00
CRQ-13*	CRISC Review Questions, Answers & Explanations Manual 2013 (200 Questions)	60.00	40.00
CRQ-13ES*	CRISC Review Questions, Answers & Explanations Manual 2013 Supplement (100 Questions)	60.00	40.00
XMXCR13-6M*	CRISC Exam Self-Study Subscription–6 Months	225.00	185.00
CACR*	Candidate's Guide to the CRISC Exam and Certification (No charge to paid CRISC exam registrants)	15.00	5.00

COBIT®

Code	Title	Nonmember	Member
COBIT 5			
CB5*	English	50.00	35.00
CB5C*	Chinese Simplified	50.00	35.00
CB5G*	German	50.00	35.00
CB5J*	Japanese	50.00	35.00
CB5SS*	Spanish	50.00	35.00
COBIT 5: Enabling Processes			
WCB5EP*	English, E-Book—PDF format (purchase online only)	135.00	FREE
CB5EP*	English, Print Format	135.00	35.00
WCB5EPG*	German, E-Book—PDF format (purchase online only)	135.00	FREE
CB5EPG*	German, Print Format	135.00	35.00
WCB5EPJ	Japanese, E-Book—PDF format (purchase online only)	135.00	FREE
CB5EPJ	Japanese, Print Format	135.00	35.00
WCB5EPS	Spanish, E-Book—PDF format (purchase online only)	135.00	FREE
CB5EPS	Spanish, Print Format	135.00	35.00
COBIT 5 Implementation			
WCB5IG*	English, E-Book—PDF format (purchase online only)	150.00	FREE
CB5IG*	English, Print Format	150.00	35.00
WCB5IGS	Spanish, E-Book—PDF format (purchase online only)	135.00	FREE
CB5IGS	Spanish, Print Format	135.00	35.00
COBIT 5 for Information Security			
WCB5IS*	E-Book—PDF format (purchase online only)	175.00	35.00
CB5IS*	Print format	175.00	35.00
COBIT Process Assessment Model (PAM): Using COBIT 5			
CPAM5*	COBIT® Process Assessment Model (PAM): Using COBIT® 5	50.00	30.00
WCPAMS*	E-book—PDF format (purchase online only)	40.00	FREE
COBIT Assessor Guide: Using COBIT 5			
CAG5*	COBIT® Assessor Guide: Using COBIT® 5	50.00	30.00
WCAG5*	E-book—PDF format (purchase online only)	80.00	30.00
COBIT Self-assessment Guide: Using COBIT 5			
CSAG5*	COBIT® Self-assessment Guide: Using COBIT® 5	50.00	30.00
WCSAG5*	E-book—PDF format (purchase online only) (does not include the Tool Kit)	30.00	FREE
Securing Mobile Devices Using COBIT 5 for Information Security			
WCB5SMD*	E-book—PDF format (purchase online only)	75.00	FREE
CB5SMD*	Print format	75.00	35.00
CB4.1*	COBIT 4.1	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. ◀

Code	Title	Nonmember	Member
COBIT Mappings			
WCMCMM*	Mapping of CMMI for Development V1.2 With COBIT 4.0	25.00	FREE
WCMISO*	Mapping of ISO/IEC 17799: 2005 With COBIT 4.0	25.00	FREE
WCMIT3*	Mapping of ITIL V3 With COBIT® 4.1	25.00	FREE
WCMNIST*	Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1	25.00	FREE
WCMPMB*	Mapping of PMBOK to COBIT 4.0	25.00	FREE
WCMSEI*	Mapping of SEI's CMM for Software to COBIT 4.0	25.00	FREE
WCMTOG*	Mapping of TOGAF 8.1 With COBIT 4.0	40.00	FREE
WCMFF*	Mapping FFIEC with COBIT 4.1	25.00	FREE
WCM20000*	Mapping of ISO/IEC 20000 with COBIT 4.1	25.00	FREE
WCMCMM2*	Mapping of CMMI for Development V1.2 with COBIT 4.1	25.00	FREE

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

COBIT® *(cont.)*

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™/RISK 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	90.00	80.00
5-RO	A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance	105.00	95.00
RITF*	The Risk IT Framework	95.00	45.00
RITPG*	The Risk IT Practitioner Guide	115.00	55.00
RISK RELATED TOPICS			
78-WRM	The Failure of Risk Management: Why It's Broken and How to Fix It	60.00	50.00
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	98.00	88.00
84-WRM	Information Technology Risk Management in Enterprise Environments	110.00	100.00
2-HBS	IT Risk: Turning Business Threats Into Competitive Advantage	45.00	35.00
1-HHOP	The Operational Risk Handbook for Financial Companies	63.00	53.00
5-PL	Risk Management & Risk Assessment	105.00	95.00
AUDIT, CONTROL AND SECURITY—ESSENTIALS			
48-CRC	Access Control, Security, and Trust: A Logical Approach	105.00	95.00
1-IT9	Accounting Information Systems, 9th Edition	324.00	314.00
93-WAAS	Auditing and Assurance Services: Understanding the Integrated Audit	235.00	225.00
6-PL	Auditing IT Infrastructures	105.00	95.00
53WAG2	Auditor's Guide for IT Auditing + Software Demo, 2nd Edition	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	94.00	84.00
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
51-CRC	Data Protection: Governance, Risk Management, and Compliance	86.00	76.00
13-ITCAT	The Definite Guide to the C&A Transformation	80.00	70.00
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
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	130.00	120.00
4-CRC4	Information Technology Control and Audit, 4th Edition	100.00	90.00
95-WISA	Interpretation and Application of International Standards on Auditing	115.00	105.00
8-PL	IT Auditing: The Process	105.00	95.00
90-WACS	IT Audit, Control, and Security	100.00	90.00
IT Control Objectives for Basel II			
WITCOB*	E-book—PDF Format (purchase online only)	35.00	FREE
ITCOB*	Print Format	50.00	20.00
IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud			
WITCOC*	English E-book – PDF Format (purchase online only)	50.00	FREE
WITCOCI*	Italian E-book – PDF Format (purchase online only)	50.00	FREE
ITCOC*	English Print Format	60.00	35.00
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
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
STDPK*	IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals	20.00	15.00
22-MSM	IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data	60.00	50.00

Code	Title	Nonmember	Member
AUDIT, CONTROL AND SECURITY—ESSENTIALS *(cont.)*			
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
14-ITOM	Once More unto the Breach: Managing Information Security in an Uncertain World	50.00	40.00
7-SYN10	PCI Compliance, Third Edition	70.00	60.00
1-RIA	Practical IT Auditing with current Supplement	470.00	460.00
12-IT	Principles of Information Security, 4th Edition	166.00	156.00
2-SAPP	SAP Security and Risk Management, 2nd Edition	80.00	70.00
28-MSM	Security Metrics: A Beginner's Guide	50.00	40.00
SOC 2: A User Guide			
WSOC*	E-book—PDF format (purchase online only)	75.00	FREE
SOC*	Print Format	75.00	35.00
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
10-ART	Identity Management: Concepts, Technologies, and Systems	119.00	109.00
16-IT	Introduction to Healthcare Information Technology, 1st Edition	83.00	73.00
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
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	80.00	65.00
ISAP3*	Security, Audit and Control Features SAP® ERP, 3rd Edition	75.00	60.00
3-JBSS	Security Strategies in Windows Platforms and Applications	106.00	96.00
30-MWNS	Wireless Network Security A Beginner's Guide	50.00	40.00
NON-ENGLISH RESOURCES			
3-TCA	Administración de la Seguridad de Información, 2nd Edition	55.00	45.00
1-AOCF	Computación Forense: Descubriendo los Rastros Informáticos	50.00	40.00
1-TCA2	Principios de auditoría y control de sistemas de información	60.00	50.00
CISA Examination Reference Material			
Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the June 2013 CISA exam—see page S5			
CISM Examination Reference Material			
Study aids available in Japanese and Spanish for the June 2013 CISM exam—see page S1			
COBIT 5			
CB5C*	Chinese Simplified	50.00	35.00
CB5G*	German	50.00	35.00
CB5J*	Japanese	50.00	35.00
CB5SS*	Spanish	50.00	35.00
COBIT 5: Enabling Processes			
WCB5EPG	German, E-Book—PDF format (purchase online only)	135.00	FREE
CB5EPG	German, Print Format	135.00	35.00
WCB5EPJ	Japanese, E-Book—PDF format (purchase online only)	135.00	FREE
CB5EPJ	Japanese, Print Format	135.00	35.00
WCB5EPS	Spanish, E-Book—PDF format (purchase online only)	135.00	FREE
CB5EPS	Spanish, Print Format	135.00	35.00
COBIT 5: Implementation			
WCB5IGS	Spanish, E-Book—PDF format (purchase online only)	135.00	FREE
CB5IGS	Spanish, Print Format	135.00	35.00

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*

IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud			
WITCOCI*	E-book – PDF Format (purchase online only)—Italian	50.00	FREE

NON-ENGLISH RESOURCES *(cont.)*

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)

INTERNET AND RELATED SECURITY TOPICS

Code	Title	Nonmember	Member
45-CRC	Cloud Computing: Implementation, Management, and Security	90.00	80.00
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
10-IT	Cybersecurity: The Essential Body of Knowledge	107.00	97.00
95-WCSP	Cyber Security Policy Guidebook	90.00	100.00
4-MGH3	Gray Hat Hacking: The Ethical Hakers Handbook, 3rd Edition	70.00	60.00
23-MHE	Hacking Exposed Web Applications, 3rd Edition	60.00	50.00
2-MCG7	Hacking Exposed 7: Network Security Secrets & Solutions, 7th 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
54-CRC	Information Security Governance Simplified: From the Boardroom to the Keyboard	90.00	80.00
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
1-WCNR	No Root for You: A Series of Tutorials, Rants and Raves, and Other Random Nuances Therein	33.00	23.00
15-IT	Official Certified Ethical Hacker Review Guide:For Version 7.1, 1st Ed	50.00	40.00

Security Considerations for Cloud Computing

Code	Title	Nonmember	Member
WSCC	E-book—PDF Format (purchase online only)	75.00	FREE
SCC*	Print Format	75.00	35.00
24-MSIEM	Security Information and Event Management (SIEM) Implementation	75.00	65.00
27-MSC	Securing the Clicks: Network Security in the Age of Social Media	50.00	40.00
2-JBSF	System Forensics, Investigation, and Response	106.00	96.00
29-MWAS	Web Application Security: A Beginner's Guide	50.00	40.00

IT GOVERNANCE AND BUSINESS MANAGEMENT

Code	Title	Nonmember	Member
94-WIFRS	An Executive Guide to IFRS: Content, Costs and Benefits to Business	50.00	40.00
3-PAGE	7 Steps to Better Written Policies and Procedures	30.00	20.00
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
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
54-WCIO2	CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition	80.00	70.00
WCCS*	Creating a Culture of Security (e-book)	50.00	FREE
11-ITDG	The Data Governance Imperative	50.00	40.00
89-WEG	Empowering Green Initiatives with IT: A Strategy and Implementation Guide	60.00	50.00
13-IT	Ethics in Information Technology, 4th Edition	110.00	100.00
3-VH	Frameworks for IT Management	65.00	55.00
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

IT GOVERNANCE AND BUSINESS MANAGEMENT *(cont.)*

Code	Title	Nonmember	Member
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
15-ITIP	Illustrating PRINCE2®: Project Management in Real Terms	40.00	30.00
4-ID	Implementing Information Technology Governance: Models, Practices and Cases	110.00	100.00
46-CRC	Implementing the Project Management Balanced Scorecard	94.00	84.00
11-ITISQ	Implementing Service Quality based on ISO/IEC 20000, 3rd Edition	35.00	25.00
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

Code	Title	Nonmember	Member
W3ITG*	E-book—PDF Format (purchase online only)	45.00	FREE
3-ITG*	Print Format	50.00	25.00
WSH*	Information Security Harmonisation: Classification of Global Guidance (E-book—PDF format purchase online only)	40.00	FREE
50-CRC	Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement	90.00	80.00
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
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	217.00	207.00
81-WIC	Internal Controls Policies and Procedures	90.00	80.00
4-ITIG	IT Governance: A Pocket Guide	25.00	15.00
5-AS13	IT Governance: Policies & Procedures, 2013 Edition	285.00	275.00
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	40.00	30.00
11-VH	IT Outsourcing: Part 1 Contracting the Partner	41.00	31.00
12-ITPM	IT Project Management: 30 Steps to Success	30.00	20.00
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
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	32.00	22.00
MIC*	Monitoring Internal Control Systems and IT	70.00	55.00
2-ITO	Outsourcing IT: A Governance Guide	60.00	50.00
3-JR	A Practical Guide to Reducing IT Costs	55.00	45.00
6-RO	Principles and Practice of Business Continuity: Tools and Techniques	85.00	75.00
1-IS	The Privacy Management Toolkit	505.00	495.00

Security Awareness: Best Practices to Secure Your Enterprise

Code	Title	Nonmember	Member
WSA*	E-book—PDF Format (purchase online only)	35.00	20.00
PSA*	Print Format	50.00	35.00
13-VH	The Service Catalog	65.00	55.00
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
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.

ISACA®
Trust in, and value from, information systems

Customer Order Form

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

OFFICE USE ONLY

Vol. 3-13

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), Puerto Rico (PR), 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 □ Discover
□ 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 v13—download.
No shipping charges apply to CISM Practice Question Database v13—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.**

ISACA
COBIT®
5
for Assurance
COMING SOON!
COBIT® 5
AN ISACA® FRAMEWORK