Data Analytics/Mining

Featured articles:
Everybody Loves Documentation
The Importance of the ARA
How to Maximize Evidential Weight of Electronically Stored Information
And more...
Do security weaknesses exist within your organization?

ANNOUNCING

COBIT® 5 for Information Security

COBIT 5 for Information Security provides a holistic, end-to-end view of COBIT® 5 to help enterprises manage risk and endure compliance, continuity, availability, security and privacy. This framework supports IT assets and business goals to help ensure that information systems comply with necessary risk controls.

To download or order COBIT 5 for Information Security or to learn more about how it can help increase trust in, and value from, information systems, visit www.isaca.org/COBIT5IS-journal or email research@isaca.org.
Regis University offers a Graduate Certificate as well as a Master’s Degree in Information Assurance. With both programs, you have the option to take classes online or on-campus. Regis University is also designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency.

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

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

The program can be taken on campus or completely online.

**MASTER’S DEGREE**
- Two year program
- Specialize in cybersecurity or policy management

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

**THE REGIS UNIVERSITY SCHOOL OF COMPUTER & INFORMATION SCIENCES**

LEARN MORE
RegisDegrees.com/ISACA | 1-877-820-0581
Guest Editorial: From Continuous Auditing to Continuous Monitoring—You Should Be the Champion
Michael P. Cangemi, CPA

Information Security Matters: Keynes, Shelley, Taleb and Watts
Steven J. Ross, CISA, CISSP, MBCP

Cloud Computing: Securing Hybrid Cloud Applications
Carson Sweet

IT Audit Basics: Auditing Applications, Part 2
Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA

Five Questions With…
Gregory T. Grocholski, CISA

Reviewed by Bright Mungongwa, CISA, CGEIT, CRISC, CIA

Everybody Loves Documentation
Adrienne Bellehumeur, CISA, CA, PMP

The Importance of the ARA
Danny M. Goldberg, CISA, CGEIT, CCISA, CIA, CPA

Seven Myths of Information Governance
Vasant Raval, DBA, CISA, and Greg Dyche

How to Maximize Evidential Weight of Electronically Stored Information
Haris Hamidovic, CIA, ISMS IA, ITIL, IT Project+

SAP Password Vulnerabilities and Access to Sensitive Business Data
Jose Espin, CISA, CISSP, MCP, SAP

Applications of Business Process Analytics and Mining for Internal Control
Filip Caron and Jan Vanthenen, Ph.D.

To Click or Not to Click? That Is the Question
Carlo Rossi, CISA, CISM, CGEIT, ISO 27001 LA

El Negocio de la Seguridad de la Información: Revelando la Potencialidad de un Concepto
Jeimy J. Cano M., Ph.D., CFE, CMAS

10 Key Rules for Using the ITIL Framework Effectively
Debasis Bandyopadhyay, CISA, CISM, CGEIT, PMP, TOGAF9, ITIL v3 (F)

Crossword Puzzle
Myles Mellor

Help Source Q&A
Gan Subramaniam, CISA, CISM, CCNA, CCISA, CIA, CISSP, ISO 27001 LA, SSCP

Quiz #143
Based on Volume 2, 2012
Prepared by Sally Chan, CGEIT, CMA, ACIS

Standards, Guidelines, Tools and Techniques
S1-S8
ISACA Bookstore Supplement

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.
Apply for a position that offers lifelong well-being.

Join the Internal Audit Consulting Group at Humana and get the kinds of benefits that can’t be quantified.

Humana is a leading healthcare company that offers you the best of both worlds. You not only get to work with our award-winning Internal Audit Consulting Group, you also get benefits that go beyond medical and retirement plans. We offer a range of programs designed to support your overall health and well-being, like a competitive Paid Time Off program and a charity matching gift program. At Humana, you get the opportunity to do your best work while you enrich your life.

Find out what opportunities await you with Humana. 
Careers.Humana.com
Keyword search: IA001
It is often said: It is better to understand than to be understood.

When a career, which started in IT audit, runs through positions including chief audit executive (CAE), chief information officer (CIO), chief financial officer (CFO), chief executive officer (CEO), public company director, audit committee chair, as well as a 20-year stretch as the editor-in-chief of the ISACA Journal, what would you expect next?

I doubt many of you would have expected a concentration on, of all things, continuous monitoring (CM). When Pfizer was facing the loss of its patent protection on Lipitor, would you expect them to turn to CM? I’ll explain this one later.

The central themes to my long career include business development, finance/accounting and information technology. I started out on Wall Street at 16, and the first computer arrived at the firm while I was in college studying accounting. My big break came when a search was made for a CFO who could advance the use of technology to grow the business.

The one skill set that propelled my career was the use of technology: first in audit, then in finance, and then in management. Technology, combined with a passion to advance the organization’s development and performance, was the ticket to success. Technology’s expansion kept the wind at my back.

Now that I can choose whatever I want to focus on, I like to spend my time with technology companies. Within technology I have a chance to promote what I have always regarded as key: CM. When I was first exposed to automated auditing in the 1970s, it fueled a desire to see a paradigm shift away from traditional backward-looking audit methods to real time. As an early adopter of computer technology for governance, risk and compliance (GRC), I predicted the explosive growth of continuous automated auditing. In fact, I predicted it at least a half dozen times!

Well, even a broken clock is correct two times a day!

My vision of the future was to come, but much more slowly than I expected. But, come it has! These days, there is an ever-expanding, Orwellian interest in monitoring in general. Think of cameras looking for terrorists, credit card fraud monitoring, traffic-signal violations monitoring, medical-condition monitoring; however, in financial areas, we have tended to focus on continuous assurance/auditing and continuous controls monitoring.

This is the era of big data, which are large pools of data that can be captured, communicated and analyzed. With advancing high-speed computer processing, CM systems are being deployed using automated advanced analytics to sift through the large volumes of structured data, such as financial transactions, that comprise a large part of an organization’s big data. Available software employing intelligent, proprietary and, in some cases, patented techniques highlights and, electronically of course, passes on to humans actionable information for follow up.

Think about how IBM’s Watson computer sifts through reams of data to estimate and weigh correct answers, allowing it, a computer, to compete against Jeopardy’s human champions.

Last year, I coauthored a research paper titled “The Benefits of Continuous Monitoring.” Under the direction of Financial Executives Research Foundation (FERF), and its Committee on Finance and Technology, the authors interviewed major companies to determine the level of understanding in organizations regarding CM and the state of plans for implementation.

The study confirmed what this former IT audit specialist always knew: While CM has some of its roots in continuous assurance monitoring, it is expanding at a rapid pace in many organizations.

The key findings of the FERF research are:

• CM deployment—Leading companies recognize the importance of monitoring, and are
effectively deploying CM across functions and departments. They recognize how CM can be a precondition for achieving superior corporate performance, as well as governance outcomes.

- **Resourcing CM initiatives**—CM programs require a company focus and a commitment of resources. Some companies mentioned the need for return on investment (ROI) estimates, but others look beyond monetary justifications and focus instead on operational effectiveness and risk reduction.

- **Need for CM champion**—CM programs need a champion, preferably at a senior executive level, because resources will be required.

- **Internal audit as evangelist**—Although CM is a business operations issue, internal audit (IA), due to its familiarity with continuous auditing (CA), often becomes the champion of CM programs.

- **CM of payment streams**—CM is often initiated in payment-related areas, such as accounts payable and claim payments, in which, due to cash recoveries, the ROI can be estimated.

- **CM software and tools**—There are many new CM software products available that have improved capabilities and lowered the cost of using CM.

- **Expanding applications**—For all of the companies that launched a CM initiative, there was a keen desire to expand the application beyond the initial sponsoring department or division, as well as to move up the maturity curve.

- **Benchmarking**—Each company in the sample was curious to learn more about how CM is deployed in other environments and industries, with a view toward improving its own processes. This was also a prime reason for each company’s participation in this research. Let’s look at a few of the key findings.

**FROM CONTINUOUS AUDITING TO CONTINUOUS MONITORING**

The use of automated monitoring by independent auditors, internal or external, is referred to as continuous auditing, or CA. In many ways, CA uses the same monitoring techniques, deployed independently, as a check on management systems and controls. Our research shows that while many companies have seen, and still see today, CM initiatives coming from base CA projects from IA, there is an emerging trend to get CM into operations. Only in operations can CM reach its full potential, become scalable and leverage the already-massive investment in IT, with continuous transaction analytics for big data.

**ASSURANCE PROFESSIONALS AS THE CHAMPIONS OF CM**

In a 2010 article titled “Internal Audit’s Role in Continuous Monitoring,” I stated: “Continuous monitoring is a business operational issue swirling around in auditing and accounting practices!” The rationale for this statement stems from the role auditors played in establishing the concept of automated monitoring and the extensive published guidance. However, as seen from the 2011 Financial Executives International (FEI) research, the real benefit comes from these assurance professionals recommending and facilitating building CM into operations.

That said, while CM is predominantly a business operations issue, it can also add to the internal control system and, therefore, most times it affects audit coverage through audit scope reductions. For example, COSO has always included monitoring in its Internal Control—Integrated Framework, and recently released a comprehensive guidance on monitoring, called Guidance on Monitoring Internal Control Systems. IT security professionals and IT managers who look to automated solutions have embraced CM software for monitoring many IT controls and security applications.

However, I like to say that internal control improvement is the tail, not the dog. First, you have to have a business function, then you need internal control.

The FERF research shows many good examples of IA leading the way on design and recommending CM. Just look at the IBM, Wells Fargo, American Electric Power and J.C. Penney examples in the study. IA should be keenly focused on making operations management aware of these new, automated CM systems to improve efficiencies and effectiveness of the operations to be audited.

In my time as a CAE, I looked for ways to go beyond audit and add to the control infrastructure of the business. I call
these positive deliverables and recommended this approach in my book Managing the Audit Function, now in a third
dition. Recommending CM is a classic example of a
positive deliverable.

PAYMENT SYSTEMS—CASH RECOVERIES ROI

Not surprisingly, many astute financial executives in major
companies have begun to use CM as an extra arrow in their
expenditure-controls quiver. Here, CM can be structured to
reduce duplicate payments, so it is an added control and,

hence, part of the expanded internal control (IC) system.

Why is this so popular? The cash recoveries often exceed the
cost of the software and implementation. What is not to love
when your cash recoveries can easily exceed your incremental
software and comparatively mild implementation costs?

For example, from the FERF research: “[United
Technology Corporation’s] Center of Excellence launched an
initiative to reduce or even eliminate duplicate payments. [The
organization] identified the Oversight Systems’ procure-to-pay
(P2P) module as a viable tool to use for this initiative. The
P2P module provides 110 predefined, customizable integrity
checks from which UTC could choose for this initiative.”

Still, many companies use contingency firms to monitor
payments, and the success of these contingency firms proves
the need to monitor. However, is giving away 45 percent of the
recovery really a positive deliverable?

At the beginning of this article, I mentioned an example
related to Pfizer’s use of CM when facing the loss of its patent
protection on Lipitor. When a company is facing the loss of a
major product, it actually does many things, including using
CM of travel and entertainment expenses to lower costs.
Pfizer Inc. launched an innovative strategy to retain sales of
Lipitor, while also launching a CM strategy to innovatively
control expenditures, with big data analytics and business
process optimization.

According to Loretta Cangialosi, controller at Pfizer:
“With CM systems for our travel and entertainment process
and three employees, we can review and act on discrepancies
identified by continuously monitoring thousands of
transactions in a way that would have required at least 30
employees using traditional auditing methods.”

In this case, the CM champion was the controller, but it
could be you!

CM SOFTWARE AND TOOLS

Financial executives understand that when there is a business
case, investment money will flow into the development of
products. One of the best examples of the coming of age of
CM is the emergence of new software companies, funded in
many cases by private equity investment funds.

The FERF research reported that “there are many new CM
software products available that have improved capabilities
and lowered the cost of using CM.” As mentioned, CM
software uses specialized monitoring techniques such as
analytics, inference, weighting and artificial intelligence. Some
call this the CM “secret sauce.” Whatever it is called, the point
is: Large investments have been made in specialized software
technology by companies who have dedicated their computer
scientists to advances in CM. Many of the companies
interviewed are taking advantage of this available CM
software. Why reinvent the wheel? I suggest that you review
the CM software tools appendix in the research.

SAP and other enterprise resource planning (ERP) vendors
have built in some aspects of CM. However, there are gaps,
especially related to continuous transaction analytics for big
data. SAP has recognized the need for expanded CM by, for
example, naming Oversight Systems as an endorsed business
partner.

SME MONITORING—CM TOOLS AVAILABILITY

Our research focused on larger entities; however, there are
tools well within the reach of smaller companies, as listed
in the software tools appendix in the research. In fact, while
CFO of Etienne Aigner, a small
cap, we used Caseware’s Idea
software, which I had been
using in internal audit and
public accounting. The product
was easy to use and low in cost.

We are all becoming more aware of and comfortable with
monitoring in general. It is all around us and facilitates our
lives in many ways. The connection between assurance and CM
knowledge is clear—the time is right to become a champion of
CM. Those of us who focus on technology will come to embrace
the movement of CM as a foundation technology for business
performance improvement, and a solution to address big data,
turning them into a useful source of business analytics. Mr. Li
Ka-shing, a post-80-year-old, semi-retired billionaire investor, who now backs tech start-ups such as Facebook, proclaims: “A person investing in technology will feel younger.”

I enjoy seeing the explosive growth of CM, within the continued evolution of technology in general. I really enjoy seeing technology make business and people’s lives better and better every day. Like Mr. Li, my pursuit of technology, like CM, provides an intellectual challenge, a rewarding career step and keeps me young at heart.

ENDNOTES
1 Author George Orwell (1903–1960) was an English novelist and journalist who wrote about invasion of personal privacy by government surveillance, among many other issues, in his novel Nineteen Eighty-Four.


3 Ibid.


5 The Committee of Sponsoring Organizations of the Treadway Committee (COSO) was formed in part to help define internal control after the passage of the Foreign Corrupt Practices Act in the US.


All security threats will eventually come to pass. With enough time, all security vulnerabilities will be exploited. John Maynard Keynes famously said that “In the long run, we are all dead.” What Lord Keynes meant is that just because something has not happened in the short term, does not mean that it will not happen over time. So, some security threats may not come to pass for any given organization; the organization may go out of business first.

These cheery predictions are brought to my mind in the context of security risk assessments, which attempt to identify the most serious threats and vulnerabilities in information systems so that management can make knowledgeable investments in safeguards, attempting to minimize the greatest risk, rather than tackle the Sisyphean task of preventing them all. Sometimes risk assessments are performed following some formal process, such as that elaborated in ISO 27005. Others rely on the personal knowledge and educated intuition of the analysts. In either case, assessing the risk of information security failures is an exercise in prediction, one that is ultimately either futile or self-defeating.

**THE STANDARD FORMULA**
I have previously discussed the limitations I see in current risk assessment techniques, both in this space and elsewhere.

My primary concern is that almost all standard methodologies rely on what I consider to be a fallacious formula, namely: Risk = Impact × Probability (or R = I × P, in common shorthand). The trouble with this simple approach is that it is indeed quite too simple. First of all, we cannot know in advance what the impact of a hack or a disaster or a leakage of data will be. At best we can guess; at worst we can tell a horror story meant to extract budget from reluctant senior managers. The fact is, risk is based on uncertainty; no one can ever know for sure what the future will bring.

The concept of probability is no better in aiding us in predicting the future. The common warning that past results do not indicate future returns when applied to financial investments seems to be routinely ignored when applied to the potential impacts of negative events on computer systems. (Come to think of it, the warning seems to be commonly overlooked by investors as well.) The rate of occurrence of security failures will always be an unknowable variable because the conditions that affect it—most notably the incentives for the attackers and the effectiveness of the safeguards—are in a constant kaleidoscope of change.

Thus, the standard formula, evoked in ISO 27005 as the “process to assign values to the probability and consequences of a risk,” is sure to fail. Is it any wonder that the multiplication of the unknown and the unknowable does not produce reliable results?

And moreover, why multiplication? Why should the formula be R = I × P, any more than R = IP or R = PI? The most we can say, if we are thoughtful about risk, is that it is a function of impact and probability at the very least. There are surely other factors to consider such as scale, duration, speed of onset, mean time to occurrence and mean time to repair. So perhaps, for the mathematically inclined, the formula should be: Risk = f (impact, probability, duration…), which can be represented graphically only in an oddly nonprobabilistic, über-Gaussian fashion.

**THE DREAM OF PREDICTION**
Nassim Nicholas Taleb’s groundbreaking book, *The Black Swan,* is essentially a lengthy screed against Gaussian bell curves and standard deviations. To condense his argument into a few sentences: Just because something happens regularly does not mean that it will continue to do so in the future. Put in a more statistical fashion, the Gaussian bell curve can show probabilities, but the Black Swan—in this case, a devastating security event—will be an outlier to the curve. “We are fooled by the rarity of Black
Swans…not only by the role they play in the aggregate, [but by] their impact.”7 In short, the effects of the security events predicted at the beginning of this article can be understood, but not their probability.

In his new book, Duncan Watts has somewhat taken even my opening predictions to task. Though they might be correct, the idea that “given enough time all bad things will happen” is of no use to anyone who needs to deal with them. He writes, “Predictions that the…sun will continue to rise in the east are likely to be accurate, but impress no one. The real problem is not that we are universally good or bad at it, but rather that we are bad at distinguishing predictions that we can make reliably from those that we can’t.”8 Therefore, the fact that over time passwords will be disclosed and hackers will try to penetrate systems can lead to a reliable risk assessment, but one that is of little use or relevance.

For complex systems, Watts says, “The best we can hope for is to correctly predict the probability that something will happen.”9 For security systems in particular, probability has little or no meaning. In almost every organization on almost every day, there are no major security breaches. Therefore, it is probable that there will not be one tomorrow, and our predictive powers, such as they are, will fully support disregarding the possibility of one occurring. But, there is a gaping difference between rarely, even extremely rarely, and never. Ignoring the remote chance of a major breach is virtually an invitation for one to occur, no matter what a risk assessment tells us. Taleb offers the analogy of the Thanksgiving turkey who is well fed and well housed for 300 days only to find out the week before the holiday that improbable events do occur with devastating impact.10

**Ozymandias**

Now, my thesis is neither that we should give in to nihilism nor that we should avoid risk assessments. However, we should proceed with an understanding that risk assessments are flawed instruments that enable management to focus on the greatest probable risk areas; they cannot predict the actual devastating events that may very well occur despite the probabilities.

As is so often the case, the poets have warned us about the evanescence of life and the futility of predicting the future. Shelley wrote:11

---

ENDNOTES

1 Keynes, John Maynard; *A Tract on Monetary Reform*, 1923, ch. 3
3 Ross, Steven J.; “Gang Aft Aglay,” *ISACA Journal*, vol. 3, 2009
5 Op cit, ISO/IEC, p.2. To be fair, ISO 27005 offers this as a definition of risk estimation, not risk assessment, but the concept behind the formula runs throughout the document.
6 Taleb, Nicholas; *The Black Swan*, Random House, USA, 2007
7 Op cit, Taleb, p. 79
8 Watts, Duncan; *Everything is Obvious: Once You Know the Answer*, Random House Digital, USA, 2011. I have mentioned Watts several times in recent footnotes and devoted an entire column, “Professor Watts Explains It All” to his previous book, *Six Degrees: The Science of a Connected Age*, in vol. 1, 2007.
9 Ibid.
10 Op cit, Taleb, p. 40–41
11 Shelley, Percy Bysshe; “Ozymandias,” 1818
The cloud is here to stay. Companies small and large, all across the globe, are investing in cloud technology. The ability to deploy and scale applications in the cloud in minutes instead of weeks is game changing in terms of speed to market, flexible growth strategies and cost management. Many companies are moving to Software as a Service (SaaS) models, which fuel cloud adoption at multiple levels. No company wants to watch its competition reap these benefits while it lags behind.

Public Infrastructure as a Service (IaaS) providers, such as Amazon, Rackspace, GoGrid and Terremark, are enjoying rapid adoption, as are hybrid-oriented cloud infrastructure technologies, such as Eucalyptus and OpenStack. Hybrid cloud hosting offers several key advantages over public or private cloud hosting:

- **Convenience**—Organizations can delay or avoid purchasing, installing and maintaining hardware. Hybrid allows a company’s virtual servers to be deployed from its private cloud environment to public IaaS easily and quickly.
- **Agility**—New servers can be up and down within minutes, either in the public cloud environment or the public IaaS environment. Use cases, such as temporary growth for product testing or rapid customer deployment, become faster and easier, and include more controlled costs.
- **Economics**—Companies no longer need to build the largest-needed server farms to handle peak capacity just to have large percentages of their server capacities idling. Using the hybrid combination of private cloud and public IaaS, capacity can scale up and down dynamically to match business needs and recover costs wasted on idle servers.

The hybrid model enables companies to cover their day-to-day computing needs using their private clouds, bursting into public cloud resources for peak workloads, transient computing needs and rapid-deployment scenarios. The benefits of this model are driving rapid growth, although the model does come with concerns.

**SERVER SECURITY AND COMPLIANCE**

Security and compliance are two of the biggest obstructions to hybrid cloud adoption. While organizations such as the Cloud Security Alliance have made great strides toward education and guidance regarding cloud security, a range of technical challenges and misunderstandings still places companies at risk.

The technology community recognizes that servers hosted in multitenant clouds are at increased risk without layers of in-depth perimeter controls, typically found in the data center. CloudPassage recently conducted a nationwide survey among 164 technology professionals and found that:

- 45 percent of respondents cited a lack of perimeter and/or network controls as their primary cloud security concern, making perimeter defenses their chief cloud security issue
- 39 percent were uncomfortable with the concept of multitenancy, where a number of companies share the same infrastructure
- 21 percent understood that their traditional enterprise security tools no longer work in the cloud
- 31 percent of respondents believe that their cloud provider will take care of securing their cloud servers

For information security and compliance professionals, the last statistic on the list should be of great concern. A large percentage of cloud users are under the misguided belief that they have no responsibility for cloud server security.

In reality, cloud providers place the responsibility for virtual server security squarely on their customers. They will, of course, secure the shared network, hardware and hypervisor environments that support the guest virtual machines, but the customers are directly responsible for protecting their own virtual cloud servers, starting with the operating system and moving up the stack to include network, application and database services in use.

**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:
Almost all providers spell this out clearly in their service level agreements (SLAs) and advise their customers to implement firewalls, intrusion detection systems and other security controls. While most providers are transparent, some providers do leave customers in the dark on this critical issue. The security SLA is one of the first areas to examine as businesses consider the risk implications of allowing servers and data into public cloud environments, a critical component to achieving the benefits of hybrid server hosting.

CLOUD SECURITY IS DIFFERENT
Data centers have long relied on strong perimeter controls to prevent server weaknesses from being exploited. Servers were safe behind the corporate firewall, and that belief in safety could lead to relatively lax enforcement of security standards at the server level. Unfortunately, weak server protection makes its way easily into private cloud hosting, making it one cloudburst from severe exposure of servers moved onto public resources.

Securing cloud servers requires a new approach. Dynamic cloud environments, especially public IaaS clouds, have greatly reduced the network and hardware control needed to create defined perimeters or security choke points. The technical nature of cloud-hosting environments also makes them more difficult to secure. Cloud server security mechanisms need to dynamically scale up and scale down with the servers themselves, and organizations need to be flexible in the ability to operate in either the private or public sides of a hybrid cloud.

The elastic nature of cloud-hosting environments can also lead to dramatic increases in exploitable server vulnerabilities. Cloud servers are easily replicated or cloned within seconds, typically to increase available computing power. If a server is vulnerable to exploit, cloning that server multiplies the vulnerable surface area available to attackers. Every single server has to be rigorously hardened before it can be exposed to public cloud threats; the speed and scale of cloud deployments coupled with deteriorating change management makes automation absolutely critical.

“Securing cloud servers requires a new approach.”

AVATAR NEW YORK’S HYBRID SECURITY APPROACH
One of CloudPassage’s customers is New York-based digital agency Avatar New York. Avatar was founded in 2003 and combines art and technology to deliver consistent branding and solid e-business solutions that are deployed on a combination of public and private cloud infrastructures.

Patrick Tully, Avatar’s chief technology officer, had the vision of leveraging the agility and scalability of the cloud to match the increasing pace of his customer’s demands. “Our Internet solutions must be delivered fast and with maximum flexibility for the future. We engineer technology requirements on a real-time basis as business models are changing in conjunction with new technologies,” Tully says. His team needed to ramp up its number of Rackspace servers frequently, using automated tools such as Puppet to meet the computing demands of the organization’s customers.

Since the organization manages valuable customer information, it has rigorous security requirements. Initially the Avatar New York team used traditional security products, but soon found that these tools were not designed to work in dynamic cloud environments. “They took hours to configure and did not have an [application programming interface (API)] for automation,” Tully recalls.

Tully had read about CloudPassage on a blog and went to its website, where he learned more about Halo. “I was impressed when I asked a question on the community site and got my answer in less than 24 hours,” remembers Tully. He signed up for the free Halo Basic platform, and in only a few minutes Halo was installed on Avatar’s cloud servers. Avatar’s main goal was to use the configuration management and software vulnerability
scanning capabilities of Halo to harden its servers. The organization found that Halo included a number of standard security policies that allowed it to get up and running quickly. Avatar soon added its own very specific policies.

Today, Avatar New York has all of its public cloud servers protected by Halo around the clock. The IT team can automatically spin up new servers within minutes, and ensure that all of them are secure. “We wrote Puppet scripts so that every new server is automatically protected by Halo right from the start, without any manual intervention,” Tully explains.

One of the challenges of relying on third-party infrastructure for Avatar New York is a lack of visibility. Some of Avatar’s customers have very specific questions regarding compliance, policies and security. “When you are running more than 50 servers in the cloud, it is hard to do it without an automated system,” Tully says. “Halo helps us make sure that nothing gets overlooked. It is our way to constantly monitor and audit our systems and policies.”

Avatar is interested in rolling out an API integration with Halo Professional as the next step. The API will play a major role in Avatar New York’s infrastructure going forward.

CONCLUSION
In summary, it is critical that companies understand their responsibility when it comes to securing their public or hybrid cloud environments. They need to review the related risks and implement security controls that are well adapted to the dynamics of the cloud. Once IT management has addressed these security issues, public IaaS will become a standard component for implementing agile and scalable computing with hybrid cloud-hosting models.
Auditing Applications, Part 2

This is the second part of a two-part article on a process-oriented framework for auditing applications. Part 1 (volume 3, 2012) detailed the first three steps: planning, determining objectives and mapping. The remaining steps are described here. The full framework includes the following steps:

- Plan the audit.
- Determine audit objectives.
- Map systems and data flows.
- Identify key controls.
- Understand application’s functionality.
- Perform applicable tests.
- Avoid/consider complications.
- Include financial assertions.
- Consider beneficial tools.
- Complete the report.

IDENTIFY KEY CONTROLS

When evaluating the relevant controls, the IT auditor will want to distinguish between customized controls and those contained in commercial off-the-shelf software (COTS). For custom-built controls, inquiry is a good place to begin the evaluation. One of the key questions is to ask management the specific nature of controls expertise being injected into the application development process. That is, who or what group is providing the expertise that makes sure adequate controls are embedded in new applications? How is that goal achieved? And, finally, the IT auditor should make sure those controls have been properly documented and tested.

For COTS, the IT auditor would probably start with a walk-through to determine what controls are actually in the application and how they function. A walk-through would involve following transactions or processes step by step, keystroke by keystroke, with the data-entry person explaining what they are doing and why. Such a process should enable the IT auditor to gain a general understanding of the applications’ controls, the adequacy of controls and the nature of them (i.e., effectiveness). This walk-through is especially necessary the first time an application is used by the entity.

Also for COTS, the IT auditor should establish a baseline of controls—tests to understand reliability and effectiveness. These would include configurations for applications, such as SAP and Oracle.

For COTS, the IT auditor needs to determine the responsibility of vendors involved. That goal is why figure 1, which is part of the mapping step and detailed in part 1 of this article, has information about the vendor and the nature of maintenance of the application. When a problem occurs with the application, management needs to have assurance of exactly who to rely upon to solve the problem. Obviously, vendor management practices apply.

Figure 1—Mapping Example Using Spreadsheet, Part I

<table>
<thead>
<tr>
<th>IT</th>
<th>Description</th>
<th>O/S</th>
<th>DBMS</th>
<th>DB Server</th>
<th>Data Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC App</td>
<td>Middleware designed to ...</td>
<td>N.A.</td>
<td>N.A.</td>
<td>XYZ</td>
<td>Birmingham</td>
</tr>
<tr>
<td>DEF App</td>
<td>CRM, target ...</td>
<td>Z/OS</td>
<td>DB2</td>
<td>Z mainframe</td>
<td>Nashville</td>
</tr>
</tbody>
</table>

Figure 1—Mapping Example Using Spreadsheet, Part II

<table>
<thead>
<tr>
<th>Developed</th>
<th>Maintained</th>
<th>Owner</th>
<th>Access Admin</th>
<th>Change Control</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-house</td>
<td>In-house</td>
<td>Sue Z.Q.</td>
<td>Active directory ...</td>
<td>Controls include ...</td>
<td>Yada ...</td>
</tr>
<tr>
<td>Vendor</td>
<td>Vendor, SOC1/2 available</td>
<td>John D.</td>
<td>Security admin ...</td>
<td>Vendor ...</td>
<td>Yada ...</td>
</tr>
</tbody>
</table>

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at Columbus State University (Columbus, Georgia, USA). Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs & Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.
The types of controls can be assessed by using the typical systems model: input, process and output. Input controls include:
- Access security
- Logical segregation of duties (SoD)
- Data validation
- Data integrity
- Coding
- Input error correction
- Batch controls (where applicable)

Typical process controls include:
- The level of automation (e.g., fully automated, IT-dependent, fully manual)
- Job scheduler dependencies (for job processing)
- Job scheduler monitoring
- Auto calculations
- Auto reconciliations
- Auto notifications

Typical output controls include:
- Reconciliations
- Reviews
- Approvals
- Error detection/error reports or lists
- Control over physical reports (ancillary control)

UNDERSTAND APPLICATION’S FUNCTIONALITY
Normally, auditing functionality is a chief audit goal. The procedures involve verifying the operational functionality, which should be described in the information requirements in the application development (AppDev) process. Besides reviewing the authorization document for the application, the IT auditor should review the end-user acceptance report—if one exists. If one does not exist, that says something about the adequacy of control procedures for AppDev. They are lacking a best practice.

Some typical objectives are related to the purpose of the application. When testing the application, consideration is given to the various scenarios needed to properly test the application. If the purpose of the application leads to a dichotomous outcome, a test of one might suffice (yes or no, approved or not approved, etc.). But, if the application is an update to payroll processing, for example, there are a large number of scenarios to consider to test all of the various combinations of factors that go into calculating payroll taxes.

The same is likely to be true of testing security and access controls.

Some special considerations include at least a couple of things that the typical end user and business manager tend to overlook in the information-requirements-gathering stage: security and proper scope of data captured. The proper level of security is obviously a critical success factor in AppDev and, thus, needs to be evaluated. Typically, users and managers do not fully grasp the scope of data that need to be captured at the point of events and transactions. This fact is especially important if the entity has any plans to ever employ, for example, business intelligence (BI) or business analytics. A richness of data becomes necessary to “slice and dice” data with data mining tools to gain the maximum benefit of the data in employing BI.

Operational controls might be in scope, depending on the consideration of purpose. The same is true for financial reporting controls.

Using the system model is likely to make analysis and testing of the application’s functionality easier and more complete.

PERFORM APPLICABLE TESTS
When an application fails to perform correctly, when there are errors created, when processes embedded in the application fail to work properly, the problem can usually be traced back to an improper testing phase. Testing the application is more than just performing a single test.

The best practice for testing involves multiple levels of testing. First, the application is tested stand-alone. That is usually done by a senior programmer or analyst who is chiefly responsible for the AppDev project. Then, the application goes through some quality control in the IT department. That is, it is independently tested by some expert in the IT department.

Next, the application is tested by actual users. Often, these end users are involved in a cyclical manner as the application is being developed. But, at a minimum, one or more end users should test the application once it is fully developed in order to determine its functionality, completeness, accuracy and efficiency. After completion, it is customary to have those end
When financial reporting is in scope, the application needs to address the primary assertions of the account balance, class of transactions or disclosure. Does the application include the appropriate controls related to the primary assertions of the end result account balance or class of transactions? The IT auditor, if applicable, should test the application against the appropriate assertion(s). For instance, if the assertion is accuracy, testing might include things such as:

- Data entry validation controls
- Automatic calculations
- Automatic reconciliations

Existence assertions might be tested for data entry validation controls. Completeness assertions might be tested for job/batch processing controls or reconciliations.

Avoid/Consider Complications

There are a number of complications that are inherently risky and, thus, need consideration during the application audit. First, proprietary (custom-built) applications have a high inherent risk. This fact affects the objectives, planning, controls and risks steps.

If a data warehouse (DW) is involved, there is a relatively high inherent risk. Almost universally, when a DW is initially implemented, data being imported into the DW have a high risk due to, for example, inconsistencies in data (same field with different names), missing data and bad data (i.e., errors). Thus, when data are extracted from the transaction processing systems (TPS), care should be taken in mapping the data and using the ETL (extract, transform and load) process to identify and correct the previously mentioned data anomalies.

For the ongoing DW, data owners could, for example, change field names and add fields, and if change controls are not effective, the data cannot pass through the next ETL process successfully. Thus, change management controls for DW are highly important. The same is true for other similar integration functions.

Some distinction should be made between two types of risk with DWs. First, there is process integrity. This integrity is about whether the processing is successful. Does the application do what it should do regarding its processing function? Second, there is data integrity or data quality, which involves the reliability and integrity of the data being processed, transferred and recorded. Were the data entered valid? Are the source data valid, accurate and complete? Was the data transfer from source to target completed effectively, with no errors?

Avoid/Consider Complications

There are a number of complications that are inherently risky and, thus, need consideration during the application audit. First, proprietary (custom-built) applications have a high inherent risk. This fact affects the objectives, planning, controls and risks steps.

If a data warehouse (DW) is involved, there is a relatively high inherent risk. Almost universally, when a DW is initially implemented, data being imported into the DW have a high risk due to, for example, inconsistencies in data (same field with different names), missing data and bad data (i.e., errors). Thus, when data are extracted from the transaction processing systems (TPS), care should be taken in mapping the data and using the ETL (extract, transform and load) process to identify and correct the previously mentioned data anomalies.

For the ongoing DW, data owners could, for example, change field names and add fields, and if change controls are not effective, the data cannot pass through the next ETL process successfully. Thus, change management controls for DW are highly important. The same is true for other similar integration functions.

Some distinction should be made between two types of risk with DWs. First, there is process integrity. This integrity is about whether the processing is successful. Does the application do what it should do regarding its processing function? Second, there is data integrity or data quality, which involves the reliability and integrity of the data being processed, transferred and recorded. Were the data entered valid? Are the source data valid, accurate and complete? Was the data transfer from source to target completed effectively, with no errors?

Avoid/Consider Complications

There are a number of complications that are inherently risky and, thus, need consideration during the application audit. First, proprietary (custom-built) applications have a high inherent risk. This fact affects the objectives, planning, controls and risks steps.

If a data warehouse (DW) is involved, there is a relatively high inherent risk. Almost universally, when a DW is initially implemented, data being imported into the DW have a high risk due to, for example, inconsistencies in data (same field with different names), missing data and bad data (i.e., errors). Thus, when data are extracted from the transaction processing systems (TPS), care should be taken in mapping the data and using the ETL (extract, transform and load) process to identify and correct the previously mentioned data anomalies.

For the ongoing DW, data owners could, for example, change field names and add fields, and if change controls are not effective, the data cannot pass through the next ETL process successfully. Thus, change management controls for DW are highly important. The same is true for other similar integration functions.

Some distinction should be made between two types of risk with DWs. First, there is process integrity. This integrity is about whether the processing is successful. Does the application do what it should do regarding its processing function? Second, there is data integrity or data quality, which involves the reliability and integrity of the data being processed, transferred and recorded. Were the data entered valid? Are the source data valid, accurate and complete? Was the data transfer from source to target completed effectively, with no errors?
Tests of Controls
Some possible tests of controls include:
• Reconciliation
• Recalculation
• Duplication
• Gaps

An example of reconciliation might be verifying the customer ID in the transaction file against the customer ID in the master file. That is, do the customers in the transaction file actually exist in the authorized customer list? Another example is recalculating where the IT auditor might extend the inventory database to see if the total inventory costs match the control total in the general ledger (i.e., the account balance). Duplicates and gaps are useful in detecting errors in data processing.

CAATs
CAATs could be used to reperform automatic calculations or automatic reconciliations.

Data Mining
Data mining could be used to support the audit objectives. In particular, it is useful in conducting IT-related substantive procedures, such as testing approvals or classification errors related to proper codes.

Purchase Order Thresholds
Any time an application involves a threshold where initial/additional approval is needed, CAATs are useful in determining if that control is operating effectively. For instance, if the application is either purchase orders or disbursements, and if purchases and payments are one-to-one (i.e., disbursements are paid by invoice and not statements), a simple test of extracting all disbursements over the threshold against the data file containing the approval (e.g., purchase order file) would expose any exceptions to the control/threshold. This also has the added benefit of fraud detection if someone is frustrating the threshold deliberately to perpetrate a fraud.

Inventory Anomalies
If the app is recording receipt of inventory, CAATs could be used to show whether the application allows zero or negative quantities to be recorded. Obviously that constitutes an error (anomaly) and, thus, the application would be seen as containing a control deficiency and in need of either a change in the application or a compensating control. There are other applications that could make use of this test.

Second, if the application is a file maintenance program, the system would (hopefully) minimize situations in which an employee could make undocumented changes to the inventory data that lead to discrepancies and data errors. Controls are needed to prevent this anomaly. For example, use of logical SoD could limit employees who can make file maintenance changes. Also, the application/system could track changes by recording data before the change and after the change. Without such tracking, employees could falsify changes and create errors or fraud in the data. Data mining could spot differences in account balances by taking the beginning balance, adding up all transactions and verifying the sum against the ending balance. A similar situation exists for any file maintenance application.

COMPLETE THE REPORT
Obviously all audits end with some kind of report. Those reports are generally proprietary in format. But, they tend to include the audit objectives, tests conducted, results of tests (usually) and recommendations.

CONCLUSION
The successful audit of applications is dependent on a reliable approach. This two-part article demonstrates a reliable approach and some tools that should be helpful in conducting the audit, especially mapping and CAATs.

ADDITIONAL RESOURCES
Five Questions With...

Gregory T. Grocholski, CISA

Greg Grocholski is the chief audit executive for The Dow Chemical Company, based at the company’s global headquarters in Midland, Michigan, USA. He reports directly to the chair of the audit committee of the company’s board of directors. As the leader of the corporate auditing department, Grocholski is responsible for assessing the adequacy of accounting, financial and operating controls for Dow’s global operations. Additionally, he leads the fraud investigative services and contract auditing groups.

Grocholski has 28 years of experience with Dow serving in various capacities and managerial positions, including accounting, information systems, auditing, controllers and most recently as senior director of the finance systems group in corporate controllers. He started his career with Dow in January 1984 as an intern in the accounting department. Soon after, he moved to the information systems group responsible for several data centers’ networks, hardware and software environments. While spending most of his career in Midland, Grocholski spent a few years in Edegem, Belgium, where he led IT and financial audits. After returning to Midland, he was named senior audit manager in 1997 and gradually added more responsibility and new titles over the years. In 2010, he was named corporate auditor.

Grocholski lives by a simple motto: Work hard, play hard, no regrets. As someone with great passion for what he does in his professional life at Dow and in the finance and IT industries, he finds the same passion in his personal life. He loves to travel, cook, read, hike, play all sports (or, as he says, at least try to play all sports), listen to his 15,000-song music library (he enjoys all types of music) and exercise. He and his wife of nearly 28 years are new grandparents—their first grandchild was born in May—adding a new, fun-filled dimension to their lives.

As the 2012–13 ISACA international president, Grocholski looks forward to working with all board and committee members, chapters and volunteers to collectively move ISACA forward in products, literature, educational events and constituent engagement.

Q  As ISACA’s incoming international president and the chief audit executive for The Dow Chemical Company, how do you see ISACA growing and adapting to the constantly changing marketplace and needs of its constituents over the next year?

A  ISACA’s growth will be in correlation to the dynamics of the IT industry and the ability to serve the varied constituents who operate in these ever-changing, complex and global elements. ISACA® must look outside the circle of IT audit and security—as it has done in the past—to further engage those professionals who also have a role to play in implementing secure applications/systems. Two great examples of ISACA adapting to this change are the recent Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) certifications. But, again, ISACA cannot sit still. We also need to attract the next layer of IT professionals who operate around or beyond the traditional assurance, risk, security and governance areas. These areas include privacy and application development professionals, for example. Integrating additional groups such as these will further bind the network and operating layers (risk, security) to the assurance layers (audit and assurance). Of course, this includes the perspective that technology and functionality demands continue to change rapidly, and as such, so must ISACA—staying relevant to the various constituents.

Q  What do you see as the biggest risk being addressed by IT auditors, governance, risk management or security professionals? How can businesses protect themselves?

A  Where do I start? I could talk for hours on each of these risk areas being addressed by IT auditors. Let me select one to discuss here: governance. Literature suggests that not enough attention is being applied to understanding the effects of moving data, functionality, support and security to the cloud. Notice that I did not include the word “responsibility” in the prior sentence? That is because although a business may move activities to the cloud, management needs to ensure that it retains the responsibility (governance) over the activities to ensure that controls are effective and assurance can be placed on the information. IT auditors have to add governance to their skill set to continue to be effective.
Q How do you see cloud computing changing the way we do business? What are your thoughts on auditing cloud computing?

A Cloud computing, as well as the exciting capabilities within it, is a fascinating option available to address new business-model demands and solutions. Given that, I strongly support auditors conducting reviews of activities transitioning to the cloud, because, at the end of the day, the data are still owned by the organization. Auditors should work with vendors to receive SOC reports, but also visit the cloud provider to assess capabilities, observe metrics and processes, and test controls, when appropriate.

Q How do you believe the certifications you’ve attained have advanced or enhanced your career? What certifications do you look for when hiring new members of your team?

A Without a doubt certifications help enhance (and advance) a person’s career and profession. Staying relevant, current and adaptable to the changing regulations and technologies further supports the need to be certified (assisted by continuing education credits). My peers and I certainly look for certified professionals when hiring, as it demonstrates that the person has achieved some degree of industry acumen. It is not the ultimate factor in hiring decisions, but it certainly helps. And, we would look to those hired who may not be certified to pursue certification within a short period of time. Certifications are valued and I encourage IT professionals to pursue relevant certification.

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

A There have been many, many challenges in my career, but one of them occurred early on. I always believed in my “technical” finance and IT skills to help me through a lot of my early projects and assignments. But, I quickly learned that I needed to equally develop the soft-skills areas—such as oral and written communications, executive presence, delivering tough messages, interpreting IT jargon to non-IT professionals to ensure risk was clearly understood, and being able to look around the corner to anticipate what else could happen given the possible existence of project deviations or variances. Developing both technical and soft skills requires attention and focus; for me, it has been a career-long and lifelong exercise. Learning and applying new skill sets never ends!

Don’t get lost in your quest for a job.

Simplify your search with ISACA’s newly enhanced online Career Centre.

Explore the ISACA Career Centre today:
www.isaca.org/careercentre-journal
The IBM Data Governance Unified Process: Driving Business Value With IBM Software and Best Practices

The importance of treating information as a key enterprise asset cannot be overemphasized in today’s corporate world. Data governance is the discipline of treating data as an enterprise asset. The benefits of treating data as an enterprise asset through disciplined data governance are many; however, enterprises also face numerous challenges in implementing proper governance over corporate data.

The IBM Data Governance Unified Process: Driving Business Value With IBM Software and Best Practices is a reference guide that provides practical steps to implement an information governance program as well as the associated tools provided by IBM software. The book is mainly targeted at data governance practitioners and draws on real-life experiences of enterprises that have implemented data governance programs.

The author leverages his data governance experience across different industries to bring out a practical guide that anyone with interest in data governance will find useful.

The book comprises 18 chapters that detail the IBM Data Governance Unified Process. Chapter 1 introduces the reader to data governance, including the key benefits that can be derived from governing data. Chapter 2 introduces the IBM Data Governance Unified Process. The author explains that 11 of these steps are required for all data governance programs. Three of the steps within the process are optional, depending on the data governance track on which the enterprise needs to focus.

The rest of the book details each of the steps involved in the IBM Data Governance Unified Process. The process begins with defining the business problem. The author emphasizes that the reason why most data governance programs fail is that they fail to identify a tangible business problem. One key step that is outlined is the performance of a data governance maturity assessment. This is important for an enterprise to build a road map to bridge the gap between current and desired states. The book provides a sample data governance charter as well as a sample data governance maturity assessment questionnaire.

The book’s key strengths are the use of real-life examples and the detailed explanation of each of the steps involved in the IBM process. While one of the aims of this book is to recommend IBM technology for data governance initiatives, this does not in any way demean the value of the book. The author recognizes that the core issues are about the process, which can be applied even if an enterprise chooses to use other software tools to implement data governance.

**EDITOR’S NOTE**

The IBM Data Governance Unified Process: Driving Business Value With IBM Software and Best Practices 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.
Everybody Loves Documentation

When IT professionals think about documentation, they tend to see folders of dry templates and stacks of binders that no one reads. Contrary to this image, documentation is far more than just piles of meeting notes, source code and diagrams. When done right, documentation is, in fact, a process that brings many compelling advantages to IT departments, including effective risk mitigation.

Documentation enables organizations to mitigate their risk across several strategic areas, including loss of intellectual capital, data and IT operations, clarity, and momentum.

INTTELLECTUAL CAPITAL
IT departments, by their nature, face tremendous risk associated with the loss of information locked inside the heads of their employees and contractors. In today’s market, this risk is intensifying as IT professionals change jobs more frequently and as layoff and retirement rates increase.

Documentation mitigates risk by helping organizations with succession planning through capturing intellectual capital. Organizations need to take a deliberate and consistent approach to capturing the knowledge of their people, through documenting job functions and technical knowledge of systems and infrastructure.

Without an effective approach to documentation, IT departments put themselves at an increasingly higher risk of losing data and functionality, resulting in considerable rework. This rework comes at an unbudgeted cost of resources, and a direct loss of productivity and profitability. Some information may even be impossible to reproduce and, if the information is critical, may cause severe damage to the organization.

DATA AND IT OPERATIONS
Documentation is essential for business recovery planning and mitigates the loss of data and the disruption of IT operations. To safeguard data effectively, IT departments must document how backups are run, where the backups are located, and the results of regular tests of backup and restore operations.

Documentation is essential for ensuring that, in the event of disaster, IT departments understand and are able to restore every aspect of their infrastructure, including computers, networks, operating systems and applications. Furthermore, the documentation of repeatable IT processes ensures that IT departments can maintain continued operations following a disruption or disaster.

CLARITY
Documentation mitigates the risk associated with miscommunication by forcing professionals to spell out exactly what they are thinking. Relying blindly on verbal discussions does not ensure that IT professionals or their team members understand each other, no matter how much the IT professional may want to believe that everyone is “on the same page.”

Only documentation can provide a certain point of reference to effectively articulate the subject matter, ideas and action items. Documentation provides clear rules and conditions that protect organizations in situations in which there are disagreements or misunderstandings with employees or third parties. Such situations include legal protection for disciplinary action against employees who breach the acceptable-use policy or the ability to resolve disputes with third-party outsourcers through defined service level agreements.

MOMENTUM
While documentation is commonly seen as a nuisance on IT projects, this perception could not be further from the truth. Documentation brings trust that enables IT departments to make decisions and, in doing so, also brings momentum that pushes the project, department and organization forward.

Project update documentation mitigates the risk of delays by providing IT departments with...
early warning signs when teams have missed or are about to miss deadlines, and enables them to bring projects back on track more quickly. Documentation can also improve momentum for operations through improved clarity and accountability over job functions, processes and controls.

THE REPERFORMANCE STANDARD
One of the key challenges that IT departments face in developing and maintaining excellent documentation is that they do not have a consistent standard for assessment. In reality, there are many types of, and uses for, documentation, and using one consistent standard is difficult. There is, however, one standard that provides a strong metric for most documentation within IT departments: the reperformance standard. This states that the documentation must enable a user to reperform the related task or process; that is, the documentation must have sufficient detail and communicate with enough clarity through its text or visuals to allow the user to execute the steps. Although more commonly used by assurance and audit professionals, the reperformance standard can be expanded to many other applications within IT departments, including training materials, user manuals, process documentation and disaster recovery documentation.

FIVE LEVELS OF DOCUMENTATION
So, where are IT departments with their documentation? There appear to be five distinct buckets into which IT departments tend to fall:
1. No documentation
2. Little and sporadic documentation
3. Average documentation
4. Optimized documentation
5. Overdocumentation

For IT departments in buckets 1 and 2, there is no culture of documenting processes, and records taken during meetings and testing are very weak. IT departments that fall in the average bucket (3) tend to document the important processes but do not recognize the strategic benefits of expanding their process. Bucket 4 is where IT departments should aspire to be. At this level, management regularly reviews and rewards strong documentation, there are established practices around effective documentation, and the reperformance standard is consistently met. The last bucket, overdocumentation, is common in environments in which there is fear of failing regulatory requirements, such as the US Sarbanes-Oxley Act, or in environments in which there is little understanding or ability to write clearly and succinctly.

One of the most significant risks is when organizations believe that they are in bucket 4 but really fall in bucket 1 or 2. This is a common problem with companies that take a checklist approach to documentation and believe that just having documentation is enough for risk mitigation—when, in fact, their documentation neither addresses the objectives of the organization nor meets the reperformance standard. Bucket 5, although less common, can also be dangerous, as the organization has a false sense of security in its documentation process, while the true objectives are not being met.

COMMON ISSUES
Most IT departments today fall short of reaching the optimized bucket for three main reasons. First, IT departments do not recognize the many advantages of documentation in helping with risk mitigation, as well as the many competitive advantages (i.e., improved clarity, trust and momentum). IT departments need to recognize that lack of documentation exposes the business to additional risk and should be highlighted during an enterprise risk management or business continuity exercise.

Second, IT departments are frequently stuck in the getting-things-done mode and never slow down to perform effective documentation. They often do not stop to evaluate the hidden costs and impacts that their decisions can have
on the organization and, therefore, do not include effective documentation practices in their projects and operations. It is often too late to gain value from documentation when documentation is created after the fact, as ideas are forgotten, projects are disbanded, and consultants and employees have left the organization.

Third, IT departments do not know how to document. Documentation does not mean writing everything down. It is actually a strategic process that consists of capturing, structuring, presenting, communicating and storing written information. While IT professionals generally understand how to capture and store information, they tend to struggle on structuring, presenting and communicating. IT professionals must be able to take unstructured information, weed out the unimportant parts, and turn the remainder into usable material that engages stakeholders and communicates the content effectively. Effective documentation demands a comprehensive set of skills that include technical writing, visualization, formatting and the ability to structure information into a cohesive package.

GETTING OPTIMIZED
Moving the team and department to the optimized documentation bucket is a three-step process:

1. The organization must adopt a strategic process for documentation. This demands that management, project managers, technical writers and technical staff all understand and engage in the process. This step requires prioritization based on risk and opportunity, as not every process, department and team require the same level of attention.

2. The organization needs to have the right people. The resources required for effective documentation are not necessarily the same for every assignment, and the appropriate professionals may come from a variety of backgrounds including technical writing, project communications, business analysis, quality assurance and audit. The organization needs team members who not only have the competence for documentation, but who also understand and appreciate its value.

3. The organization needs to build a culture of accountability and best practices around effective documentation. This culture must stem from senior management and trickle down throughout IT operations. A culture of accountability requires regular audits of operational and project documentation and a system for rewarding staff who maintain strong documentation practices.

CONCLUSION
Documentation is essential for IT departments to achieve their objectives: protecting their intellectual capital and business continuity, and improving clarity and momentum in projects and operations. Unfortunately, IT professionals often overlook documentation as a critical tool. They fail to understand the many advantages of effective documentation and the risk of ineffective documentation. IT departments cannot rely on a checklist approach to performing or assessing their documentation; they must use the reperformance standard to ensure that the documentation meets the needs of the organization.

Moving documentation to the optimized level does not come overnight, but adopting a strong process, engaging the right people and building an accountable culture around documentation will take the IT department forward significantly. Documentation at the optimized level is more than just good practice; it is a strategic advantage for the team, IT department and organization as a whole.

ENDNOTES
2 Ibid.
The Importance of the ARA

Chief audit executives (CAEs) cannot forget the importance of the audit risk assessment (ARA). The basics of internal auditing always start with the assessment of audit risk. This is the foundation for the audit work plan and the deployment of resources for the year. However, in these difficult economic times, many audit departments have become reactive and have difficulty seeing the entire picture. Additionally, many audit departments become complacent and routine oriented. Internal audit (IA) departments should not lose sight of the importance of the ARA and its tangible and intangible benefits to the company and the department.

THE IIA STANDARDS ON THE ARA AND RELATED INTERPRETATIONS

The Institute of Internal Auditors (The IIA) standards are what guide IA departments on basic principles. As outlined here, the standards are explicit as to the importance of the audit risk assessment:

• **2000 Managing the Internal Audit Activity**—The CAE must effectively manage the internal audit activity to ensure it adds value to the organization.
• **2010 Planning**—The CAE must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals.
  – Interpretation: The CAE is responsible for developing a risk-based plan. The CAE takes into account the organization’s risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, CAEs use their own judgment of risk after consultation with senior management and the board.
  – **2010.A1**—The internal audit activity’s plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.
  – **2010.A2**—The CAE must identify and consider the expectations of senior management, the board and other stakeholders for internal audit opinions and other conclusions.
• **2020 Communication and Approval**—The CAE must communicate the internal audit activity’s plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The CAE must also communicate the impact of resource limitations.
• **2030 Resource Management**—The CAE must ensure that internal audit resources are appropriate, sufficient and effectively deployed to achieve the approved plan. As noted in the extracts from The IIA standards, audit departments are required to perform an audit risk assessment annually. The risk-based priorities must be consistent with the organization’s goals, which many CAEs tend to overlook at times. Although internal audit is an objective and independent body, it wants to improve the organization through a risk-based conscience.

As outlined in the standard interpretation, the audit risk assessment is guided by the risk appetite of management and the audit committee. This process is very similar to the enterprise risk assessment (ERA), which is the assessment of risk for the enterprise risk management (ERM) process.

ERM is defined as a process “affected by an entity’s board of directors, management and other personnel; applied in strategy setting and across the enterprise; and designed to identify potential events that may affect the entity and manage risks to be within its risk appetite and to provide reasonable assurance regarding the achievement of entity objectives.” Accordingly, internal audit typically does not own the ERM process, but can be integrally involved. Internal audit can assist management and the board/audit committee in the process by:

• Monitoring
Examining
• Recommending improvements
• Evaluating
• Reporting

Additionally, internal audit can provide key assistance in the assessment of enterprise risk, as the process of interviewing/questionnaires, compiling results and ranking risk is similar to the ARA. The focus of each is slightly different; the ERA takes a more holistic view of the risk for the entire organization, while the ARA is focused more on risk that is auditable. For example, the ERA focuses on risk areas that could hinder the overall success of the organization. Many areas of risk are not auditable. On the other hand, risk that is auditable should be addressed in the ARA. However, IA involvement in each risk assessment process can be extremely beneficial. Some of the underlying benefits to IA of conducting risk assessments include:
• Increasing exposure to varying levels of management
• Continuing to build rapport and trust with management
• Providing true value to the organization via a detailed understanding of what the significant risk is to the organization and key unwritten and, possibly, undocumented issues
• Refocusing energies on risk and objectives key to management, meeting the organization’s goals and objectives

LOST VALUE: RISK OF NOT PERFORMING THE ARA

Those internal audit shops that do not value the formal assessment of risk on an annual basis omit the impact and significant exposure that not performing an ARA may bring to management. In many instances, this might be the most in-depth conversation IA will have with some key personnel throughout the year. Additionally, the more people are engaged with IA, the greater the chance of building a trustworthy relationship. Without trust, IA will have a significantly more difficult time penetrating the proverbial wall between management and IA and building a strong advisory role inside the organization. To truly provide value inside an organization, IA needs to have a strong rapport with management. An audit department that is valued and trusted inside an organization is more likely to receive incoming calls to assist departments, as needed. This cannot happen without the face time involved in the risk assessment process.

Shelby Faubion, a CAE of a global defense services provider, said, “As a service function within an organization, IA must market its services with its customers as any service provider, internal or external. Its customers must understand the nature of services offered and the value they receive for their effort. To remain relevant, IA departments should establish and deliberately execute customer relationship management plans with accountability clearly defined. If a CAE only has contact with his/her business leaders annually, the CAE probably does not really know what is going on with the business. Many organizations today are rethinking their strategies and are looking to enter new markets, which poses new risk to their organizations. Businesses that are to survive and thrive in the current marketplace are likely seeing significant shifts in strategy.”

Without performing a risk assessment, IA is at risk of losing its relevance. Whether the organization is seeking to enter new markets, leverage new technologies (e.g., social media, cloud) or expand its business portfolio organically or inorganically, IA has a role in helping the organization understand and prepare for the associated risk implications. Ultimately, if IA cannot effectively articulate how its work relates to the company’s goals and strategic objectives, it may indeed have lost its relevance to the company.

Finally, many internal audit departments get stuck in an extended audit cycle. The audit cycle can be very long and arduous and, in many respects, never ending, even after...
audit follow-up. To be a true advisor to the organization, continuous monitoring and recommendations are critical. On the other hand, it is easy to get caught up in this never-ending audit cycle. When audit departments are busy throughout the majority of the year, the fourth quarter rolls around and there are too many audits to get through to complete the ARA. As a result, by the time year-end comes around, the ARA process is internalized and reproduced from the prior year.

However, performing a more formal ARA helps audit refocus its efforts on the true risk areas and goals of the organization. Understanding risk, with consensus from all parties as to the risk exposure reported, helps the audit activity understand the point of view of management and how best to assist the organization.

COMBATTING THE ENDLESS CYCLE OF THE AUDIT PLAN

Many internal auditors do not perform the annual risk assessment because there is an innate belief that there is little overall control of the audit schedule. Shops tend to reproduce the work from the prior year or budget hours based on man-hours available rather than actual risk to the organization. Additionally, it is not the audit department’s responsibility to budget to man-hours rather than organizational risk. Audit’s role is to outline the risk and exposure to the organization and allow the audit committee to determine whether additional resources are necessary. If audit budgets are based only on man-hours available, the audit committee will never fully understand the risk to the organization and the risk areas not addressed.

One way to assist audit departments in alleviating this stress at year-end is to establish ample amounts of audit flex time in addition to creating an audit plan based on risk to the organization. Flex time is the part of the audit schedule that is grayed out and establishes flexibility in the audit plan. The audit department should identify specific audits to conduct if the schedule does not change, but most organizations find that the schedule always changes. For example, fraud investigations are difficult to plan for, and there are special request audits that cause changes to the original plan.

Finally, 2010.A of The IIA standards states that risk must be assessed at least annually. However, in today’s current depressed economy, is it sufficient to assess risk only annually? Many organizations have evolved to more of a continuous risk assessment, in which audit activities identify and evaluate companywide risk levels by examining trends and comparisons within a single process or system throughout the year. An example of this is when results are compared to their past performance and other business systems. Ongoing trending of business and compliance metrics (including profit margin, earnings before interest and taxes [EBIT], win rate, open positions, days sales outstanding, hotline complaints) can help to identify problems in their early stages, according to Faubion. Used by IA as a tool, an ongoing risk assessment can help IA proactively respond to risk indicators and, in turn, help the company minimize exposure. In summary, risk assessment is a valuable tool to proactively leverage risk indicators to prioritize a company’s limited IA resources.

In practical terms, IA will utilize computer-assisted audit techniques (CAAT) (regardless of sophistication) to monitor risk. This would entail monitoring key indicators/ratios that could change the risk profile of the organization, which, in turn, would alter the ARA and the audit plan. Having sufficient audit flex time in the audit plan will give the department flexibility to alter its plan in an efficient and effective manner.

CONCLUSION

Internal auditors should not underestimate the importance of the internal ARA and completion of the formal process at least annually. The exposure and relationship development opportunities with management are endless and, in these times of consistent financial pressure, staying on top of key organizational risk areas and goals is one of the most important steps that continue to add value. Regardless of the benefits, performance of the ARA at least annually assists audit in right-sizing expectations and refocuses the department on the goals and objectives of the organization.

ENDNOTES

2 Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management—Integrated Framework, 2004
Seven Myths of Information Governance

The term “governance” has different interpretations depending on the perspective of the user. In mechanical engineering, the term “governor” conveys the presence of a feedback device on a machine (system) that is used to provide automatic control of, for example, speed, pressure or temperature. As defined by ISACA, governance ensures that “stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.”

In essence, the role of governance is to empower the principal to monitor and control the behavior of the agent. For example, in corporate governance, the principal—particularly the shareholder—is represented by the board of directors, which is charged with the duty of oversight over management. The purpose of corporate governance is to persuade, induce, compel and otherwise motivate corporate managers to keep the promises they make to investors. In addition to these high-level meanings assigned to governance, the notion of governance can also be discussed from the viewpoint of firm characteristics (e.g., public vs. private companies, large vs. small companies, partnerships), sector (e.g., hospitals, government, cooperatives, nonprofit entities) or stakeholder orientation (e.g., shareholders, customers, employees, the public).3

Interestingly, governance is also used to convey the monitoring and control of different intraorganizational domains of an entity. When used in this sense, governance suggests a subset of entity-level governance. For example, the overall governance of an entity encompasses information governance—monitoring and control of data capture, data storage and creation, and distribution and use of information. Information governance, in turn, includes data governance.4

When a major technological innovation becomes a key driver of the economy, the innovation could take on its own governance angle, e.g., governance of cloud computing. Thus, the variety and shades of governance perspectives could be confusing and counterproductive if, at the outset, it is not clear which part of the governance schema is the reference point for the discussion. In this article, the term “governance” is used in the sense of information governance to discuss certain myths or misunderstandings of governance.

FOCUSES OF GOVERNANCE: RESOURCES AND PROCESSES AND BUSINESS VALUE

The Committee of Sponsoring Organizations of the Treadway Commission defines “enterprise risk management” (ERM) as follows:

Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The notion of governance entails the monitoring of ERM, which is strategic in nature, is driven by processes and aims at the achievement of intended objectives. Thus, governance involves guiding and steering the process so that the process remains in control and continues to deliver desired results in terms of business value (BV). A process “remaining in control” and “delivering desired results” are two related, but distinct, focuses of governance. The resources and processes focus refers to controlling risk of processes and resources; the BV focus involves monitoring decisions to create BV. Although notionally separate, the two focuses influence each other because every initiative to deliver BV is likely to be accompanied by additional risk that may warrant additional controls. For example, a business acquisition...
possibly adds BV while also adding to the need to control the resources and processes of the larger entity.

In the arena of information governance, the resources and processes focus suggests the need to control information resources and processes to mitigate their risk exposures and achieve systems performance goals. This focus ensures that IT resources and processes and their performance and risk management are addressed. Often, this is achieved through cost budgets. Concurrently, the BV focus centers on control of the system behavior so that expected information outcomes are delivered to the users. The resources and processes focus centers on processes that create information, and the BV focus centers on processes that use information to generate BV.

The accountability for IT resources and processes is easier to identify and evaluate than the accountability for the creation of BV. BV emerges throughout the organization, and while IT may be a facilitator in doing so, it may not be the sole or dominant actor. BV from IT investments cannot be realized by IT, but will always be created on the business side,

The two focuses overlap and impact one another. Take, for example, a decision to outsource some IT services to a cloud computing environment. This decision may result in cost reduction, which, in turn, improves operating profits—a measure of BV. However, the decision also leads to new risk that needs to be assessed and mitigated. The decision also impacts the risk of resources and processes that create information. Although the underlying decision involves both focuses, knowing the difference between the roles of the two and providing requisite variety to control each are critical in effectively addressing information governance issues.

Every move on the part of an organization comes with risk and opportunities, and both must be managed.

Use of the term “information governance” in a broad sense often leaves out or implicitly assumes the focal point. Is the focus on controlling resources and processes that create information, or is it on those resources and processes that use information outputs to create BV? Although the treatment of each focus is best done in somewhat separate ways, there has to be clarity on the two focuses of governance, how each is achieved and where the two converge. Within this context, this article discusses certain misconceptions of information governance; illustrates key points; and, where possible, suggests ways to overcome such misconceptions. Of these, the first four myths presented clearly point to a weak distinction between the two focuses of information governance—resources and processes, and BV.

MYTH 1: RISK IS SEPARATE FROM OPPORTUNITIES

Every move on the part of an organization comes with risk and opportunities, and both must be managed. While there is temptation to leverage an opportunity, it should not be entertained without regard to the landscape of risk that the business decision will change. Thus, risk is not separate from opportunities, and considering one and leaving out the other is not an option. Where a firm’s emphasis is in favor of opportunity and against risk, the positioning of the chief risk officer (CRO) is ineffective because risk management is not valued as an equal discipline to opportunity pursuit.

Often, problems arise from thinking that the governance of risk related to resources and processes is unrelated to the...
governance of BV (BV focus). Decisions about risk management are in tandem with decisions about exploiting opportunities to improve substantive performance. Addressing risk, for example, from outsourcing to cloud services may be seen as a process evaluation, whereas exploiting the opportunity may be gauged in terms of the present value of cost savings from outsourcing. In terms of accountability, risk could fall in one area (e.g., the chief information officer) and financial performance management in another (e.g., the chief financial officer). Thus, the burden of taking on a new opportunity could fall exclusively in one area and potential benefits may be credited to another. While there may be a general understanding that risk and rewards come together, in reality, accountability for each may be segregated and may never get reconciled on the same page.

The frameworks that provide structure to information governance are COBIT and Val IT.10 Roughly, COBIT leans toward the resources and processes focus and Val IT leans toward the BV focus. Whereas each framework supports the unique needs of each governance perspective, there must be an effective, sustained alignment between the two. Several measures can be taken to meet this end. For example, business key performance indicators (KPIs) can be mapped to IT KPIs and an appropriate set of balanced scorecards (BSCs) can be developed to link business and IT KPIs.11, 12 Whereas these steps will likely help, a systematic development of a comprehensive “bridge” between COBIT 4.1 and Val IT can provide the greatest benefit, as seen in COBIT 5. Such a bridge can offer a common ground to both creators and actors of information in which the accountability for alignment is shared by both groups.

**MYTH 2: GOVERNANCE IS A DESTINATION**

As discussed previously, governance warrants monitoring the risk and opportunity sides of every event, current or proposed, in light of the intended objectives. It is not a one-time event; it is a journey. Related to the resources and processes focus, continual evaluation of the control framework and, where necessary, appropriate corrective actions may not occur, leaving new areas of risk unmitigated and keeping in force controls that address risk that no longer matters to the organization. On the BV focus, continual innovation in business strategy and value creation is imperative; it is also not a one-time event.

In part, this sort of impression—that governance is a destination—could result from the perception that controls, once designed, continue to effectively serve the risk mitigation objective and, therefore, the only thing that needs to be cared for on an ongoing basis is the creation of BV, not mitigation of risk. It is likely that those in charge of information governance are not convinced that continual evaluation and realignment of the control framework that serves the resources and processes focus can be cost-effective. Once the framework is in place, they may see comfort in what already exists. If so, it would be necessary to discourage the mind-set that what exists does not require a second look, especially when the company makes major operational, tactical or strategic changes on the business side to impact future outcomes. For example, if a company decides to lay off several hundred employees, it will likely improve the bottom-line financial performance; however, this will also raise questions of potential gaps in process controls created by the departure of people in key positions.

In fact, compliance initiatives never really end. To ensure continuous compliance, a model such as Deming’s Plan-Do-Check-Act cycle should work well.13

**MYTH 3: REGULATORY COMPLIANCE IS THE KEY OUTCOME**

Regulations and laws have a place in society and business. Without legal requirements, it is difficult to ensure that a company does all that is necessary. Consequently, much credit is given to the US Sarbanes-Oxley Act and Europe’s Basel II for requiring corporations to meet threshold governance requirements.

Thus, regulatory compliance with enacted governance standards has become an overwhelming force. Just recently, some members of the US Congress have encouraged the US Securities and Exchange Commission (SEC) to require companies to disclose incidences of data breaches and related facts about their information systems.14 Additional burdens of monitoring and disclosure requirements could cause the governing authorities, such as the board of directors, to feel that meeting the letter of the law is sufficient. “An often-mentioned myth or misunderstanding is that better governance...will take too much time or cost too much. This is typically mentioned by people who think that ‘governance’...
means only dead-weight compliance.” The perception that may further reinforce this behavior is that there are no tangible benefits, just costs, of doing more. Consequently, organizations may not subscribe to additional governance measures as value-added initiatives.

However, first and foremost, governance is supposed to benefit the owner entity. Hence, to stop at the door of compliance and do nothing more with it is a disappointing state. For example, the SEC has recently mandated that public companies must use Extensible Markup Language (XML)-based Extensible Business Reporting Language (XBRL) tags to meet the agency’s filing requirements. Companies can do this in two ways: by “bolting on” the tags to the final filing papers or by embedding the tags throughout the general ledger of the company. The latter option potentially benefits the company in that the tagged data could be used by management for efficient and effective decision making. Often, instead of considering this avenue in which lasting benefits could occur to the company, most filers are likely to use the shortcut of bolting on the tags. The result is that the benefit of using the tags to track transactions (e.g., to prepare internal reports to compare plans with actual performance) is not chosen; only the regulatory compliance requirement is met.

Regulations related to risk management and related disclosures set the minimum across-the-board generalized requirements. Where good governance exists, meeting legal requirements is likely to be the least concern. If anything, compliance in such cases would have an ancillary effect rather than a primary outcome.

Finally, regulatory compliance, by itself, may project only the resources and processes focus, which is not enough to execute the company’s business strategy. The BV focus is an integral aspect of information governance.

To address this myth, business and IT leaders should emphasize a customized approach to meeting these requirements within their firms, producing synergy well beyond the regulatory threshold. This is why tone at the top—including consistency among statements, assertions, and explanations of management and its actions—is vital to effective governance.

**MYTH 4: GOVERNANCE IS SEPARATE FROM BUSINESS PERFORMANCE**

This myth is a corollary to the first myth. From within an organization, one may look predominantly from the viewpoint of mitigating risk related to resources and processes. However, the delivery of BV through management’s actions, the BV focus, is also integral part of governance. Is it likely that management places a disproportionate weight on the resources and processes focus at the cost of the BV focus? Because monetary revenue is often not the focus of information systems management, governance of risk is often considered a role in which accountability of costs matters, not revenues or profits. On the other hand, governance of opportunities is often seen as a revenue, profit or investment center. These perspectives often cause different reactions because cost control is predominantly centered on a budget rather than a strategic plan.

The dichotomy—resources and processes vs. BV—may cause one to perceive the governance of risk as a domain logically separate from the governance of opportunities. Tensions between the two focuses may heighten the challenge of keeping the two in alignment. For example, outsourcing some of the transaction processing systems to an offshore vendor could be an opportunity for huge cost savings annually. As management considers this an attractive option to lower costs and improve profits, it should also tackle related issues present in the governance of risk. For example, who owns client data, how secure are these data and what happens if in the future the client company wants to exit the outsourcing arrangement? Clearly, the governance of risk is not separate from the governance of opportunities, although it may appear so in some instances in which the issue is almost exclusively either of risk management related to resources and processes (with the creators of information) or of opportunity leverage (with the actors of information).

Regardless of the impact on either type of governance, a careful evaluation of both should be undertaken jointly by the managers responsible for the areas of risk and for opportunities. The guidance suggested in the first myth also applies here. Moreover, the Responsible, Accountable, Consulted and/or Informed (RACI) chart recommended and illustrated in the COBIT framework is an effective integrating mechanism to overcome this misunderstanding. COBIT 5 articulates how enterprise goals that signify business value cascade into IT-related goals targeted to mitigate resources and processes risk areas.
**MYTH 5: GOVERNANCE IS AN ALL-OR-NOTHING PROPOSITION**

Looking at elaborate frameworks such as COBIT, one may be impressed and puzzled at the same time. COBIT is a powerful framework that cannot be brought to its full potential within a short period of time. It will take a prolonged period of time to set the framework right. Such a challenge may tempt some people to quit altogether because the task of implementing the framework looks imposing. On the other hand, any controls that may be in place in the absence of the rigor of a control framework may be random, deficient in design or operation, and collectively spotty. To identify and fill the voids, the use of a control framework is essential. To abandon the adoption of a control framework would be counterproductive in the long run. Even if the benefit of a control framework is in doubt, publicly traded companies in the US are subject to legal requirements to implement an appropriate framework for internal controls related to their financial systems.

Whereas a control framework is a crucial requirement for disciplined risk management, it may not be necessary to work through every objective of each domain concurrently. As long as a broad map is drawn and the overall view is clear, it would be appropriate to address first those objectives in which a serious lack of control effectiveness exists. Once risk exposures are rated and prioritized, it becomes feasible to prioritize action items. This is much like deploying a divide-and-conquer approach that allows for a step-by-step implementation of controls and that, over time, leads to the implementation of almost an entire control framework. Local initiatives to identify and address control objectives also reinforce a culture in which risk management is everybody’s business, not just the CRO’s. While a top-down approach to plan for an implementation of a control framework is almost a requirement, the implementation sequence of specific control initiatives may not follow this path. As long as pieces of the puzzle are determined, it could be appropriate, and effective, to fit the identified and prioritized piece within the puzzle.

To address this negative bias toward information governance frameworks, a program of pilot projects can be used. Executing a pilot project to achieve compliance within a small team, system or area can provide reassurance over the approach, serve as an example for other teams and help dodge associated pitfalls before a framework is implemented organizationwide.21

**MYTH 6: GOOD GOVERNANCE WARRANTS NEW TECHNOLOGY**

The pace at which technology advances is so impressive that access to new technology is an imperative for organizations. New technology also creates significant comparative advantages in terms of green initiatives, energy savings, productivity improvements and better security. Moreover, technology vendors may, after some time, not support prior versions, and incompatibility between recently acquired technology and existing infrastructure may begin to frustrate both systems and management professionals. For these and similar reasons, adopting new technology may be an attractive option. In summary, as often prescribed, technology is there for business reasons, not for its own sake. The justification to adopt a new technology should come from its BV to the firm. Making the case for the adoption of a new technology purely from the vantage point of the resources and processes focus is likely to be less successful than from that of the BV focus.

For effective governance, the adoption of a new technology is likely, but it is not imperative. Generally, if the mitigation of a particular exposure can be achieved cost-effectively using a new technology that fits the current technology in use, the new technology’s adoption can be supported. Clearly, effective governance is not a product of new technology, although it may facilitate or improve governance. If a technology that is vastly different from what exists within the firm is adopted, the governance of risk is likely to pose a bigger challenge.

"Good governance cannot happen without allocating resources."

**MYTH 7: GOOD GOVERNANCE REQUIRES SEPARATE FUNDING**

Good governance cannot happen without allocating resources; however, the assumption that each governance measure must be supported by separate funding is misleading. In fact, management, using the BV focus, often thinks about what is needed to leverage an identified opportunity; the mitigation of risk emerging from such an action is considered a subset of the same action, not a separate action. Therefore, the expenditure budget for the governance of risk may not change materially every time a new opportunity is exploited by the organization.

A side effect of this management behavior could be that new risk stemming from management decisions is not noticed and, therefore, is not addressed. This may happen
regardless of whether such risk will require additional funding to manage it. One way to force the discovery of risk-related issues and how they will be addressed is to include within the BV justification process a specific question that pertains to the potential impact of the decision on risk related to resources and processes.

CONCLUSION
A clear comprehension of the two focuses of governance—resources and processes that generate information and BV—is a key prerequisite for addressing information governance at any level within a firm. Without understanding the distinction between the two, debates will ensue and different paths will be taken because of unstated assumptions about whether one is looking at risk related to resources and processes or risk related to opportunities (BV). ISACA’s recently released COBIT 5 integrates the two focuses into a single view, thus facilitating and simplifying the governance of enterprise IT (GEIT) in a unified manner.

Several myths, or misconceptions, persist because of oversight of this dichotomy and other similar concepts working behind the governance scene. This article outlined seven such myths and, where possible, suggested ways to counter such perceptions. The ERM plans of a firm can become ineffective because of misperceptions or biases, and these should be challenged and removed through systematic communication and orientation so that any drag on the organization’s governance initiative is minimized, if not eliminated.
Haris Hamidovic, CIA, ISMS IA, ITIL, IT Project+, is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the North American Treaty Organization-led Stabilization Force in Bosnia and Herzegovina. He is the author of five books and more than 70 articles for business and IT-related publications. Hamidovic is a certified IT expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina and the Federal Ministry of Physical Planning of Bosnia and Herzegovina. He is a doctoral candidate in critical information infrastructure protection at the Dzemal Bijedic University in Mostar, Bosnia and Herzegovina.

How to Maximize Evidential Weight of Electronically Stored Information Recommendations of BS 10008

Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation’s security and economic well-being. Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of information and communications technologies (ICTs) for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.1

Apart from substantive criminal law provisions, law enforcement agencies need the necessary tools and instruments to investigate cybercrime. Such investigations present a number of challenges. Perpetrators can act from nearly any location in the world and take measures to mask their identity. The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.2 Furthermore, as stated by Jerker Danielsson and Ingvar Tjøstheim:

In many jurisdictions, it is unclear to organizations which requirements and constraints the legislation sets on collection and preservation of potential digital evidence. Often it’s also unclear how the responsibility is shared between law enforcement organizations and organizations affected by criminal activity leaving digital traces. It can be argued that organizations have to take a greater responsibility in the cyber-world than they currently do in the physical world. This is due to the complexity of the environment and consequently the complexity of investigations of crimes in this environment. Law enforcement needs support in getting an overview of affected systems. Additionally, law enforcement can only collect evidence post mortem and is consequently dependent on the fact that organizations affected by crime have collected and preserved potential digital evidence in a way that guarantees that it is authentic, accurate and complete.3

In most jurisdictions and organizations, digital evidence is governed by three fundamental principles: relevance, reliability and sufficiency. These three principles are important for the digital evidence to be admissible in a court of law, as stated in ISO/IEC DIS 27037. Digital evidence is relevant when it goes toward proving or disproving an element of the specific case being investigated. The meaning of reliability varies between jurisdictions; however, a general principle of it is to ensure that the digital evidence is what it purports to be and has not been spoiled. The concept of sufficiency means that digital investigators need only to collect enough evidence to prove or disprove the elements of the matter (ensuring that no exculpatory material has been overlooked).4

There has been much discussion about the value of information stored electronically when required as evidence in a court of law or for other purposes. British Standard BS 10008 specifies the requirements for the implementation and operation of electronic information management systems, where the issues of authenticity, integrity and availability, as required by legal admissibility and evidential weight, are important.5 This article introduces the basic recommendations, based on BS 10008, for improving the reliability of, and confidence in, electronically stored information.

PRINCIPLES OF GOOD PRACTICE FOR INFORMATION MANAGEMENT

Code of Practice for the Implementation of BS 10008 is structured according to a set of five principles of good practice, which are defined...
The principles of good practice for information management. The five principles (figure 1), as defined in PD 0010, are:

1. Recognize and understand all types of information.
2. Understand the legal issues and execute duty-of-care responsibilities.
3. Identify and specify business processes and procedures.
4. Identify enabling technologies to support business processes and procedures.
5. Monitor and audit business processes and procedures.

“The ordering of the five principles also reflects a cascade from the high-level classification of information streams to responsibilities, and then on to operational, technological and system monitoring considerations.”

The following sections outline some of the most important processes and procedures that need to be established to ensure compliance with this code.

**DUTY OF CARE**

The board of directors (or other equivalent group) of an organization is responsible for the conduct of that organization in every way—financially, operationally, legally and ethically. Specifically, it has responsibility for the organization’s assets and their use. One such asset is information—not information systems, but stored information itself. It is essential that organizations be aware of the value of information that they store.

**DESIGN FOR EVIDENCE**

Traditionally, corporations have considered the evidentiary implications of electronic documents only when it is required for litigation, or forensic practitioners have focused on collecting IT evidence as artifacts of an investigation. Unlike latent evidence that is inadvertently produced when a person contacts something (e.g., fingerprints, DNA), computer systems must be specifically designed to generate electronic records in a manner that maximizes their potential evidentiary value. Once electronic records are created, they must be carefully handled to maximize their evidentiary weight.

**SECURITY MEASURES**

All information, irrespective of the media on which it is stored, is vulnerable to loss or change, whether accidental or malicious. To protect information stored electronically, security measures need to be developed and implemented to reduce the risk of a successful challenge to its authenticity.

---

**Figure 1—The Principles of Good Practice for Information Management**

![Diagram showing the five principles of good practice for information management]

Source: BSI Group, PD 0010:1997

---

---

Enjoying this article?

- Read Electronic Discovery. [www.isaca.org/e-discovery](http://www.isaca.org/e-discovery)
- Learn more about, discuss and collaborate on cybersecurity and business continuity/disaster recovery planning in the Knowledge Center. [www.isaca.org/knowledgecenter](http://www.isaca.org/knowledgecenter)
However, security is not a concern with computer systems only. Security and availability of the operating environment (e.g., buildings, temperature controls, network links, physical media) and the auditable implementation of procedures by all staff are key elements.

Security measures are often developed in an unstructured way, by reacting to security incidents and/or to available computer software tools. This approach on its own can easily leave gaps in security, which are filled only at some later date, typically after a security breach. A more structured approach is to review the information assets of the organization, and then assign risk factors based on asset value, potential threats, system vulnerability and likelihood of attack. These should be assigned on the basis of which appropriate, cost-effective security measures can be identified.9

ACCESS RIGHTS

“The segregation of roles is a fundamental aspect of duty of care,” according to the Code of Practice for the Implementation of BS 10008. It provides a check on errors and on the deliberate falsification of records. In this respect, segregation of roles is particularly important in systems where there is risk of fraud or other malicious action.

Code of Practice for the Implementation of BS 10008 further suggests that it is also important to ensure that the physical and managerial segregation that exists around a system is mirrored by the logic access control within it, via the implementation of an access control system. Only staff with relevant access rights should be permitted to enter data or amend stored data. It is also important to ensure that a suitably granular level of automatic logging is applied to the process to record the activities performed, times and dates.10 System access rights should be granted only after the members of staff have successfully proved their competence.

Some of the electronic data files can have a nonhuman author. A computer-generated record is the output of a computer program untouched by human hands, thus the author can be considered to be a particular computer program or programs executing on a particular computer or multiple computers. One computer program may author many records, and many computer programs may author elements of a single record. Each computer program generating elements of the electronic record must be identified clearly in the record. The key evidentiary issue is demonstrating that the computer program generating the record is functioning properly.11

Further, some data files, particularly those generated by word processor or spreadsheet programs, may contain automatically executable code (often referred to as macros), which can have the effect of modifying the file each time it is retrieved, viewed or printed out. It may be difficult to assess what evidential weight is attached to such files.12

RELIABLE AND TRUSTWORTHY SYSTEMS

It is important to be able to demonstrate that the computer system has been functioning properly (i.e., according to agreed-upon procedures) in order to authenticate data stored on the system. Arguments over admissibility of information as evidence can lead to an investigation into the system from which the information came, the method of storage, operation and access control, and even into computer programs and source code. It may be necessary to satisfy the court that the information is stored in a proper manner. This could be a tactic used to try to discredit the evidence and to make inadmissible, or reduce the evidential weight of, that evidence and any similarly stored information that is produced.

Questionable hardware reliability, for example, could be used to discredit the information management system. This could call the whole system into question and cause information stored within it to be ruled inadmissible.15

It is important to utilize reliable and trustworthy technology to store electronic information over a long period of time. Each part of the system needs to be chosen with care, taking into account the possible need to demonstrate the proper and appropriate working of the system some time in the future. This demonstration may need to encompass both technology itself and the methods by which it was configured and used.14

The information management system should be maintained and corrective maintenance should be carried out only by qualified personnel to ensure that its performance does not deteriorate to such an extent that the integrity of the data captured, created by or stored within it is affected. A maintenance log should be kept, stating the preventive and corrective maintenance procedures completed. The log should include information regarding system downtime and details of action taken. Where system access control can be bypassed during maintenance of hardware and/or software, personnel performing such processes should be strictly controlled, monitored and audited.15
BUSINESS CONTINUITY PLANNING

From time to time, problems arise with information management systems that require emergency procedures to be implemented in order for recovery. Such procedures may involve the temporary use of additional or third-party resources. To ensure that the integrity of information is not compromised during these operations, an agreed-upon and approved business continuity plan (sometimes known as a disaster recovery plan) may be implemented.

Procedures to be used in cases of major equipment, environmental or personnel failure should be developed, tested, maintained and implemented. Such procedures should ensure that the integrity of stored information is not compromised during implementation. Issues surrounding the security of backup data may be important in the event of a dispute over authenticity. It may be argued that backup media had been compromised, and then used to recover from an information loss, thus affecting the authenticity of stored information. In some cases, the availability of backup data that have been in secure storage, to be used only in the event of a challenge to the authenticity of the live data, can be used to enhance the evidential weight of the stored information.16

DATE AND TIME STAMPS

Being able to determine the date and/or time of an event can be an important piece of evidence. Thus, all appropriate events should be date- and/or time-stamped. Where accuracy of date and/or time stamps is important, regular checking of system clocks should be carried out. Any errors should be corrected and any actions taken should be documented. Only authorized personnel should be able to change system clocks.17

AUDIT TRAILS

Code of Practice for the Implementation of BS 10008 further suggests that when preparing information for use as evidence, it is often necessary to provide further supporting information. This information may include details such as date of storage of the information, details of movement of the information from a medium, and evidence of the controlled operation of the system. These details are known as audit trail information. This audit trail information is needed to demonstrate that the system is working as well as the progress of information through the system. Audit trails need to be comprehensive and properly looked after, because without them, the integrity and authenticity and, thus, the evidential weight of the information stored in the system could be called into question.

The audit trail consists of the aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the information management system. As such, it covers the answers to all classic questions concerning the provenance of any piece of information stored within the information management system:18

1. Who?
2. What?
3. Where?
4. When?
5. Why?
6. How?

Access to the audit trail information needs to be controlled. In some applications, access may be needed only infrequently, so it is important that the interpretation procedures be documented. As audit trail data may be inspected by authorized external personnel (such as auditors) who have little or no familiarity with the system, interpretation procedures should be understandable to nontechnical users. The storage of audit trail data is a topic often not included in an organization’s information management policies. As they are frequently created automatically and infrequently accessed, they are forgotten and, thus, not subject to adequate control.19

Some systems control the size of audit trail data files by the use of looping. Looping sets the maximum size for the data file, and when the size is reached, new data overwrite the oldest data in the file. Thus, old audit trail data are lost. This process may not be in compliance with required retention policy. This should not be the case with audit trail data from information management systems, which should be stored for the same period as that of the data to which they relate.

In a general sense, if an attacker gains unlimited access to a system, if the audit trail is not protected by write-only or write-once technology, and if no physical means are used or are effective in determining authenticity of audit trails, it is possible to create a forged audit trail that is not differentiable from a legitimate audit trail.

When attackers try to cover up attacks, they tend to do one of three things:
1. Attempt to delete all files on a system to remove all traces of their entry.
2. Try to modify selected audit trails to remove any indication of their use.
3. Try to prevent their attack from being audited by avoiding the use of audited events.

If they prevent their attacks from being audited by avoiding the use of audited events, there is little that can be done to detect their tampering within the system.\textsuperscript{20}

**CONCLUSION**

ICT brings potentially increased, or at least different, risk in terms of civil or criminal wrongdoing, and organizations must be able to protect themselves against such risk. Failure to do so raises governance and accountability issues for which management of the organization could be held responsible.

When information is used as evidence in the event of a dispute, the maximum weight of evidence is not affected by the size or shape of the organization and its own view of security risk. It frequently depends on the opinion of an independent arbiter. That view may well be affected by the opposing party in the dispute attempting to discredit evidential value.

Legal admissibility concerns whether a piece of evidence would be accepted by a court of law. To ensure the admissibility, information must be managed by a secure system throughout its lifetime (which can be for many years). Where doubt can be placed on the information, the evidential weight may well be reduced, potentially harming the legal case.

BS 10008 can provide assurance that any electronic information required as evidence of a business transaction is afforded the maximum evidential weight. Compliance with this standard does not guarantee legal admissibility. It defines best practice. The standard pays particular attention to setting up authorized procedures and subsequently being able to demonstrate, in a court of law, that these procedures have been followed.

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

**ENDNOTES**

\textsuperscript{1} International Telecommunication Union (ITU), *Understanding Cybercrime: A Guide for Developing Countries*, Switzerland, 2009

\textsuperscript{2} Ibid.

\textsuperscript{3} Danielsson, Jerker; Ingvar Tjøstheim; “The Need for a Structured Approach to Digital Forensic Readiness: Digital Forensic Readiness and E-commerce,” IADIS International Conference e-Commerce, 2004


\textsuperscript{5} BSI Group, BS 10008:2008 *Evidential weight and legal admissibility of electronic information*—Specification, UK, 2008

\textsuperscript{6} BSI Group, PD 0010:1997 *The principles of good practice for information management*, 1997

\textsuperscript{7} BSI Group, BIP 0008-1:2008 *Evidential Weight and Legal Admissibility of Information Stored Electronically. Code of Practice for the Implementation of BS 10008*, UK, 2008

\textsuperscript{8} Australian Standards, HB 171—2003, *Guidelines for the management of IT evidence*, Australia, 2003

\textsuperscript{9} Op cit, BSI Group, BIP 0008-1:2008

\textsuperscript{10} Ibid.

\textsuperscript{11} Op cit, HB 171—2003

\textsuperscript{12} Op cit, BSI Group, BIP 0008-1:2008

\textsuperscript{13} Op cit, BSI Group, BS 10008:2008

\textsuperscript{14} Op cit, BSI Group, BIP 0008-1:2008

\textsuperscript{15} Ibid.

\textsuperscript{16} Ibid.

\textsuperscript{17} Ibid.

\textsuperscript{18} Ibid.

\textsuperscript{19} Ibid.

\textsuperscript{20} Cohen, Fred; *Challenges to Digital Forensic Evidence*, Fred Cohen & Associates, 2008
SAP is a business system widely used across geographies and industry sectors that supports the most critical business processes. SAP has also increased its presence on the Internet and provided an architecture that facilitates integration with other business solutions. All these characteristics have increased the risk of security breaches that have the objective of obtaining access to sensitive information and performing fraudulent business transactions.

During recent years, security-related sites on the Internet have significantly increased the amount of information available on SAP vulnerabilities, and security professionals have made SAP part of the agenda at national conferences. At the same time, information sharing and collaboration among hackers have increased, and the tools to break into SAP systems are already provided at no charge on the Internet.

SAP comprises different layers and components to respond to a wide and demanding spectrum of business requirements. These elements have a security dimension that could open the system to potential vulnerabilities and increase the risk that unauthorized users could gain elevated access to business data.

This article focuses on the application-level risk that arises from inappropriate implementation of access controls. One of the most critical issues is the ability to compromise user passwords using freely available tools found on the Internet. While there are reported vulnerabilities at different levels involving the database, operating system, Java and other components, attacks at the application level facilitate many activities for the attacker, including, for example, access to sensitive information and the ability to perform fraudulent business transactions.

The following sections provide foundational concepts and technical details to facilitate a comprehensive understanding of password-related attacks that could be performed and appropriate actions to prevent SAP security breaches.

**Hashing**

Hashes are widely used to verify the integrity of data and identify duplicate information. They also play an important role during authentication processes. But, what is a hash? A hash is the result of processing a block of data—in this case a password—through a procedure or algorithm that returns a fixed number of characters. The related output should meet the following conditions:

- **Functional**—Generating a hash from a given block of data should be performed through a simplified process that can be quickly executed.
- **Irreversible**—It should not be feasible to take a given hash and find the original block of data.
- **Collision free**—It should not be feasible for two different blocks of data to produce the same hash.

SAP uses hashes during the authentication process to verify that the password entered by the user matches the password stored in the system. Basically, the user enters the ID and password for authentication, and a hash is generated from the password that was entered. The hash and ID are sent out over the network to the main system for validation, and the received hash is compared against the stored hash. If they match, the user is successfully authenticated.

**Techniques to Decode a Hash**

Hashes are based on mathematical algorithms that meet the aforementioned conditions. Throughout the years, cryptographers have developed techniques to analyze these algorithms and find the block of data that generates a given hash. Such techniques are aimed at breaking the essential
conditions of a hash and should be irreversible and collision free. Hash attacks are mostly based on the following two techniques:

• **Random attack**—A large number of passwords are automatically generated; each password is converted into the corresponding hash and compared against the value stored in the system. A match indicates that the user password has been found. A dictionary attack, which is based on a predetermined list of potential passwords, can also be used to find a matching hash; there are free dictionaries available on the Internet to facilitate this type of attack.

• **Collision attack**—Different blocks of data and the resulting hashes are analyzed to find two different entries that generate the same hash. Once this is obtained, mathematical conclusions can be reached and potential weaknesses in the hashing algorithm identified. This information facilitates the creation of an automated procedure to find a block of data that generates a given hash.

The time necessary to find a matching hash depends on the hashing algorithm being used, the size of the hash to be produced and the potential characters to be included in the block of data. These conditions increase the number of passwords to be generated and the complexity of the process.

**SAP PASSWORD CRACKING**

**Figure 1** shows hashes that were obtained from an SAP system and processed via freely available tools found on the Internet using a brute-force attack technique. Please note that the password complexity increases the processing time that was necessary to break the hash and determine the actual password.

**Figure 2** shows the results from previous evaluations of password vulnerabilities in corporate SAP systems. The following results were obtained using a dictionary-based attack with word lists freely available on the Internet. Tables from two different SAP systems containing user IDs and passwords were processed. System 1 contained about 2,500 hashes, and system 2 contained about 4,500.

![Figure 1–Hashes Obtained From an SAP System](image)

<table>
<thead>
<tr>
<th>Password</th>
<th>SAP Hash</th>
<th>Processing Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOSE01</td>
<td>85A159EB01D4CF7F</td>
<td>1 minute 48 seconds</td>
</tr>
<tr>
<td>JOSE9!</td>
<td>9292594E34EAC311</td>
<td>4 hours 58 minutes</td>
</tr>
<tr>
<td>JOSEESPI</td>
<td>174BF27C78402208</td>
<td>1 day 21 hours</td>
</tr>
</tbody>
</table>

Note: Data were processed using a Toshiba Satellite A105, 1.50 Ghz dual processor, 2 GB RAM.

**Figure 2—Results From Previous Evaluations of Passwords in Corporate SAP Systems**

<table>
<thead>
<tr>
<th>SAP System</th>
<th>Words in Dictionary</th>
<th>Passwords Guessed</th>
<th>Processing Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>System 1 (2,500 users)</td>
<td>Over 17 million</td>
<td>1,600</td>
<td>6 hours</td>
</tr>
<tr>
<td>System 2 (4,500 users)</td>
<td>Over 17 million</td>
<td>2,500</td>
<td>15 hours</td>
</tr>
</tbody>
</table>

Note: Data were processed using a Toshiba Satellite A105, 1.50 Ghz dual processor, 2 GB RAM.

It is important to emphasize that the hashes in **figures 1 and 2** were obtained from actual SAP systems that authenticate users with access to the system via SAP GUI (Graphical User Interface). Various companies have implemented other systems to enable single-sign-on functionality; in such cases, the main authentication is performed by a different system and hashes cannot be retrieved from SAP. However, even with the use of single sign-on, there is typically a group of selected users who continue to access the system using SAP GUI.

**OBTAINING SAP PASSWORD HASHES**

The following are the methods used to obtain the password hashes described in the previous section. The same techniques can be followed to access sensitive business data such as vendor names, pricing, raw materials, and personal and financial information.

Password hashes are stored in user master and historical tables. Hashes associated to previous passwords should be
taken into consideration because an attacker can analyze the related data and establish patterns to determine the actual password. There are several approaches that could be followed to obtain the hashes, but perhaps one of the easiest ways that is often available to users in the production environment relates to table browsing.

**Table Browsing**

SAP provides the ability to browse tables through several transaction codes. Often, business users and IT personnel have access to view tables and download information without appropriate restrictions to prevent access to sensitive information.

Appropriate access to tables is not difficult to establish. However, the following aspects are usually overlooked:

- **Authorization groups**—SAP provides the ability to restrict access to tables based on table groups; these groups are standard, delivered by SAP and typically contain a large number of tables. Although table groups can be customized to tailor user access based on the demonstrated need to view data, often standard, delivered groups are used, and wide access to view data is granted to many users in production environments.

- **View-only access**—On the premise that update access to business data constitutes the highest risk and table browsing provides only the ability to view it, inappropriate access to critical data, such as password hashes, often goes unnoticed, and the ability to browse tables containing private information and key business data is frequently overlooked.

SE16 is one of the transaction codes that could be used to obtain SAP password hashes through table browsing. The process is fairly easy to perform. For instance, once the transaction code is executed, the information can be downloaded to an Excel file following four simple steps (see figures 3–6).

**Debugging**

The ability to debug programs in production environments offers another way to obtain password hashes. Depending on additional authorizations, a user could execute a program that reads tables with hashes and start debugging it. Debug mode makes it possible to look at the values being processed and obtain password hashes. For example, the ability to execute a basic report, such as RSUSR200—List of Users According to Logon Date and Password Change, which reads “a table that contains user-related data, could be sufficient to obtain a hash,” as illustrated in figures 7–10.

**RFCS**

Remote function calls (RFCs) are used to establish connections with SAP and non-SAP systems. For example, an application might connect to an SAP system through an RFC and execute a program that returns data. In this case, the application is known as the caller and SAP is known as the calling system or destination.

It is possible to take advantage of RFCs that are already configured in SAP and gain unauthorized access to the system. For example, a development kit, which enables the use of RFCs, can be obtained on the Internet at no cost and installed on Windows computers to access the SAP production system and download tables containing sensitive information. Furthermore, libraries installed on Windows desktops/laptops for users to access the SAP system can be reused from MS Office applications to connect to production environments and download data. Although...
some programming is necessary, the associated code is freely available on the Internet. Another aspect to consider is that authentication controls through RFCs might not be as strong as those associated to user logons.

THE RISK
Breaking passwords might seem to be a difficult activity to undertake; however, no significant effort was required to perform the activities described in the previous sections. The
Following the program indicates that table usr02 is being retrieved. Double click on iusr02.

Figure 8—Enable Debugging

2. Enable debugging.
3. Execute report.

Figure 9—Follow the Program in Debug Mode

4. Following the program indicates that table usr02 is being retrieved. Double click on iusr02.

Figure 10—Obtain the Hash

5. Password hash associated to the DDIC account. DDIC usually provides wide access to the system.

necessary tools can be easily downloaded and installed without sophisticated computer literacy, and the sites providing such tools are based on collaboration and address questions about installing, using or even making improvements to the tools provided. The following are some of the most relevant areas of risk:

- **Corporate espionage**—There have been several incidents over the last few years that point to an increase in corporate espionage and involve companies of all sizes, targeted, in some cases, by competitors to obtain trade secrets. The attacks have been significant enough in the US for the government to investigate and increase the level of awareness around the risk.

Security breaches have originated outside and inside of the network perimeter, including external attackers as well as internal personnel. Corporate espionage is not the only concern; confidential data have also been exposed due to other types of incidents in various companies. SAP systems hold trade secrets and confidential information; therefore, inappropriate safeguards could have costly consequences to the enterprise and might also place it at a considerable disadvantage against its competition.
• Increasing number of users with access to sensitive information—This article has explored only a few ways that could be used to obtain password hashes and access sensitive business data. The methods used require access to the SAP system and authorizations to browse tables, debug programs or connect to the system using RFCs. Although the access to these special functions should be restricted, large numbers of users are often found to have unnecessary access to them.

Once attackers cross the network perimeter, they can specifically identify the SAP system and target the database. Even before access is obtained, they already know the specific tables that will provide them with valuable information to gain application-level access. Depending on the objective, database-level access may be sufficient to obtain sensitive business data.

• Ineffective segregation-of-duties (SoD) controls—SoD controls are often in place to prevent users from engaging in fraudulent activities that involve the execution of conflicting business functions. Although this is a necessary control, it may not be sufficient to address the risk when individuals have the potential to obtain access using multiple IDs. An attacker can easily impersonate a number of users involved in an entire business process, gain access to conflicting functions and successfully circumvent controls.

• User accountability cannot be established—Establishing accountability of the impersonated users could be a complicated task. Although there are SAP system logs that might help establish accountability, the necessary logs might not be enabled or retained. Additional system logs that go beyond the SAP system could also be necessary.

ADDRESSING RISK
To address the risk of inappropriate access to the SAP systems, the following activities should be considered:

• Identify and secure sensitive data—An attacker might not be willing to carry out fraudulent business transactions in the SAP system; instead, the attacker’s objective could be focused on trade secrets and business-related information that could be valuable to competitors. Therefore, it is necessary to risk-assess the data from this perspective and identify the actual repository (i.e., tables) in the system to secure it. Reports and other programs that could provide the ability to perform massive downloads of this information should also be identified to implement appropriate safeguards. Although this might seem to be a laborious exercise, it is important to take into account that the SAP system provides the ability to automate many of the related time-consuming tasks.

A limited number of users with access to sensitive data certainly decreases the risk, mostly because the attacker might not be able to break all the user passwords in the SAP environment, and having fewer IDs that can be used to obtain the information reduces the overall exposure.

• Perform a comprehensive SAP security assessment—There are several ways to gain unauthorized access to sensitive information in the SAP system. A comprehensive assessment combined with a penetration test constitutes an effective method to prevent attacks. There are specific and extensive security guidelines provided by SAP that can be incorporated in the assessment. A comprehensive assessment should also consider the analysis of SAP audit trails to identify indicators that point to the inappropriate use of IDs.

CONCLUSION
The following factors increase the risk of SAP security breaches and could have costly consequences to the enterprise in terms of trade secrets, confidential information and compliance mandates:

• Recent activity reflecting that unauthorized access to sensitive business information is on the rise; attacks involving internal and external attackers
• SAP systems holding valuable business information and sensitive data
• Rapid dissemination of SAP hacking techniques and related vulnerabilities
• Freely available software to attack SAP systems and related components
• System complexity leading to inappropriate implementation of access controls
• Increasing presence of SAP systems facing the Internet

The following are actions that can be taken to minimize risk associated with security breaches in SAP environments:

• Risk-assess the different components of the SAP system, and take action to evaluate controls intended to deter security breaches; prioritize systems facing the Internet and highlight real exposures.

• Perform a risk assessment to identify the most critical business data, and classify the information that could place the enterprise at a disadvantage against competitors.
Address the risk of noncompliance with external mandates and other threats that could cause reputation damage.

- Use SAP functionality to identify tables, programs and reports that provide access to sensitive information, and take action to validate that access is based on a user-demonstrated need to view and change data.
- Secure back doors at the application level, and validate that only users who require access based on assigned job responsibilities have the ability to execute critical system functions that provide access to sensitive information.
- Perform penetration testing specifically targeting SAP systems to assess current vulnerabilities; take appropriate action, depending on the results, to secure the weakest security links.

REFERENCES
SAP, “Password Parameters for Logon and Password,”
SAP, Note 862989—New Password Rules (NW ABAP 7.0), valid since 2007
SAP, Note 874738—New Password Hash Calculation Procedure (code version E), valid since 2005
SAP, Note 991968—Value List for login/password_hash_algorithm, valid since 2009
SAP, Note 1023437—Downwardly Incompatible Passwords (since NW 2004s), valid since 2007
SAP, Note 1237762—ABAP Systems: Protection Against Password Hash Attacks, valid since 2009
Lehnert, Volker; Katharina Bonitz; Authorizations in SAP Software—Design and Configuration, SAP Press

ENDNOTES
1 SAP, “Logon and Password Security in the ABAP System,”
http://help.sap.com/saphelp_nw04s/helpdata/en/52/6717ed439b11d1896f0000e8322d00/content.htm
3 SAP, SAP Business Planning and Consolidation 7.0 SP02, “SAP Netweaver Application Server Security Guide,”
http://help.sap.com/saphelp_bpc70sp02/helpdata/en/57/d8bfc5a586f46b95ce1f52b5f5184/frameset.htm
Contemporary enterprises have become aware of the need to intensively manage their business processes. Process flexibility and efficiency are generally considered important determinants for the ability to achieve operational excellence. However, less-strict information systems that provide high process flexibility implicitly enable the occurrence of process behavior that significantly deviates from a designed model. In the ideal situation, this business process model takes into account the applicable legislation, directives and business policies.

Business process analytics and mining techniques address the problem that most internal control experts have very limited information about what is actually happening in the business processes. This article aims to introduce business process analytics and mining to the information systems (IS) audit and control community. Focus is placed on discussing the central concepts and on providing useful cases for process analytics and mining in the internal control setting.

**BUSINESS PROCESS ANALYTICS**
Business process analytics is a new and promising way of acquiring insights into an enterprise’s business processes. This set of techniques enables the analyst to extract knowledge from previous process behavior, as described in the event logs of process-aware information systems (figure 1). These event logs contain a multitude of information on events that are of importance in the context of the business process supported by the information system (e.g., who performed an activity and when it was performed). In many enterprises, such event logs are already available and conceal an untapped reservoir of knowledge about the way employees and customers conduct everyday business transactions. For example, popular enterprise resource planning (ERP) systems, such as SAP and Oracle E-Business Suite, and workflow management systems, such as ARIS, TIBCO and Biztalk, already keep track of these events.
The business process analysis techniques that are of interest for internal control experts can be roughly categorized into three classes:

• **Process discovery and visualization**—These techniques provide the analyst with a visual summary of a specific aspect of the business process (e.g., the activity sequences). A typical application is the heuristics miner algorithm, which provides easy-to-understand process graphs.

• **Conformance checking and delta analysis**—The second class of techniques aims at detecting inconsistencies between a prescriptive process model (i.e., a designed process model) and the corresponding real-life process behavior. The major difference between them lies in the comparison base for the real-life process: Conformance checking uses the event log, while delta analysis uses a process model obtained with a process discovery technique. The conformance checker is the most fundamental contribution in this technique subset.

• **Rule-based checking**—The third set of techniques enables the analyst to verify whether a specific business rule is satisfied (e.g., segregation of duties, execution of an approval cycle). The linear temporal logic (LTL) checker with configurable rule patterns can be considered one of the most influential contributions in this subset.

Business process analysis techniques have mainly focused on extracting knowledge on common activity sequences. However, each of the three technique classes consists of a wide spectrum of techniques that together cover the main aspects of a business process (i.e., the process perspectives).

**PROCESS PERSPECTIVES**

Business processes commonly cover several aspects of an enterprise’s operations. Consequently, business process management focuses on structuring, for example, what needs be done, who will be doing it and when it must be done. Accordingly, the business process management literature discerns the following four perspectives:

• **Functional perspective**—Deals with the occurrence of a particular process element in the entire process history or in the context of a specific process execution (e.g., presence of a certain activity)

• **Process-flow perspective**—Covers the process behavior in terms of when process elements can occur in a process instance. This includes a wide variety of ordering relations between activities, as well as complex decision-making conditions and activity preconditions. The process mining research primarily centers on this perspective.

• **Organizational perspective**—Focuses on the enterprise behind the business process, which agent performs the different process elements in a process instance, taking into account factors such as timing and environmental conditions. The term “agent” can have a broad interpretation, varying from a single person over a department to a whole enterprise.

• **Data perspective**—Handles the information elements (e.g., documents, messages) that are used, produced or manipulated during the process, as well as the prescribed relationships among them.

For each individual process perspective there exist a variety of business process analysis techniques. The following section elaborates on this topic and links the combinations with common activities in an internal control setting.

**BUSINESS PROCESS ANALYTICS AND INTERNAL CONTROL**

Each of the business process analytics technique sets allows for a wide variety of applications in the internal control setting.

**An Overview of Business Process Analytics and Mining Applications for Internal Control**

Figure 2 provides a detailed overview of the potential business process analytics and mining support for the activities performed by internal control experts. It also indicates for each general activity type which business process analytics and mining techniques are most suitable.
In addition to post mortem analysis, the business process analytics techniques may provide adequate tool support for continuous process improvement. For example, an open-minded analysis in combination with a rule-based service-level analysis might uncover process deviations that frequently result in performance decreases. Consequently, timely and effective recommendations can be drawn up.

Most of the supporting business process analytics and mining techniques for each of the different process perspectives are supported by the open-source tool ProM. The tool, as well as more information on the specific techniques, can be found on the process mining web site of the Process Mining Group.6

Illustration of Business Process Analytics and Mining for Internal Control

This section provides an example of the application of business process analytics in an internal-control setting. Due to limited space, only three analysis techniques that produce strong and easy-to-understand summaries of certain process aspects are elaborated. Figure 3 provides the designed process model (in the business process modeling notation [BPMN]) of a rather straightforward purchase process, including a management approval cycle. An event log containing 300 process instances, including several process instances with harmful deviations, was artificially constructed.

<table>
<thead>
<tr>
<th>Risk identification and assessment</th>
<th>Process Discovery and Visualization</th>
<th>Compliance Checking and Delta Analysis</th>
<th>Rule Checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open-minded analysis of process reality</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis of infrequent behavior</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Risk identification</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Historic data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simulation of extreme situations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessing likelihood and risk impact</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Historic data</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Simulation of extreme situations</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control activities</th>
<th>Process Discovery and Visualization</th>
<th>Compliance Checking and Delta Analysis</th>
<th>Rule Checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing detective controls</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Determining effectiveness of (preventive) controls</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Collecting detailed evidence on control effectiveness</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Monitoring evolution in likelihood and risk impact</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Generation and communication of information</th>
<th>Process Discovery and Visualization</th>
<th>Compliance Checking and Delta Analysis</th>
<th>Rule Checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating clear, focused, honest, accurate and timely reports</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2—Business Process Analytics and Mining Support for Internal Control

Figure 3—Designed Prescriptive Process Model for Purchasing Goods
Figure 4 represents an extract process model that was derived from the process history recorded in the event log. An open-minded analysis would immediately result in the identification of important irregularities:
• There exists at least one process instance in which the changed order was not approved afterward.
• It seems that there are process instances, including a pay activity, for which the information system did not record any handling activities performed upon receipt of the goods.
• The enterprise did not pay for all the goods it received.

The originator-by-task matrix in figure 5 provides a strong visual summary of the organizational perspective (i.e., who did what?). In figure 5, Richard is a clerk in an enterprise in which approving an order can be done only by management. As a result, the internal-control expert must investigate the six times Richard executed the activity “approve order,” as it may indicate fraudulent behavior. The results can be easily compared to a Responsible, Accountable, Consulted and Informed (RACI) chart.

Previously, the heuristics miner output enabled the internal-control expert to identify a potentially harmful issue: Some process instances did not contain an approval activity for a changed order. Figure 6 provides the output of a rule-based checking technique that was configured to evaluate the following statement: If a change order activity is executed, it must always be followed by an “approve order” activity. As the output in figure 6 shows, in 14 out of 48 process instances...
containing a “change order” activity (based on a total of 300 instances), there was no order approval after the order had been changed. This enables the internal-control expert to assess the likelihood of occurrence of this process deviation and to identify the exact cases that require further investigation.

**OPPORTUNITIES**

Business process analytics and mining techniques have multiple advantages that present opportunities for a more efficient and effective control environment. The following are the four major advantages:

1. **Acquiring detailed and objective information on the business operations**—Flexibility is becoming an important determinant for the operational excellence of an enterprise, resulting in business process behavior that significantly deviates from designed process models. Additionally, the business processes performed by knowledge workers often tend to be rather nondeterministic. In particular, process discovery and visualization techniques can help the internal control expert with exposing the business process reality, based on which the expert can make better informed decisions in the planning of further internal-control-related activities.

2. **Pursuing absolute assurance**—Business process analytics and mining techniques enable internal-control experts to perform their testing procedures on the full population, thereby offering (near) absolute assurance. While attaining an absolute level of assurance can be undesirable due to budget and time restrictions, it can be achieved with process analytics and mining techniques with only a marginally higher cost in terms of processor time compared to sample-based testing with the same techniques. Consequently, the risk of the evidence failing to uncover misstatements can be significantly reduced.

3. **Auditor independence**—The value of internal-control expert reports is largely determined by the controller’s independence from the daily operations in the enterprise under review. Business process analytics and process mining techniques do not directly affect the enterprise’s information systems, as they use only the event log system. Consequently, this approach does not require any cooperation from the process owner, which could result in *a priori* knowledge on the control procedures.
4. Obtaining persuasive evidence—The persuasiveness of the evidence obtained through process mining techniques is expected to be high because of the competence and the sufficiency that can be attained. The competence of the evidence is mainly determined by the independence from the enterprise, the internal-control expert's direct knowledge, the degree of objectivity and the timeliness (referring to both the period covered and the ability to reduce the time delay). These determinants can be easily related to business process analytics and mining as discussed in the previous sections. Due to the fact that the whole population of transactions can be efficiently inspected, the sufficiency of the evidence can be optimal.

CONCLUSION

As business process management becomes more established, the need for appropriate analysis and evaluation tools grows. Business process analytics and mining techniques enable the internal-control expert to acquire detailed insight into the real process behavior and to perform a wide variety of control-testing procedures. Additionally, these techniques can provide adequate support for continuous process improvement, e.g., by monitoring compliance with directives and service level agreements (SLAs) or by providing warnings when harmful process deviations occur.

The business process analytics and mining approach is characterized by the ability to acquire objective and persuasive evidence, via the auditor’s independence and the pursuit of absolute assurance. Consequently, the use of business process analytics and mining techniques can contribute to a more effective and efficient control environment in process-oriented enterprises.

ENDNOTES

3 Weijters, A.; J. T. S. Ribeiro; “Flexible Heuristics Miner (FHM),” IEEE Symposium on Computational Intelligence and Data Mining (CIDM), 2011, p. 310–317
8 Op cit, van der Aalst, 2005, p. 130–147
9 Arens, A. A.; R. J. Elder; M. S. Beasley; Auditing and Assurance Services: An Integrated Approach, Pearson Education, 2005
ACROSS
1. It is described as the new era of technology (2 words)
5. Former president of FEI, past international president of ISACA and author of “Managing the Audit Function,” Michael __
10. Add
11. Bring disparate parts together
12. SEC has mandated that public companies must use this programming language to meet the agency’s filing requirements
15. Salvage loss, for short
18. Commission formed in 1985 relating to fraudulent financial reporting
21. Deceived
22. Southeast US state
23. Short for a lot of money
25. Marketing medium
27. Abbreviation for a tool that enables testing and auditing of applications and can also reperform automatic calculations
30. Duplicate
31. Obscure
33. Vital for IA to earn this with company executives
35. Theoretical distribution with finite mean and variance
37. Valuable member of a company
38. Cloud hosting that permits use of public and private clouds
41. Best guess, abbr.
43. See 44 across
44. Maximum electrical demand (goes with 43 across)
45. IBM’s Jeopardy champion

DOWN
1. Dangerous form of SEO (2 words)
2. IaaS provider enjoying rapid adoption (2 words)
3. Predicts and prevents from occurring
4. Saying
5. Executive position over audit, abbr.
6. Veto
7. Useful tool for detecting flawed data and tracking the application that caused it, abbr.
8. Rare earth mineral, for short
9. IT Infrastructure Library, for short
13. Can
14. Control
15. Public relations effort
17. Mouse home
19. Also called
20. Enter a system
23. The M in CM
24. Gravitated toward
26. Part of some email addresses
27. Computer vacuum, for short
28. Anchorage locale, abbr.
29. Groups of people working for a common purpose
32. While
34. Automated
35. Nerd
36. Demonstrated
39. Facebook filed for one
40. Impenetrable
42. Author of The Black Swan
46. Dispose of
47. Most important
49. Popular
50. Ford model
51. Leonardo’s middle name

(Answers on page 54)
Q There is a lot of talk about Bring Your Own Device (BYOD) initiatives. It is widely predicted and discussed that such an option will be the order of the day in the future. What kind of security controls must be in place to tackle BYOD? Will conventional security controls work, or do you envisage the need for any new controls?

A The main argument in favour of BYOD initiatives is that the new generation of employees prefers to bring its own devices to work. With the advancements in mobile technologies, the widespread use of smartphones and tablet PCs, and the proliferation of wireless and broadband, voices in support of BYOD continue to rise.

But, what does it mean to a corporate organisation? Should it choose to heed to demand, or should it clearly ban BYOD ab initio?

Let us discuss the controls that ought to be in place if BYOD were to be implemented. As always, please note that this is just an indicative and not an exhaustive list:

• It must be impossible to transfer any data belonging to the entity, at any cost, to the local or employee-owned devices. The employee must simply be able to browse the information and enter data. In other words, local storage of information must not be possible. The device may be capable of storing locally. What we aim to achieve here is that the employee, while logged on to the corporate network, must not be able to capture data in any form and store them on the local device.

• Even printing may require restriction. Many business process outsourcing (BPO) companies do not allow printing facilities to their employees. The control is aimed at avoiding any data spillage or theft.

• Strong authentication and authorisation controls must be in place. This is a basic control that must be in place irrespective of whether the device is employee-owned.

• Proper logs must be created and maintained for a pre-defined period. It is essential to have a policy that defines the activities that require logging. The archival period must also be defined. Processes to analyse logs in an intelligent manner and make informed decisions must also be in place.

• Employers must have controls to permit only those specific devices that are pre-authorised and configured to access the corporate network. Something called MAC binding is in practice even today. This control means that only certain machines, whose MAC addresses are designated as allowed, are permitted to log on to the network.

• Background checks of the employees play a key role in successful BYOD initiatives. Impeccable integrity is a must—non-negotiable. Of course, this is something that is essential in any operating model, but in this case, it is even more necessary.

• Encryption is another mandatory control that must be in place. This is particularly essential because encryption is the only option to protect the data from unauthorised access should the device ever get lost and fall into the hands of someone who is not authorised to access such information. When we talk about encryption controls, it goes without saying that key management processes must be in place.

• It must also be possible to wipe data off employees’ devices, even though the devices are owned by the employees and not by the employer. It is possible to achieve this, and a number of companies have this control in place even for smartphones that employees use to access their email.

• Employers must also obtain legal advice and put proper controls in place to face litigation that may arise. This control is as important as technology controls.

• Data leakage prevention (DLP) solutions are becoming very popular. Again, in certain countries, the legal environment does not permit easy implementation of DLP due to privacy laws and regulations. DLP controls should play a significant role if BYOD initiatives are to be implemented.
Looking at all the controls collectively, we can infer that, except for a few, most are conventional or traditional. Nothing major has changed in the security controls environment to support the BYOD movement, except that the importance of certain controls has increased.

Some employers may take a narrow view that BYOD is a great cost-saving option—that they do not need to provide any IT support. But, that is a very short-term view. There is a good deal of risk about and for which organisations must be cognisant and take relevant actions. If not, they are likely to find themselves in deep trouble.

Learn more about, discuss and collaborate on controls monitoring and risk management in the Knowledge Center.

www.isaca.org/knowledgecenter
Quiz #143

Based on Volume 2, 2012—Extended Enterprise

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

TRUE OR FALSE

SINGLETON ARTICLE

1. Most ad hoc transfers, be they system-to-system or person-to-person, tend to need a user interface that is simple to use to minimize transfer risks.

2. Full duplex is a methodology that echoes the data received back to the sending computer, which then checks those data against the original to make sure that the data received at the other end match the data that were sent, ensuring that no bits were distorted during transmission.

3. A cyber audit trail associated with a data transfer would not capture important information, such as what data structure (e.g., xls, csv, txt, xml) was used.

PIRONTI ARTICLE

4. A 2008 IDC study found that the majority of senior managers surveyed believed that IT security risk is the largest single obstacle to innovation in their businesses.

5. When creating a risk-conscious and security-aware culture, it is important to resist the temptation to use techniques such as threat and vulnerability analysis to provide information about the probability and business impact of attack scenarios.

6. By implementing controls and capabilities that are designed to protect the information infrastructure and data assets from their users, organizations may actually alienate these same users and make them feel untrusted.

7. One of the key components of any threat and vulnerability analysis capability is threat intelligence. It is essential to have accurate and credible intelligence to be able to project the likelihood and business impacts of threats. Multiple sources of intelligence should be used to produce confidence in the credibility of data.

TRULL ARTICLE

8. Covert penetration tests test every security control, identify each vulnerability and assess all systems within an organization.

9. A drawback to an overt penetration test is that it does not fully demonstrate the real-life impact an organization would sustain if it were to fall victim to a hacker. As a result, high-ranking decision makers may not fully appreciate the potential business implications of ignoring IT security vulnerabilities.

10. To be successful, a large-scale, covert penetration should be conducted by business users who will be responsible for remediating any vulnerabilities.

GELBSTEIN ARTICLE

11. The benefits of reasons for adopting and adapting the Risk IT framework for business continuity managers include better understanding of how to identify and manage IT risk and of how to communicate IT risk to business decision makers.

12. Regardless of the route through which the policies are developed, to be effective, the policies must be understandable to everyone who needs to comply and must be effectively deployed. Most important, they should be enforceable.

13. The speed of innovation has produced players that are intent on breaking an organization’s protective measures such as malicious software designers working with organized crime.

ANDERSON ARTICLE

14. Records information management (RIM) looks to maximize the disposal of obsolete electronic records to minimize potential e-discovery risk. Information security seeks to avoid the retention of unnecessary electronic information to mitigate any potential data piracy issues.

15. The optimal way to reduce risk from both RIM and information security perspectives is to ensure that records exist beyond their planned destruction date.

16. Corporate governance boards provide another avenue to develop closer integration between the RIM and information security teams by inclusion of both groups in regular meetings and cross-pollinating project teams among both teams’ members.
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.
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 is 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.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

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

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

The titles of issued standards documents are:

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

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

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

**Standards for Information System Control Professionals** Effective 1 September 1999
- S10 Statement of Scope
- S10.01 Responsibility, Authority and Accountability
- S10.02 Independent
- S10.03 Professional Independence
- S10.04 Organisational Independence
- S10.05 Professional Ethics and Standards
- S10.06 Code of Professional Ethics
- S10.07 Due Professional Care
- S10.08 Competence
- S10.09 Skills and Knowledge
- S10.10 Continuing Professional Education
- S10.11 Planning
- S10.12 Control Planning
- S10.13 Performance of Work
- S10.14 Supervision
- S10.15 Evidence
- S10.16 Effectiveness
- S10.17 Reporting
- S10.18 Periodic Reporting
- S10.19 Follow-up Activities
- S10.20 Follow-up

**Code of Professional Ethics** Effective 1 January 2011
Leaders and Supporters

Editor
Deborah Vohasek
Senior Editorial Manager
Jennifer Hajigeorgiou
publication@isaca.org

Contributing Editors
Sally Chan, CGEIT, CMA, ACIS
Kamal Khan, CISA, CISSP, CITP, MBCS
Vasant Raval, DBA, CISA
Steven J. Ross, CISA, CBCP, CISSP
Tommie Singleton, Ph.D., CISA, CMA, CPA, CITP
B. Ganapathi Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCISA, BS 7799 LA
Smrita Totade, Ph.D., CISA, CISM, CGEIT, CRISC

Advertising
The YGS Group
media@isaca.org

Media Relations
news@isaca.org

Editorial Reviewers
Matt Altman, CISA, CISM, CGEIT, CRISC
Brian Barnier, CISA, CGEIT, CRISC
Linda Betz, CISA
Pascal A. Bizarro, CISA
Jerome Capirossi, CISA
Cassandra Chasnis, CISA
Joao Coelho, CISA, CGEIT
Reynaldo J. de la Fuente, CISA, CISM, CGEIT
Christos Dimitriadis, Ph.D., CISA, CISocusing
Joao Coelho, CISA, CGEIT
Reynaldo J. de la Fuente, CISA, CISM, CGEIT
Christos Dimitriadis, Ph.D., CISA, CISM, CRISC
Ken Doughty, CISA, CRISC, CBCP
Ross Dworman, CISM, GSLC
Robert Findlay
Sailesh Gadia, CISA
Anuj Goel, Ph.D., CISA, CISM, CRISC, CISSP
Manish Gupta, CISA, CISM, CISSP, CSSP
Jeffrey Hare, CISA, CPA, CIA
Francisco Igual, CISA, CGEIT, CISSP
Khawaja Faisal Javed, CISA, CRISC, CBCP
José LSMA
Romulo Lompante, CISA, CGEIT, CRISC
Juan Macias, CISA, CRISC
Norman Marks
David Earl Mills, CISA, CGEIT, CRISC, MCSE
Robert Moeller, CISA, CISSP, CPA, CSQE
Aureo Monteiro Tavares Da Silva, CISM, CGEIT
Muthoni Mutonyi, CISA
Gretchen Myers, CISSP
Mathew Nicho, CEH, RWS, SAP
Daniel Paula, CISA, CRISC, CISSP, PMP
Pak Luk Pooh, Ph.D., CISA, CSQA, MIEEE
John Pouey, CISA, CISM, CRISC, CIA
Steve Primost, CISM
Panavithi Ramesh, CISA, CA
Vasant Raval, DBA, CISA
David Ramirez, CISA, CISM
Ron Roy, CISA, CRP
Venkateshwaran Setty, CISA
Johannes Tekle, CISA, CFSA, CIA
Iljja Vadjoan, CISA
Ellis Wong, CISA, CRISC, CFE, CISSP

ISACA Board of Directors
(2012–2013)
International President
Greg Grocholski, CISA
Vice President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA, CISSP
Vice President
Juan Luis Canselle, CISA, CGEIT, CRISC
Vice President
Ramoses Gallego, CISM, CGEIT, CISSP, SCPM, 6 Sigma
Vice President
Tony Hayes, CGEIT
Vice President
Marc Vaclav, CISA, CISM, CGEIT, CISSP
Past International President, 2011–2012
Kenneth L. Vander Wal, CISA, CPA
Past International President, 2009–2011
Emil G. D’Angelo, CISA, CISM
Director
John Ho Chi, CISA, CISM, CRISC
Director
Kysten McCabe, CISA
Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC
Chief Executive Officer
Susan M. Caldwell

Subscriptions:
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
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

**COBIT**

**COBIT 5 for Information Security**
2012, 220 pages—**CB5IS**

- **Member**: $35.00
- **Nonmember**: $75.00

**2012, 220 pages—**WCB5IS

- **E-book—PDF Format (purchase online only)**
- **Member**: $35.00
- **Nonmember**: $75.00

**IT Governance and Business Management**

**Ethics in Information Technology, 4th Edition**
2012, 480 pages—**13-IT**

- **Member**: $91.00
- **Nonmember**: $101.00

**Featured...**

www.isaca.org/featuredbooks

**Cybersecurity: The Essential Body of Knowledge**

**Code 10-IT**

- **Member**: $81.00
- **Nonmember**: $91.00

**IT Audit, Control and Security**

**Code 90-WACS**

- **Member**: $85.00
- **Nonmember**: $95.00

**COBIT 5: Enabling Processes**

**Code CB5EP**

- **Member**: $35.00
- **Nonmember**: $135.00

**Securing the Clicks: Network Security in the Age of Social Media**

**Code 27-MSC**

- **Member**: $40.00
- **Nonmember**: $50.00

**IT Project Management: 30 Steps to Success**

**Code 12-ITPM**

- **Member**: $20.00
- **Nonmember**: $30.00

**Protecting Industrial Control Systems from Electronic Threats**

**Code 1-MPPI**

- **Member**: $80.00
- **Nonmember**: $90.00

**The Operational Risk Handbook for Financial Companies**

**Code 1-HHOP**

- **Member**: $80.00
- **Nonmember**: $90.00

**Security, Audit and Control Features Oracle PeopleSoft, 3rd Edition**

**Code ISPS3**

- **Member**: $65.00
- **Nonmember**: $80.00

**2012 CISA/CISM/COSO/CRISC Study Aids**

*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 BOOKS  www.isaca.org/newbooks

**COBIT 5® for Information Security**

COBIT® 5 for Information Security is a COBIT 5 Professional Guide. It examines COBIT 5 from a security view, placing a security lens over the concepts, enablers and principles within COBIT 5. Appendix B, Detailed Guidance: Processes Enabler is presented in the same format as the tables in COBIT 5: Enabling Processes and provides security-specific process goals and metrics, inputs/outputs, and activities. COBIT 5 for Information Security is intended for all stakeholders in the enterprise because information security is the responsibility of all enterprise stakeholders. Using it can result in enterprise benefits such as improved risk decisions and cost management related to the information security function.

COBIT 5 for Information Security aims to be an ‘umbrella’ framework to connect to other information security frameworks, good practices and standards. It describes the pervasiveness of information security throughout the enterprise and provides an overarching framework of enablers. The relevant information security frameworks, good practices and standards need to be adapted to suit specific requirements of the enterprise’s specific environment. The reader can then decide, based on the specific needs of the enterprise, which framework or combination of frameworks is best to use, also taking into account the legacy situation in the enterprise, the availability of the framework and other factors. For this, the mapping of COBIT 5 for Information Security to related standards in appendix H will help find a suitable framework according to relevant needs.

2012, 220 pages. **CBSIS**  
Member $35.00  |  Nonmember $175.00

2012, 528 pages. **WCBSIS—E-BOOK—PDF FORMAT**  
Member $155.00  |  Nonmember $165.00

**Ethics in Information Technology, 4th Edition**

George Reynolds

The latest edition of this dynamic text provides the most up-to-date, thorough coverage of newsworthy technology developments and their impact on business today. Examine issues surrounding professional codes of ethics, file sharing, and infringement of intellectual property, security risk assessment, Internet crime, identity theft, employee surveillance, privacy, compliance, social networking, and the ethics of IT corporations. This book offers an excellent foundation in ethical decision-making for current and future business managers and IT professionals. *Ethics in Information Technology, 4th Edition* provides thorough coverage focused on preparing the individuals who are primarily responsible for addressing ethical issues in today’s workplace. Future business managers and IT professionals learn how to examine the various ethical situations that typically arise in IT and gain experience from the book’s practical advice for addressing the issues. Up-to-the-minute business vignettes and thought-provoking questions challenge the readers’ knowledge; while features focused on decision making, such as this edition’s updated Manager’s Checklists, provide brief, critical points to consider to making key business decisions.

2012, 480 pages. **13-IT**  
Member $91.00  |  Nonmember $101.00

**FISMA Principles and Best Practices: Beyond Compliance**

Patrick D. Howard

While many agencies struggle to comply with Federal Information Security Management Act (FISMA) regulations, those that have embraced its requirements have found that their comprehensive and flexible nature provides a sound security risk management framework for the implementation of essential system security controls. Detailing a proven approach for establishing and implementing a comprehensive information security program, *FISMA Principles and Best Practices: Beyond Compliance* integrates compliance review, technical monitoring, and remediation efforts to explain how to achieve and maintain compliance with FISMA requirements.

Clarifying exactly what it takes to gain and maintain FISMA compliance, the author provides detailed guidelines so you can design and staff a compliance capability, build organizational relationships, gain management support, and integrate compliance into the system development life cycle. While there is no such thing as absolute protection, this up-to-date resource reflects the important security concepts and ideas for addressing information security requirements mandated for government agencies and companies subject to these standards.

2011, 345 pages. **S3-CRC**  
Member $80.00  |  Nonmember $90.00

* 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
Guide to Firewalls and VPNs, 3rd Edition
Michael E. Whitman, Herbert J. Mattord, Andrew Green

Firewalls are among the best-known network security tools in use today, and their critical role in information security continues to grow. However, firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection systems, and related tools. Guide to Firewalls and VPNs, 3rd Edition explores firewalls in the context of these critical elements, providing an in-depth guide that focuses on both managerial and technical aspects of security. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The text also features an abundant selection of realistic projects and cases incorporating cutting-edge technology and current trends, giving readers the opportunity to hone and apply the knowledge and skills they will need as working professionals. Guide to Firewalls and VPNs includes new and updated cases and projects, enhanced coverage of network security and VPNs, and information on relevant National Institute of Standards and Technology guidelines used by businesses and information technology professionals.

2012, 528 pages. 11-IT
Member $155.00 | Nonmember $165.00

Handbook for Internal Auditors
Matthew Bender

Handbook for Internal Auditors provides guidance on every aspect of internal auditing from establishing and managing an internal auditing function within an organization to performing audit fieldwork and addressing governance issues for the organization. It contains checklists, flowcharts, exhibits, sample forms, and complete audit programs. The scope of coverage includes practical advice on effective governance and policy management; maintaining an effective systems of internal controls and performing audit assessments of internal controls effectiveness; quality management and quality control reviews; procedures for implementing and performing IS general, technical, and application reviews; tools used by auditors, the tools used throughout the organization for management and control; and the existing and emerging practices for effective internal auditing. Included with this title is a CD-ROM containing interactive checklists and audit programs that can easily be customized to fit any entity’s business environment.

2011, 2 volumes. 1-LN
Member $619.00 | Nonmember $629.00

Michael E. Whitman, Herbert J. Mattord

Principles of Information Security, 4th Edition explores the field of information security and assurance with updated content including new innovations in technology and methodologies. Readers will revel in the comprehensive coverage that includes a historical overview of information security, discussions on risk management and security technology, current certification information, and more. The text builds on internationally-recognized standards and bodies of knowledge to provide the knowledge and skills students need for their future roles as business decision-makers. Information security in the modern organization is a management issues which technology alone cannot answer; it is a problem that has important economic consequences for which management will be held accountable. Readers can feel confident that they are using a standards-based, content-driven resource to prepare for their work in the field.

2012, 656 pages. 12-IT
Member $142.00 | Nonmember $152.00

* 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
### 2012 CISA® EXAM REFERENCE MATERIALS

To prepare for the December 2012 CISA exam, order:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSM-12</td>
<td>English Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CSM-12C</td>
<td>Chinese Simplified Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CSM-12F</td>
<td>French Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CSM-12I</td>
<td>Italian Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CSM-12J</td>
<td>Japanese Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CSM-12S</td>
<td>Spanish Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
</tbody>
</table>

### 2012 CISM® EXAM REFERENCE MATERIALS

To prepare for the December 2012 CISM exam, order:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMI-12</td>
<td>English Edition</td>
<td>$115.00</td>
<td>$85.00</td>
</tr>
<tr>
<td>CMI-12J</td>
<td>Japanese Edition</td>
<td>$115.00</td>
<td>$85.00</td>
</tr>
<tr>
<td>CMI-12S</td>
<td>Spanish Edition</td>
<td>$115.00</td>
<td>$85.00</td>
</tr>
</tbody>
</table>

### 2012 CGEIT EXAM REFERENCE MATERIALS

To prepare for the December 2012 CGEIT exam, order:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGM-12</td>
<td>CGEIT Review Manual 2012</td>
<td>$115.00</td>
<td>$85.00</td>
</tr>
<tr>
<td>CGM-12S*</td>
<td>CGEIT Review Questions, Answers &amp; Explanations Manual 2012 Supplement</td>
<td>$60.00</td>
<td>$40.00</td>
</tr>
<tr>
<td>CGM-11*</td>
<td>CGEIT Review Questions, Answers &amp; Explanations Manual 2011 (90 Questions)</td>
<td>$60.00</td>
<td>$40.00</td>
</tr>
</tbody>
</table>

### 2012 CRISC EXAM REFERENCE MATERIALS

To prepare for the December 2012 CRISC exam, order:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPR-12</td>
<td>CRISC Review Manual 2012</td>
<td>$115.00</td>
<td>$85.00</td>
</tr>
<tr>
<td>CPR-12S*</td>
<td>CRISC Review Questions, Answers &amp; Explanations Manual 2012 Supplement (100 Questions)</td>
<td>$60.00</td>
<td>$40.00</td>
</tr>
<tr>
<td>CPR-11*</td>
<td>CRISC Review Questions, Answers &amp; Explanations Manual 2011 (100 Questions)</td>
<td>$60.00</td>
<td>$40.00</td>
</tr>
<tr>
<td>CCR-12</td>
<td>Candidate's Guide to the CRISC Exam and Certification</td>
<td>$15.00</td>
<td>$5.00</td>
</tr>
</tbody>
</table>

### 2012 COBIT® EXAM REFERENCE MATERIALS

To prepare for the December 2012 COBIT exam, order:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CB4.1*</td>
<td>COBIT 4.1, Print Format</td>
<td>$190.00</td>
<td>$75.00</td>
</tr>
<tr>
<td>CB5*</td>
<td>COBIT 5</td>
<td>$50.00</td>
<td>$35.00</td>
</tr>
</tbody>
</table>

### COBIT 5: Enabling Processes

- **WCB5EP**: E-book—PDF format (purchase online only) $150.00 FREE
- **CBS5**: Print format $135.00 FREE

### COBIT 5 Implementation

- **WCB5IM**: E-book—PDF format (purchase online only) $150.00 FREE
- **CBS5**: Print format $135.00 FREE

### COBIT for Information Security

- **WCB5IS**: E-book—PDF format (purchase online only) $175.00 FREE
- **CBS5**: Print format $175.00 FREE

### COBIT and Application Controls: A Management Guide

- **WCBAC**: E-book—PDF format (purchase online only) $55.00 FREE
- **CBSAC**: Print format $35.00 FREE

### COBIT Self-assessment Guide: Using COBIT 4.1

- **WCBO**: E-book—PDF format (purchase online only) $30.00 FREE
- **CBSO**: Print format $20.00 FREE

### COBIT Process Assessment Model (PAM): Using COBIT 4.1

- **WCOPAM**: E-book—PDF format (purchase online only) $40.00 FREE
- **CPAM**: Print format $50.00 FREE

### COBIT User Guide for Service Managers

- **WCBUS**: E-book—PDF format (purchase online only) $35.00 FREE
- **CBSU**: Print format $20.00 FREE
- **CB4**: IT Assurance Guide: Using COBIT 4 $165.00 $55.00
- **CBIT**: Implementing and Continuously Improving IT Governance $115.00 $55.00

### COBIT Online 4.1

- **ICOLB**: Annual Full Subscription + Benchmarking (purchase online at www.isaca.org/cobitoline) $400.00 $200.00
- **ICOB**: ISACA members SAVE 75% $50.00

Visit www.isaca.org/cobitoline for additional information.

### COBIT Mappings

- **WCCM**: Mapping of CMMI for Development V1.2 With COBIT 4.0 $25.00 FREE
- **WCMSO**: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0 $25.00 FREE
- **WCMIT**: Mapping of ITIL V3 With COBIT 4.1 $25.00 FREE
- **WCMN5T**: Mapping of NIST SP800-53 Rev 1 With COBIT 4.1 $25.00 FREE
- **WCPMB**: Mapping of PMBOK to COBIT 4.0 $25.00 FREE
- **WCMSF**: Mapping of SET’s CMM for Software to COBIT 4.0 $25.00 FREE
- **WCMTC**: Mapping of TOGAF 8.1 With COBIT 4.0 $40.00 FREE
- **WCMFF**: Mapping of FLEC with COBIT 4.1 $25.00 FREE
- **WCM2000**: Mapping of ISO/IEC 20000 With COBIT 4.1 $25.00 FREE
- **WCMCM2**: Mapping of COBIT 4.0 With COBIT 4.1 $25.00 FREE

Sets of related COBIT products focusing on your professional needs are available—purchase a focus set and save! See www.isaca.org/cobitolines 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/cobitoline for descriptions and pricing)

See [NON-ENGLISH RESOURCES](#) for additional COBIT material.

### Enterprise Value:

**Governing IT Investments**

- **VITM**: Getting Started With Valuation Management $40.00 $25.00
- **VITF**: The Val IT Framework 2.0 $90.00 $45.00
- **VITB**: The Business Case Guide—Using Val IT 2.0 $40.00 $25.00
- **VITG**: Value Management Guidance for Assurance Professionals—Using Val IT 2.0 $40.00 $25.00
- **VITIS**: Complete Set $185.00 $105.00

**39-ERC**: The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results $86.00 $76.00

**5-RO**: A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance $105.00 $95.00
**INTERNET AND RELATED SECURITY TOPICS (cont.)**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-HA</td>
<td>Scrapy Information Security: The Easy Way to Keep the Cyber Wolves at Bay</td>
<td>30.00</td>
<td>20.00</td>
</tr>
<tr>
<td>3-CRC</td>
<td>Implementing Information Security Policies</td>
<td>100.00</td>
<td>90.00</td>
</tr>
<tr>
<td>24-MSEM</td>
<td>Security Information and Event Management (SIEM) Implementation</td>
<td>75.00</td>
<td>65.00</td>
</tr>
<tr>
<td>27-MSC</td>
<td>Securing the Clicks: Network Security in the Age of Social Media</td>
<td>50.00</td>
<td>40.00</td>
</tr>
<tr>
<td>1-GSM</td>
<td>Security Monitoring</td>
<td>55.00</td>
<td>45.00</td>
</tr>
<tr>
<td>2-BJSF</td>
<td>System Forensics, Investigation, and Response</td>
<td>100.00</td>
<td>90.00</td>
</tr>
</tbody>
</table>

**Governing and Business Management**

- **94-WIFRS**: An Executive Guide to FRPs: Content, Costs and Benefits to Business
- **3-PAGE**: 7 Steps to Better Written Policies and Procedures
- **4-PAGE**: Best Practices in Policies and Procedures
- **1-ITG**: Board Briefing on IT Governance, 2nd Edition
- **6-SYN**: Business Continuity and Disaster Recovery Planning
- **BMIS**: The Business Model for Information Security
- **42-CRC**: Creating a Culture of Security (e-book)
- **32-CRC**: Crisis Management and Operations
- **11-ITDG**: The Data Governance Imperative
- **37-CRC**: Digital Privacy: Theory, Techniques, and Practices
- **89-WEG**: Empowering Green Initiatives with IT: A Strategy and Implementation Guide
- **9-ART**: Enterprise Information Security and Privacy
- **1-CMP**: Enterprise Security Architecture: A Business-Driven Approach
- **13-IT**: Ethics in Information Technology, 4th Edition
- **23-WIT**: The Executive’s Guide to Information Technology, 2nd Edition
- **10-VR**: Foundational IT Management Based on ITIL® V3
- **3-VH**: Frameworks for IT Management
- **85-WF101**: Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition
- **64-WGRC**: Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Governance and Best Practices
- **42-CRC**: The Green and Virtual Data Center
- **7-ITR**: Green IT in Practice, 2nd Edition
- **20-MHE**: Hacking Exposed Malware and Rootkits: Malware & Rootkits Secrets & Solutions
- **67-WHF**: Human Factors in Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation
- **1-IBM**: The IBM Data Governance Unified Process
- **W0GALS**: Identifying and Aligning Business Goals and IT Goals
- **4-ID**: Implementing Information Technology Governance: Models, Practices and Cases
- **46-CRC**: Implementing the Project Management Balanced Scorecard
- **19-TSSQ**: Implementing Service Quality Based on ISO/IEC 20000
- **29-CRC**: Information Security: Design, Implementation, Measurement and Compliance

---

**SUPPLEMENT**

**RETURN POLICY**

All purchases are final. No refunds or exchanges.

**PUBLICATION QUANTITY DISCOUNTS**

A cademic and bulk discounts are available on books published by the ISA CA 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.

---

**FOUR EASY WAYS TO PLACE AN ORDER:**

- **Order online at www.isaca.org/bookstore**
- **Call toll-free at 1-847-253-1443**
- **Fax order at 1-847-660-5650**
- **Send electronic payments in US dollars to: Bank of America, ABA #0260-0959-3, ISA CA Account #22-71578, S.W.I.F.T. code BOFAUS3N**
Customer Order Form

Order Online at www.isaca.org/bookstore

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/Postal Code ________________
Phone Number ( ) ________________________________
Fax Number ( ) ________________________________
E-mail Address _______________________________________

Shipping Information  (If different from customer information)
If shipping to a P.O. Box, please include street address to ensure proper delivery.

Name ____________________________________________
FIRST MIDDLE LAST/FAMILY
Company Name ________________________________________
Address: (If Part of Shipping Address) __________________________
City __________________________ State/Province ________________
Country ______________________ Zip/Postal Code ________________
Phone Number ( ) ________________________________
E-mail Address _______________________________________

Code | Title/Item | Quantity | Unit Price | Total
---|-----------|----------|------------|--------

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

Payment Information—Prepayment Required

☐ Payment enclosed. Check payable to “ISACA” in US dollars, drawn on US bank.
☐ Bank wire transfer in US dollars. Date of transfer __________________________
☐ Charge to ☐ Visa  ☐ MasterCard  ☐ American Express  ☐ Discover
Credit Card #: __________________________
Exp. Date __________________________
Print Cardholder Name __________________________
Signature __________________________

Payment Information—Prepayment Required

Shipping & Handling Rates for Orders

For Orders Totaling
Up to US $30.00 outside US US $10.00 US $0.00
US $30.01 to US $50.00 outside US US $15.00 US $0.00
US $50.01 to US $80.00 outside US US $20.00 US $0.00
US $80.01 to US $150.00 outside US US $26.00 US $0.00
Over US $150.00 outside US US $32.00 US $0.00

No shipping charges apply to MyISACA (CA) or MyISACA (JP).
No shipping charges apply to CSQ Practice Question Database v1.2—download.
No shipping charges apply to CSQ Practice Question Database v12—download.

All orders outside the US are shipped Federal Express Priority.

Sales Tax: Add sales tax if shipping to:
Louisiana (LA)—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.

Subtotal __________________________

Sales Tax: __________________________
CDC Required: __________________________
For all orders please include shipping and handling charge—see chart below.

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.
Registration now open!

Exam Date: 8 December 2012
Registration Deadline: 3 October 2012

ISACA members save US $150 off registration

www.isaca.org/certification
Integrate and report all your GRC data from one place:
- Data Warehouse in weeks
- Data model integrating AdaptiveGRC suite data and open to your existing data sources
- Appealing BI reporting with newest technologies
- Agile teams adopting solutions to your custom requirements.

Web: candf.pl
E: adaptive@candf.pl
T: +44 207 022 4884 (UK)
T: +48 22 898 72 66 (Poland)
Customer Friendly Sp. z o.o. S.K.A.