Privacy and the Cloud

Featured articles:

Social Networks and Privacy—Threats and Protection
Meeting PCI DSS When Using a Cloud Service Provider
Cloud Risk—10 Principles and a Framework for Assessment
And more...
2012 ISACA

Member Get A Member

When ISACA grows, members benefit. More recruits mean more networking, more connections, more resources, and more chances to win valuable prizes!

Connect
For each new member who credits you as their recruiter (by entering your ID#), you are entered to win one of our Monthly Prizes. Plus, a Top Recruiter Grand Prize will be awarded to the individual who recruits the most new full-dues paying* members to ISACA.

Winners will have the opportunity to receive global recognition in @AGlance and on the ISACA website for encouraging colleagues to join ISACA.

Recruit
- Colleagues or new college graduates invested in professional growth
- Someone interested in taking a CISA®, CISM®, CGEIT® or CRISC™ exam
- A full-time student majoring in fields including: information systems, business administration, accounting, information technology, engineering, computer science

* Full-dues includes US $135 ISACA International dues, plus chapter dues if applicable.

TO LEARN MORE
Contact mgam@isaca.org or visit www.isaca.org/mgam.

© 2012 ISACA. All Rights Reserved

Win!

GRAND PRIZE
The Top Recruiter will receive either a 2013 ISACA conference or exam registration plus travel expenses or study materials (maximum value US $1500). Winner will be awarded in January 2013.

MONTHLY PRIZE DRAWINGS
Monthly Prize Winners will be announced from August — December 2012.

One Professional Member and one Student member who have recruited at least one new Member during each month will be eligible to receive a prize (value US $50). There will be two winners each month.
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.

**MASTERS DEGREE**
- Two year program
- Specialize in cybersecurity or policy management

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

The curriculum is modeled on the guidelines and recommendations provided by:
- The Committee on National Security Systems (CNSS) 4000 training standards
- The (ISC)² Ten Domains of Knowledge
- ISACA

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

**The program can be taken on campus or completely online**
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.

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

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

- An Introduction to Crisis Management
  Haris Hamidovic, CIA, ISMS IA, ITIL, IT Project+

- Identity Mining and Insider Threat Monitoring
  Simon Moffatt, CISA, CISSP, MBCS

- Réseaux Sociaux et Vie Privée: Menaces et Protections
  Guy-Hermann Ngambeke Ndiandukue, CISA, CISM, CRISC, ITIL V3(f), PMP

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

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

Follow ISACA on Twitter: http://twitter.com/isacanews; Hashtag: #ISACAJournal

Join ISACA LinkedIn: ISACA (Official), http://linkd.in/ISACAOfficial

Like ISACA on Facebook: www.facebook.com/ISACAHQ
ID Yourself as an IT Expert.

Prepare for Industry Certification
100% Online!

Advance Your Career With a Master Certificate From Top-Ranked Villanova University

With network security, software quality and other business-critical projects at stake, employers require their IT teams to possess the most current, comprehensive knowledge. Start obtaining the skills you need to thrive in this fast-paced field with 100% online master certificate programs from Villanova, ranked by U.S. News & World Report as the #1 Regional University in the North for nearly two decades.

Increase Your Expertise — and Salary Potential

Villanova’s multi-course, video-based programs help you to gain news skills in some of today’s most in-demand disciplines:

- Project Management
- Lean Six Sigma
- Business Analysis
- Business Intelligence
- IS Security
- Software Testing
- IT Service Management/ITIL®
- And more

Each program can prepare you to earn industry certification – including PMP®, CAPM®, CBAP™, CISSP®, Security+™, CTFL and ITIL® v3 Foundation – increasing your expertise and your salary potential.

Discover New Methodologies and Technologies That are Changing Business — and the World.

You can make yourself more valuable by possessing skills that are in-demand and making a difference:

- General Electric realized an estimated $10 billion in benefits during its first five years of Six Sigma implementation – iSixSigma.com, What is Six Sigma, 2010
- Seven out of 10 companies use formal project management methodologies – Information Week, Project Management is Finally Getting Real Respect, 2010
- Projected national employment growth for business analysts is expected to grow 29% through 2016 – CNN Money, Best Jobs in America, 2010
- Total U.S. economic costs of insecure software is $180 billion per year – CNET News, Software Interrupted, 2008

Get Your Career-Building Credentials!
Call or go online today for more information:
877-553-5976 | VillanovaU.com/ITExpert

© 2012 All Rights Reserved. Made Available by University Alliance® – The Nation’s Leading Universities Online. SC: 197265v1 | MCID: 20138
PMP® and CAPM® are Registered Marks of the Project Management Institute, Inc.
In a recent meeting, the question being debated was whether there were situations in which the security of information could be prudently reduced. If an organization has established a security posture of X, is there any justification for anything less than X? In other words, is security a monolithic wall—a continuous barrier against misuse of information resources at all times? Or, is it a flexible doorway that can be opened or closed in different ways in different circumstances? The participants in the meeting fell into two camps. The issue became focused on emergencies; some felt that a willingness to lower the security threshold is an invitation to hackers to create a crisis and then exploit the breach in the wall to misuse the information (i.e., to take something of value). Some among them felt that an emergency calls for a higher level of security. The other camp (okay, I was the other camp) thought that there are justifications for less security when the risk of keeping the wall intact is outweighed by that of lowering it.

Now, as a committed information security professional, I am not in the habit of advocating less security. At the same time, I am in favor of organizations having the security they need, not less…but not more, either. Thus, the issue is whether an emergency changes the need for security, and if so, does a crisis raise or lower the requirements? Which in turn raises some questions: What is an emergency? And, existentially, what is security?

DATA PROTECTION AND ACCESS CONTROL
Let me tackle the second question first. Security is derived from the object (the information, in this case) and the subject (the person or system using it). Information security consists of protecting the actual contents of an information medium (e.g., electronic, paper, voice) and controlling access to it. In the first instance, the contents can be secured through encryption, retention and disposal processes, lockboxes, and other means of making certain that information cannot be read, changed or destroyed. I cannot see any circumstances in which these controls should be eliminated. And since they are rather binary in nature—data are either encrypted or they are not—once it is determined that information must be protected, the controls must stay in place at all times. There is no justification for reduced security; no purpose is served cutting back 256-bit encryption to 128-bit in an emergency.

But, access control maps people to functions and functions to information, or at least a subset of an organization’s overall information resources. Here I see room for judgment and nuanced responses to changing situations. Some functions may well require access to certain information in different ways and to different extents; by association, the people in those functions will need access other than that which they usually have. Therein lies the need to define appropriate responses to different types of emergencies.

There are different sorts of emergencies, ranging from the problematic to the catastrophic, so some calibration is required. For the present purposes, I distinguish between emergencies, which require immediate action to prevent short-term, bounded repercussions and disasters, which are caused by the loss of critical resources without which there are long-term, unbounded consequences.

EMERGENCIES
One person’s emergency is another’s operational hiccup. The common element is that action must be taken to prevent a bad result, such as financial penalties, lost opportunities or damaged reputation. The action is known (or knowable) and the result of not taking that action is calculable. Thus, for example, in many systems in the financial services industry, there is a need for trades and transfers to be entered by one person, executed by another and approved by a third before they can be...
released. If they are not released, the institution must pay a percentage of the transaction as a penalty (known as “fails”). If, for example, the system were down for hours during the day and the deadline were approaching, would it be permissible to override the separation of duties and have the transactions released? Could people who are not approvers be granted the short-term ability to perform the approval function? The answer, to my mind, is yes. And, in fact, many transfer systems contain a bulk override provision for such circumstances. Given that some banks deal in billions, the potential of a security breach is overwhelmed by the reality of imminent fines.

For another example, many consulting firms require all reports and proposals to be signed by the partner in charge of the project. This is a major control over the integrity of a firm’s name and it denotes acceptance of the risk associated with the contents of a document. When I was employed by such a firm (and before I had the right to sign my own documents), I admit that I bypassed this security measure when the relevant partner was unavailable and a proposal deadline was minutes away. The risk was marginal and the loss of an opportunity would have been severe.

In both examples, prudence is called for and the person making the decision would face severe repercussions if the action resulted in negative consequences. But, they are reasonable decisions that put human judgment before mechanistic security provisions.

**Disasters**

The disruption of one or more critical resources, be they computers, work spaces, people or telecommunications, can have far-reaching negative impact, including the ultimate disappearance of an organization. With a business’s demise as a potential result, it would be foolish to insist on maintaining security at a high level while the corporate ship sinks beneath the waves. Fortunately, I am unaware of any catastrophe that might have been mitigated by lax security.

Disasters do have a way of changing things. In my experience and that of companies I have researched, many people are suddenly thrust into unaccustomed roles following disastrous events. This shift of responsibilities should be considered and planned for in advance of such incidents. ISO 27002 states: “A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity.” To my mind, this control means that alternative role models should be developed *a priori* for rapid implementation when needed. I realize that some people may disagree and may say that what a person has access to does not change during an event. For them, the same restrictions that were in place during normal operations need to be in place during an event. Since different individuals may be performing tasks beyond their normal responsibilities, a process must be in place to provide them with the needed access. Thus, to my mind, the issue does not concern a modification to security, but merely the timing of it and I suggest that it is better to think about changed roles in advance than to consider them in the midst of chaos.

There is a special case that demands special handling: an emergency caused by a failure of a security system. Sadly, today such incidents must be considered as malicious attacks. Even if it were not caused by a hacker, a failed security system will attract malefactors like piranhas to a roast beef. In my opinion, prudence demands either halting processing on the affected systems or isolating them so that the damage cannot spread. Hawkeyed monitoring for a considerable period of time is necessarily concomitant to the emergency response in this instance.

**Endnotes**

1. That is thousands of millions in the American vernacular. It does not matter what the denomination is; with amounts that large, a lot of money is at stake.
Cloud Storage—Bursting Through the Hype

By now, you have definitely heard: Cloud is clearly the next big thing. But, is it just hype? Do cloud and cloud storage really deliver on the promise of cost savings, faster deployment times, and scalability?

LOOKING CLOSELY AT CLOUD
To understand the value of cloud, you must first understand the technology behind it. A recent article in Forbes reports: “Cloud computing, as defined by the National Institute of Standards and Technology is a model for enabling ‘convenient, on-demand network access to a shared pool of configurable computing resources’.”1

By most reports, cloud goes way beyond an emerging technology trend. What’s actually happening is that the very manner in which companies conduct business is changing: “Cloud computing is often referred to as a technology. However, it is actually a significant shift in the business and economic models for provisioning and consuming IT that can lead to significant cost savings.”2

Simply put, cloud gives companies a way to expand their IT resources without making significant upfront IT capital expenditures. And that’s a good thing, because infrastructures simply cannot keep up with the amount of data being generated. That’s what we found when we dug a little further.

KEEPING UP WITH INFORMATION
Much like data, at DiCicco, Gulman and Company, the digital universe of information is exploding, and there’s simply no place to put it. The vast amount of email, Word documents and spreadsheets that the enterprise encounters is growing so fast, there simply is not enough data storage equipment to house it. Analyst firm, IDC reported that the digital universe of information was expected to reach 2 zettabytes in 2011.3 This is nearly twice the number reported in 2010.

IDC also expects stored data to double every two years: “The amount of data being stored is more than doubling every two years, and could grow 50 times by 2020, showing the need for new ways to manage data and derive value from it…The new survey has serious implications for those who store and manage data.”4

Need some perspective? Well, IDC offers ways to think about 1.8 zettabytes of data in other terms. How about the following:
- Three tweets per minute from every person in the US for 26,976 years
- More than 215 million high-resolution MRI scans per day for everyone in the world
- A pile of data and information 25 times larger than Mt. Fuji

That’s a lot of data. And, DiCicco and Gulman was feeling it and decided that, perhaps, cloud storage was the solution.

CLOUD BY THE NUMBERS
Driven by the explosion of data, the cloud market is responding. Recently, Forrester Research estimated that the cloud computing market will reach US $241 billion by 2020.5 That is an increase of US $200 billion in just 10 years. IDC reports that spending on equipment for both public and private cloud storage systems will hit US $72.9 billion by 2015.6 And looking at the expanding digital universe, it is not hard to see why companies are making the investment.

DiCicco and Gulman knew that there was something there. It knew cloud storage would reduce the need for physical storage. This would mean less capital expenditures and the ability to scale faster, bigger. Businessweek even said that it is time for companies to actually believe in the hype that is cloud storage: “With most emerging technologies, the hype is bigger than the reality. A welcome exception is cloud storage, which is enabling many organizations to achieve major economies of scale and greater control of growing data volumes. Companies of all sizes can reap the benefits of cloud storage.”7

Rico Barrasso is IT manager at DiCicco, Gulman & Company.

Matt Wallace is vice president of marketing, research and development at Venyu.

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:
That sounds great in theory, but does it work in the real world? Could cloud storage really transform DiCicco and Gulman’s business and drive these cost savings? The team at the firm certainly thought so, and set out to try.

A BRIEF HISTORY
Based in Woburn, Massachusetts, USA, DiCicco, Gulman and Company is a public accounting and business advisory firm in New England. With more than 100 employees, it specializes in helping privately held companies become successful.

For years, the firm’s IT environment relied on the tried-and-true physical infrastructure. During that time, it spent a lot of time changing, storing, cataloging and testing tape-based storage. This caused problems for a number of reasons.

First, the IT department is run very lean—with only three employees managing the entire infrastructure. Second, and perhaps more important, were the security and disaster recovery issues. The firm handles sensitive financial information. Critical data of billions of dollars of transactions are regularly stored and managed by the enterprise’s accountants. If any of this information is lost or compromised, it could spell disaster for the enterprise. Just look at the industry in general.

An article in USA Today estimates that US businesses stand to lose more than US $18 billion per year due to data loss. The article also points out that 70 percent of all business people have experienced data loss. This can be due to disk failure, accidental deletion, viruses, data breach or natural disaster. But, it is not just about the direct costs. For most enterprises, every piece of lost data means lost business.

BEGINNING THE JOURNEY
DiCicco and Gulman’s journey to the cloud started several years ago. The enterprise began using electronic documents because they made life easier, but realized a significant strain was placed on storage capacity. Tapes run out, they are hard to restore and they are not very reliable. Additionally, the firm needed to upgrade its backup and disaster recovery planning to meet higher standards for protection. At this point, the enterprise began exploring options for cloud backup.

Not all cloud solutions were created equal.

Immediately, it became apparent that not all cloud solutions were created equal. Technology needed to provide adequate storage capacity, while costs down. After exploring numerous options, Venyu’s cloud-based enterprise backup and storage proved to be the most effective fit to achieve the enterprise’s cost-efficiency and security goals. Venyu’s RestartIT platform can work across Windows, virtualized servers and IBM equipment, allowing companies to put a solid recovery plan in place in the event of a disaster.

CALCULATING RESULTS
The great thing about this project is that it made DiCicco and Gulman’s transition away from tape easy. There was one secure storage device delivered to the facility. The staff loaded the device with the entire contents of the network. This served as the starting point for the backup process.

The team at the firm saw the results of the new cloud storage system right away. Immediately, the team sent gigabytes of highly sensitive encrypted data to the cloud using deduplication and compression to keep costs down. The system eliminated the painful process of keeping up with old tapes—meaning no more digging through boxes of tapes to change, store, catalog and test.

Furthermore, the burden of backup was now eliminated. All backups are automatically created over the Internet and placed into a secure cloud environment using data deduplication. The
process monitors each file, recognizes when it is changed, and only transmits those pieces of the file altered. The enterprise has also placed management of the backup process, including server provisioning, file transfer scheduling and process management, with the web-based Venyu management console.

Finally, there is a disaster recovery plan in place that lets the team sleep at night. The enterprise has weathered a significant number of natural disasters over the years, including hurricanes, ice storms and tornadoes. With an offsite disaster recovery plan in place, the firm can continue its day-to-day operations without worrying about “what if.”

MOVING FORWARD

DiCicco and Gulman’s road to cloud storage was not easy, but it is already saving the enterprise hundreds of hours of manual labor each year. The up-front investment has paid for itself, and now the enterprise can focus on goals more critical to its business. The firm has completely transformed the old backup system into a modern, highly-effective component of its overall disaster recovery strategy.

Cloud-based storage is significantly transforming the manner in which businesses protect, access and restore their critical data and information. Based on our experiences at DiCicco and Gulman, it is a project that should immediately move to the top of any enterprise’s to-do list.

ENDNOTES


2 Ibid.


4 Ibid.


6 Ibid, Kovar


Since COBIT 5 has recently been released, it is timely to look at the threads of information ethics in the fabric of this substantially improved and integrated framework. The approach selected for this review is not an exhaustive analysis of the microcontent of COBIT, but a reflection on three questions for consideration in linking ethics to the expanded reach of COBIT 5.1 A continuing discussion in the comments section of this article (see the QR code below to link directly to the article or visit www.isaca.org/currentissue to navigate to it) would be helpful to exchange ideas and “snowball” our efforts to improve our practices.

WHAT HAS CHANGED FROM COBIT 4.1?
COBIT 5 takes a nested approach. Stakeholder drivers influence stakeholder needs, which cascade to enterprise goals, which in turn cascade to IT-related goals, which ultimately cascade to enabler goals. Enablers include processes, organizational structures and information; for each enabler, a set of specific relevant goals can be defined in support of the IT-related goals.2 The leap from COBIT 4.1 to COBIT 5 is significant in many respects,3 including the recognition of ethics. A search for the word “ethics” shows that the term appeared twice in the former edition compared to 23 times in COBIT 5. This is impressive, especially knowing that the former is 213 pages long and the latter 94 pages. Several of these references surface in the citation of the enabler Culture, Ethics and Behavior. The breakdown of the references to “ethics” is: Table of contents (2), enabler description in the title of a Table/figure or in a list (5), glossary (2), and as a part of the discussion (14). A review of the context where the term was used in the discussion seems to suggest that a conscious effort was made to embed ethics into the overall design.

In COBIT 5, an enabler is defined as anything that can help achieve the objectives of the enterprise.4 Included among the seven categories of enablers is the category that combines Culture, Ethics and Behavior. The ultimate expression of ethics is in the choices we make; therefore, the inclusion of behavior in this category is meaningful. Likewise, culture is a key influencer of the organization’s climate of ethics; consequently, it is appropriate for ethics to be a part of the same family of enablers. However, although somewhat intuitive, it is unclear how these three elements as a unified enabler are related to one other.

COBIT 5 links the enabler Principles, Policies and Frameworks with the enabler Culture, Ethics and Behavior. This is because the former “should reflect the culture and ethical values of the enterprise and they should encourage the desired behavior.”5 As discussed previously in this column (volume 3, 2012), overarching pillars that help set the behavioral expectations include policies and other related elements such as principles, core values and frameworks that should be adopted by the organization. Clearly, the bond between these two enablers has to be strong to set an effective tone to deliver expectations of ethical behavior.

With a detailed description of the enabler Culture, Ethics and Behavior in appendix G, COBIT 5 provides additional insights on ethics. For example, the framework identifies two types of stakeholders—external (e.g., regulators) and internal—and notes personal values of individuals (e.g., employees) and the organizational values mirrored in the organization’s code of ethics. According to COBIT 5, stakes are twofold: Some stakeholders (e.g., remuneration boards and officers) deal with defining, implementing and enforcing desired behaviors, and others have to align with the defined rules and norms. As to a goal related to ethics, the framework posits:

- Organizational ethics, determined by the values by which the enterprise wants to live
- Individual ethics, determined by the personal values of each individual in the enterprise6
While there is a notable effort here to spell out some of the finer points, as with all aspects of COBIT, it is almost always necessary to seek other sources for a serious effort to implement ethics. The context of the nature of the enterprise is referenced in the framework in chapter seven, Implementation Guidance. However, domain-relevant knowledge of ethics and related skills and processes need to be augmented. Understandably, no framework can be considered exhaustive in all aspects of implementation; further mapping of ethics implementation to COBIT should prove helpful to the COBIT user community.

HOW CAN ONE MAP GUIDANCE TO IMPLEMENT ETHICS?
The discussion of enabler 5, Culture, Ethics and Behavior, offers probably the most informative content in respect to the implementation of ethics in an organization.7 The practices noted in this enabler are communication, enforcement, incentives and rewards, awareness, rules and norms, and champions. Although not exhaustive, this list compares well with the other tool kits for ethics implementation.8 For example, the steps identified in the Omaha (Nebraska, USA) Business Ethics Alliance’s tool kit are compared in figure 1 with the specific references in COBIT 5. Many of the 10 steps can be inferred as elements within the interconnected enablers of COBIT 5.

A KPMG white paper, “The Road to a Model Ethics and Compliance Program: Ten Things We Learned on Our Journey,” posted on the ethics alliance site, is an insightful case study in ethics implementation.9

WHAT CAN BE DONE TO ENRICH THE EXISTING KNOWLEDGE BASE?
The knowledge base represented by COBIT 5 is significant.10 Externally, the framework interfaces with myriad standards.11 But knowing this much is not enough; further efforts on how to leverage two or more frameworks and align them to produce synergy for an entity is required. In this area, the user community, by sharing experiences, can help generate a better understanding of inter- and intra-framework implementation challenges and potential synergies in doing so.

ISACA’s Business Model for Information Security™ (BMIS™) provides an excellent supplement to COBIT 5. In reference to ethics, BMIS includes the following statement: “Compliance required at a personal level should be reflected in the Culture DI (dynamic interactions), such as when people are

<table>
<thead>
<tr>
<th>Steps in the Ethics Implementation Tool Kit</th>
<th>Broad Implementation Guidance (COBIT 5, Chapter 7)</th>
<th>COBIT 5 Reference Elsewhere</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Assessment of the organization’s current ethical standing</td>
<td>Need for self-assessment is in the introduction. (35)</td>
<td>Champions are noted as a good practice in enabler 5, Culture, Ethics and Behavior. (79)</td>
</tr>
<tr>
<td>2 High-level responsibility assignment with resources</td>
<td>Key success factors for implementation include top management direction and mandate and visible ongoing commitment and support. (35)</td>
<td>Sole reference in the glossary (90). Rules and norms are noted as a good practice in enabler 5. (79)</td>
</tr>
<tr>
<td>3 Written ethical standards (values statements and code of ethics)</td>
<td>In a general context, training is mentioned in principle 6, Behavior, and in other places. (59)</td>
<td></td>
</tr>
<tr>
<td>4 Ethics training program</td>
<td></td>
<td>Incentives and rewards are noted as a good practice in enabler 5. (79)</td>
</tr>
<tr>
<td>5 Advice mechanisms</td>
<td>No specific match</td>
<td></td>
</tr>
<tr>
<td>6 Employee compensation and evaluation</td>
<td></td>
<td>Enforcement is noted as a good practice in enabler 5. (79)</td>
</tr>
<tr>
<td>7 Hiring and promoting</td>
<td>No specific match</td>
<td></td>
</tr>
<tr>
<td>8 Consistent enforcement</td>
<td></td>
<td>A key reference to evaluate/monitor as a part of the life cycle of the enabler. (79)</td>
</tr>
<tr>
<td>9 Avoiding future violations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Monitoring and auditing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1—Omaha Business Ethics Compared to COBIT 5 Ethics References

(COBIT 5 page number is noted in parentheses.)
expected to make a personal commitment to a code of ethics or other document that mandates personal responsibility and adherence to rules.” BMIS refers to ethics just once. This model articulates six DIs: Governing, Culture, Architecture, Enabling and Support, Emergence, and Human Factors. Interconnected enablers in COBIT 5 and DIs in BMIS seem to overlap in places. For example, the Culture, Ethics and Behavior enabler of COBIT 5 is closely related to the Culture and Human Factor DI of BMIS.

Outside of the basic framework, a considerable amount of space and thought in COBIT 5 is devoted to demonstration by example. The document itself appropriately cautions against mere copying.

Two concrete suggestions are offered for future consideration. First, the term “information ethics” is now widely accepted. Computer and information ethics is a branch of ethics that emerged in the 1980s; it is devoted to the study of social and ethical impact of information and communication technology. It is clear that the term “ethics” encompasses almost everything one refers to in this area; as an all-inclusive term, a generic reference to ethics is appropriate in any framework that includes ethics. However, where specificity would make COBIT 5 more meaningful, it would help to discreetly use “information ethics” in place of “ethics.” While this profession’s interface with business has to do with almost everything that is in the larger nature of ethics, the profession itself is apparently closer to information ethics. Selective usage of “information ethics” will help people relate more effectively to ethical dilemmas closer to the profession.

Second, it would help to review the definition of the term “code of ethics” in COBIT to ensure consistency across the literature and practice of ethics. Specifically, three areas of the current definition warrant a revisit: (1) The use of “employees” is too limiting; ethics is for all stakeholders; (2) the phrase “in certain situations” is probably too prescriptive for a definition; (3) the phrase “those in the enterprise called upon to make decisions” would presumably include everyone. The cleaning crew landing on confidential data is no different from those who draft privacy policies.

The debate will continue. Feedback and improvement are part of the life cycle of any framework. For now, it is time to celebrate the arrival of a new, more inclusive and robust framework that promises to serve the profession and the user community well.

ENDNOTES
1 This is not a comprehensive evaluation of COBIT 5, and the questions relate only to ethics.
2 ISACA, COBIT 5, USA, 2012, www.isaca.org/cobit, p. 18
3 For example, the bridging of governance and management accountabilities
4 Op cit, ISACA, p. 14
5 Op cit, ISACA, p. 68
6 Op cit, ISACA, p. 79
7 Op cit, ISACA, p. 79
8 See, for example, http://businessethicsalliance.org at Creighton University.
10 Refer to COBIT 5, figure 10, p. 25, for an overview.
11 Figure 25 (p. 61) of COBIT 5 is an impressive testimony to this.
13 For a detailed discussion of the history and development of computer and information ethics, refer to http://plato.stanford.edu/entries/ethics-computer/.
What Every IT Auditor Should Know About Auditing Social Media

Social media has taken the planet by storm over the last few years. Much has been said and written about the potential advantages of using social media for business or organizational purposes. Those advantages include, among others, enabling 24/7 communications with customers and prospects; finding, attracting or reaching new customers; building new business opportunities; increasing customer loyalty; diversifying marketing channels; recruiting IT-savvy employees; increasing collaboration among employees; and building personal, professional and organizational networks. One survey found that 40 percent of executives, not the typical users of social media, use social media multiple times a day.1

For example, Ford Fiesta used social network systems (SNS) in the US to generate a mass reach of its target market and to build relationships with customers and potential buyers. Ford achieved reservation to conversion sales rates 10 times higher than expected with SNS. Over 40 million impressions occurred with Twitter, and 30 percent of those were people under 25 (i.e., repeat buyers).2

Facebook is growing by an additional 100 million users every three months since it reached its first 100 million, and is approaching 1 billion users today.3 Twitter has about 140 million members and 340 million tweets are sent per day.4 Businesses use YouTube as a social media and training facility. For example, Red Robin Restaurants offers its training regarding the proper temperature for food as a video online on YouTube, and it is the conventional comedic videos found on YouTube that go viral. There are more than 150 million blogs in existence, and they have millions of followers and readers.5 LinkedIn has 135 million members worldwide and is commonly used by professionals to build networks.6 Other SNS include Xing and Plaxo (similar to LinkedIn), Ning (allows individuals to build a custom SNS), Rediff (India portal), Pinterest (pinning things of interest), and a host of others.

As is true with all IT, social media also brings inherent risk. These risk areas are similar to those brought about by other IT, such as inefficiency, wasted investment, insufficient effectiveness and lost opportunity. But, it also has some unique risk areas, including public image damage created by negative comments and postings in social media venues.

For the purposes of this article, the definition of social media will be “using Internet-based applications or broadcast capabilities to disseminate and/or collaborate on information.”7

A FRAMEWORK FOR AUDITING SOCIAL MEDIA

There are really two different spheres of risk and concern regarding social media: public image and operational effectiveness.

Public image is related to an entity trying to manage and protect its public image. It is quite easy for almost anyone to post something negative and false about an entity. It is vital that entities with social media risk are proactive in their searches for and management of false statements and negative postings on the web.

Like any other IT, the entity’s management should be concerned with the operational effectiveness of using social media tools and, thus, needs to include social media audits in its internal audit function. This audit is not unlike all other audits—beginning with a risk assessment, determining management’s goals (which should be tied back to the business model, goals and objectives of the entity), and auditing for effectiveness and efficiency in using the particular IT.

THE RISK

Figure 1 presents some of the main risk areas when using the framework discussed previously. As can be ascertained, many of the effectiveness/operational risk areas, if they occur, are likely to result in damage to reputation/public image. Those risk areas are probably higher than ones with a single-side impact.

---

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 accountability 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.
Statistics show that, with regard to employees using social media at work, there is considerable risk beyond the risk of lost productivity (see figure 2).

One of the things that makes social media risk different from other IT risk is risk velocity. That is, information spreads extremely quickly across SNS, and transitions to conventional news media, in some cases, within a few minutes of some controversial statement or inappropriate remarks. Thus, the velocity is very quick in SNS, while in other IT arenas, the pace is not quite as fast or broad. Some videos, e.g., Susan Boyle singing on a British TV program, get millions of hits in a very short time; this is described as “going viral”—a now common term in SNS and in general. Going viral is an illustration of the extremely high-risk velocity SNS objects can attain. This is of particular importance in building controls and countermeasures for social media risk and should be factored into the risk assessment of an entity’s social media.

**AUDITING PROACTIVELY FOR IMAGE AND PUBLIC RELATIONS**

The control for reputation and public image risk is to proactively search SNS regularly (risk might require it to be daily) for negative comments and postings, and to have a plan on how to respond to both true negative comments as well as false postings. The main thing is for someone familiar with social media to spend time daily searching the Internet/SNS for damaging posts. To be actively engaged in responding to comments and statements that could adversely affect the organization, this person should be active in all major SNS. While this process/control is not complicated, it is not without substantial costs, as specialists may need to spend all of their work hours on monitoring social media and an enterprise may even require more than one expert. The greater the reputation risk, naturally, the more necessary this kind of audit is.

**AUDITING TRADITIONALLY FOR OPERATIONAL EFFECTIVENESS**

Auditing social media for operational effectiveness is not much different from other IT audits of systems and technologies. What is the risk assessment, in particular the inherent risk? What controls are in place to mitigate the risk, and to what degree do they reduce the inherent risk? The risk areas can be ranked using a combination of impact and probability. In this case, the IT auditor should include the aspect of risk velocity as well. Then, starting with the highest risk, the IT auditor should begin to audit and evaluate the controls.
In addition, the IT auditor should consider what organizational goals and objectives are tied to the use of SNS. Then, the IT auditor should audit the effectiveness of social media compared to a metric or benchmark of the goal, objective or business model. This audit would benefit from the use of the COBIT 4.1 Plan and Organize domain (e.g., PO1 Define a strategic plan, PO3 Determine the technological direction and PO5 Manage the IT investment).

CONCLUSION
The proliferation of social media and the fact that major risk areas are associated with it (whether an organization uses it or not) create a need for IT auditors to assist management in managing the associated risk and making sure that social media is an effective tool. The effectiveness is tied to organizational goals, objectives or strategies (if the entity is actively involved with SNS). A framework for social media is presented in this article, which suggests that the audit of the social media IT (being used by the organization) be separate from the auditing/monitoring of the social media being used (SNS in general).

The audit of the IT (social media) itself is not much different from the approach used in other IT audits, but the risk assessment component has some special considerations (e.g., risk velocity, employee abuse). As usual, COBIT provides an effectual tool to do the audit. Such an audit, as with most IT audits, would involve auditing the controls’ operational effectiveness and the organizational (managerial) strategic effectiveness.

Social media should be proactively monitored to minimize adverse effects of SNS on the organization, especially from false or negative postings. This audit/monitoring increases in importance based on how much the organization is being discussed on SNS, and could require one or more full-time employees spending all of their work hours monitoring the various SNS.

ACKNOWLEDGMENT
The author would like to thank Allen Johnston, Ph.D., and Jamey Worrell, Ph.D., of the University of Alabama at Birmingham for their insights and assistance with this content.
Q What is the difference between information security and cybersecurity? Why is cybersecurity getting so much attention now?

A In reality, not much. Both involve the protection of information and data, but I think it is more of an evolution of terminology than any real significant difference in meaning. Over the years, terms such as information security, computer security, information assurance and, now, cybersecurity have become almost indistinguishable to most people, but they are all essentially about the protection of information or data in a networked environment.

Cybersecurity is getting more attention these days because cyberthreats have grown exponentially over the last several years. Consequently, there is a broader and more significant impact on businesses and consumers today than ever before. Ten years ago, very few people had ever heard the term “spear phishing.” Today, it is a fairly common term and many more people are aware of what it is, have experienced it themselves or have heard about it in the media.

As our level of awareness increases, so does our insight into the cyberthreat landscape. The general public is hearing about these issues much more often these days because it seems as though we read reports almost weekly about data breaches, web site denial-of-service (DoS) attacks, or personal information and credit card numbers being stolen. This increased awareness of cyberthreats and vulnerabilities is responsible for a greater volume of incident reporting, which has, in turn, led to better situational awareness for both government and the private sector.

Q How can the cybersecurity problem be addressed? Is this something for government only or is the involvement of nongovernmental organizations required?

A Defense-in-depth never goes out of style and, as with dressing for cold weather, layers of security provide a better level of fundamental protection than almost anything else. It is not, however, just about better and faster technology or good security hygiene, such as updating your antivirus software and creating a complex password. Good security policies, broad security awareness and robust training programs are critical. And that requires everyone to play a part, including federal, state and local governments; international partners; the private sector; academia; and even the general public.

That said, I believe the federal government plays a particularly critical role in cybersecurity because we have a broad responsibility to understand the cyberthreat landscape and protect our citizens from those dangers that could have an impact on the efficient and effective functioning of our society. DHS has the specific
role of protecting US federal civilian government networks, or the dot-gov domain, but we also work with our private sector partners to secure the nation’s critical infrastructures. This is obviously not something the federal government can do alone. Timely and efficient information sharing is crucial to our efforts where the threats we face across state and international borders and the strategies we take must be collaborative. In our interconnected world, it is more important than ever to foster productive relationships that result in broad information sharing between the public and private sectors.

We have a number of programs and initiatives at DHS that facilitate information sharing and collaboration with the private sector; our federal, state and local government partners; intelligence and law enforcement entities; our international partners; and the general public.

One rapidly maturing and profoundly collaborative effort is our National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC is a national point of operational integration for cyberrelated expertise and collaboration, particularly when developing guidance to mitigate risks and resolve cyberincidents. Members from different private-sector groups work side by side with government professionals and representatives from our intelligence and law enforcement partners on the NCCIC watch floor. This is where the magic of proximity occurs, as information is shared, collaboration ensues, and cyberincidents are acted on with a common understanding and national level of awareness.

We also work closely with government and critical infrastructure entities through the US Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

US-CERT provides actionable cybersecurity information to the public, addresses cyberthreats and develops security responses. The team works to monitor and protect federal civilian agencies on a 24/7/365 basis and, if invited, provides mitigation strategies and advises private-sector companies during incidents. US-CERT can also deploy onsite fly-away teams and make recommendations to improve overall network security if invited by the private sector.

ICS-CERT also provides onsite support to private-sector industrial control systems owners and operators when invited. This support includes protection and response to cyberthreats, including incident response, forensic analysis and site assessments. Industrial control system security is particularly important because of the oftentimes symbiotic relationship between critical infrastructure sectors and their dependence on one another.

In addition to all of our operational cybersecurity activities, DHS is also engaged in national awareness efforts through our “Stop.Think.Connect.” campaign. “Stop.Think.Connect.” is our national public-education campaign designed to increase public understanding of cyberthreats and how to develop safer cyberrelated habits to help make networks and the Internet more secure.

Cybersecurity is a shared responsibility and we all—from the government to the private sector to the individual user—have a role to play.

Q There have been claims that there is a lack of cybersecurity professionals. What new skills are required? Will new positions need to be created?

A It is hard to overstate the growing importance of the cybersecurity professional in today’s society. A technically skilled and cybersavvy workforce with an effective pipeline of future talent is an acknowledged necessity in both the public and private sectors and for continued economic prosperity. The problem is that these truly skilled individuals are not developed in a few weeks or even a few months. It takes years of training and experience to develop true experts, which means we need to identify the talent early, then nurture and cultivate those professionals throughout their educational career and as they move into the workforce. In response to the 2009 Cyberspace Policy Review, the current US administration established the National Initiative for Cybersecurity Education (NICE), distinguishing cybereducation and workforce development as a national priority.

DHS is focused on building a world-class cyberorganization by hiring a diverse group of cybersecurity professionals—computer engineers, scientists and analysts—to secure the US’s digital assets and protect against cyberthreats to our critical infrastructure and key resources. We are recruiting across a technical spectrum that includes people with expertise in cyberincident response, cyberrisk analysis,
vulnerability assessments, intelligence, and networks and systems engineering. Most important, however, are the deep technical skills that come from years of experience or, as we used to say in the Navy, “miles on the dials.”

Building a cybersecurity workforce requires a holistic approach for the education and development for cybersecurity professionals. It is really about making sure that we have a pipeline across the board, starting with awareness and moving forward. It is about ensuring that these professionals are not just educated, but have the true skills that come only with experience.

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

A The two certifications I have—CISM and CISSP—have certainly helped me in my career and I have been selected for jobs that I am pretty convinced I would not have been offered without them. These two particular certifications have provided great opportunities for me.

The greatest value of a security certification, even though they should never be the distinguishing factor of a security professional, is that they can be a true discriminator between equally qualified people. There are a number of security certifications—some that require very little effort and others that require a tremendous amount of study and previous experience. I prefer those certifications that require motivation, discipline and, most important, time to become the expert.

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

A My current role at DHS is easily the biggest personal career challenge that I have faced because of the very broad scope and vast responsibilities of the job. It is not something you can truly prepare for because so many of the daily challenges are unique. I am humbled to work with a wonderful team of dedicated, talented and committed career professionals at DHS, which makes the challenge exciting and worthwhile.

A recurring workplace challenge that I have faced in every one of my CISO and CSO leadership roles over the years is attracting and retaining talented people. There is a lot of competition in both the public and private sector for skilled, technical cyberprofessionals, so finding ways to bring people to government is challenging. It is a bit of a cliché, but... technical people are not always motivated by money. This requires innovative and creative leadership because inspiring and motivating is so personality dependent. People want to be challenged and they want to work in an interesting, rewarding environment where they are valued, so it is my job to create avenues for that to happen...even in government.

I think it is important to recognize that the employment environment for cybersecurity professionals is not static. It is equally as important to accept that individuals will move back and forth between the government and the private sector throughout their careers. I am an example of going from the private sector to state government, back to the private sector and now to federal government, and I encourage it because I believe that the experience is good for the individual, which makes it good for both government and the private sector.

And, that is one of my goals—to make DHS the employer of choice for cybersecurity professionals in the US and a must-stop on the career ladder. We are building a major-league team here that can compete with any organization in the world, public or private, and my goal is to create opportunities to keep that team trained, skilled and, most important, motivated. A big reason that I came to DHS is that I cannot imagine any organization with a more important role, such fascinating challenges and such great responsibility for the security of a nation.
Handbook for Internal Auditors

By Charles H. Le Grand

Reviewed by Horst Karin, Ph.D., CISA, CRISC, CISSP, president of DELTA Information Security Consulting Inc., which provides consulting services in information security and risk management. Karin's advisory services focus on SAP security; governance, risk and compliance; public key infrastructure; WebTrust; and sustainable regulatory compliance. He is the coauthor of SAP Security and Risk Management and chair of the ISACA Publications Subcommittee.

Two volumes, 41 chapters and a CD with ready-to-use forms and checklists presented in two big binders—this is the new 2011 version of the Handbook for Internal Auditors. It is not compact. It is comprehensive and extensive, and qualifies as one of the most useful resources for the internal auditor.

Organizations consider it a must to pass external audits periodically. So how does an organization avoid or minimize the rush and pressure to get things in order before the external auditor begins the review and remain prepared for those audits on an ongoing basis? Ultimately, there should be no rush and no pressure. There should be a controls environment in place that allows an organization to say that it is ready for an audit at anytime.

This is the goal, and the internal auditor and the internal audit department have key roles. Their task is to support management in its responsibility to build a framework of controls for continuous compliance and sustainability. The results of this effort are streamlined, and more efficient processes and cost savings are certainly part of that objective.

For these reasons, internal audit departments are in demand, and management considers the internal auditor a role that enhances operations and meets business objectives. This can be compared, for example, with IT departments, which provide service to the organization, in many cases as a critical backbone for business success. From this point of view, the high expectations organizations have of quality and value delivered by their internal auditors is understandable. Internal auditors need to be prepared and qualified to meet these permanent demands.

The Handbook for Internal Auditors delivers a message for the internal audit function in the 21st century: The old approach of the reactive audit is past. Charles H. Le Grand describes the new audit direction's emphasis on risk assessment, risk management, proactive audit consultation, assurances, guidance in governance and process improvements. For example, the integration of the information systems function, information security and automated controls into the internal audit function and audit programs is addressed throughout.

The Handbook for Internal Auditors delivers essential knowledge, tools and information to develop the audit department, audit skills, judgment and efficiencies in providing the audit service and more. Presenting the handbook in two binders allows it to become a living document that can be updated via subscription or by readers with their own documents and audit programs.

The 41 chapters are structured in five parts. Each chapter starts with a synopsis and includes tables, exhibits, checklists, worksheets and flowcharts. The five parts of every chapter are:

• Auditing standards and emerging best practices
• Establishing the internal auditing department
• Managing the internal auditing department
• Conducting internal audits
• Individual audit work programs

Four of the chapters address audits of information systems and information security. A detailed index simplifies a focused search for keywords. The handbook encompasses the full cycle of the internal audit process, starting with the applicable standards and ethics to the preparation of the audit report and exit conference. The provided audit checklists and programs are very useful as starting points for new auditors or as a reference for experienced auditors who want to compare their own tools with this comprehensive collection of knowledge and experience.

EDITOR’S NOTE
The Handbook for Internal Auditors is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this Journal, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.

Do you have something to say about this article? Visit the Journal pages of the ISACA website (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.
“Broadcast yourself!” YouTube’s slogan alone could summarize the spirit of the social revolution caused by the tidal wave of social networks. These have emerged as one of the main channels of communication on the web: links of all kinds are being forged, developed and broken almost instantly.

According to a study published in France by the French Institute of Public Opinion (IFOP) on social networks, carried out using a sample of 1,002 people aged 18 years and over, 77 percent of Internet users say they are a member of at least one of the online social networks included in the study. These social networks’ notoriety is not simply the result of a mere fad. They allow their members to connect in a useful and enjoyable way by offering a variety of applications and benefits tailored to their target audience. LinkedIn has a huge employment market; for example, Jeff Epstein, chief financial officer of Oracle, was allegedly recruited thanks to his profile on this network.2

However, it would be unrealistic to think that the exponential growth of social networks has only positive effects. Indeed, publication and sharing of personal information exposes Internet users to all types of abuse and violation of their privacy. In 2009, a worker was fired for using Facebook during her sick leave from work due to migraines when using computers. Her boss said that if she could use Facebook, she was capable of working on a computer. This incident launched the issue of spying using Facebook.3

The aim of this article is twofold: to identify, based on the motivations of Internet users visiting social networks, the risk of violating users’ privacy, and to analyze and evaluate the effectiveness of the control methods used.

**Figure 1**—Groups of Users of Social Networks

<table>
<thead>
<tr>
<th>Group</th>
<th>Motivations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
<td>Interaction with family and friends, research, and professional opportunities</td>
</tr>
<tr>
<td>Employers and recruiters</td>
<td>Psychological and social profiling of applicants</td>
</tr>
<tr>
<td>Criminals</td>
<td>Spam, scams and sexual crimes</td>
</tr>
<tr>
<td>Police, army, secret services and government agencies</td>
<td>Staff profiling, criminal investigations and quick communication with the public, particularly via Twitter</td>
</tr>
<tr>
<td>Politicians and activists</td>
<td>Ideological propaganda, research and gauge of popularity</td>
</tr>
<tr>
<td>Businesses</td>
<td>Profiling and targeting potential markets, deepening customer relationships, online promotion and sales, and online surveys and studies</td>
</tr>
</tbody>
</table>

Figure 1 shows that the most vulnerable group is individuals, who make up the majority of social network users. In fact, the other groups freely make use of the information published by individuals for a variety of purposes.

So, what are the types of risk facing the hundreds of millions of people connected to Facebook, LinkedIn, Twitter and Myspace?
Each Internet user connected to social networks has a digital identity. It is made up of everything users publish on their various accounts and allows a sketch to be drawn of their personalities. “On each login, sending of e-mail and search on a search engine, there are private conversations, IP addresses and addresses of sites visited that are archived and possibly exploited for commercial purposes.”

The financial or strategic stakes of access to this identity by various interest groups are obvious. As a result, there are many types of risk for social network users and the security of the information shared on social networks:

- **Identity theft**—Access to basic information constituting the identity of the Internet user (i.e., name, surname, date of birth, place of birth, photo) opens the door to the risk of identity theft. In France, for example, this risk has been recognized and has led to a change in legislation. Thus, a new section 226-4-1 of the Law of Orientation and Programming for the Performance of Internal Security (LOPPSI 2) was adopted by the French legislature on 8 February 2011.

- **Pedophilia and sexual crimes**—Teenagers, who are more numerous and more active on social networks, are exposed to sexual predators. Predators have time to make contact with their victims, most of the time under a false identity, and locate them geographically. The risk is even greater as teenagers are less likely than adults to be careful on these networks. A survey carried out in 2006 in the US, as part of research conducted by Princeton University, found that of 935 teenagers:
  - Four out of five teenagers put their first name in their profile.
  - Four out of five teenagers post their photo and two out of three teenagers post photos of their friends. When they are reminded of the public nature of the publication of photos, most of them say they are not concerned about the risk to their privacy. They think that the photos, even combined with the other information in the profile, do not give enough details to compromise their safety.
  - Six out of 10 teenagers put the name of the town where they live.
  - One half of teenagers post the name of their school.
  - Four out of 10 teenagers post their messaging nicknames (e.g., MSN address).
  - Three out of 10 teenagers include their surnames in their profiles.
  - Two thirds of teenagers restrict access to their profile (e.g., by making it private, protecting it with a password, completely hiding it from the view of others).

The results of this survey show the vulnerability of younger people, and their obvious lack of information on the risk of pedophile attacks through social networks. It is also worth noting the risk of teenagers developing trauma or dependencies with regard to some pornographic and obscene content published on these sites.

- **Dismissal/disqualification/serious misconduct**—Some social networks, such as Viadeo or LinkedIn, allow their users to post their curriculum vitae (CV) and provide opportunities to find career prospects. In contrast, people’s publications on a general social network, such as Twitter or Facebook, can strike a blow to their career aspirations. An employer may find that obscene photos or foul language may undermine the image of the company, and dismiss the offending employee. In the US, 45 percent of employers search through social networks when they want to recruit.

While the debate on the involvement of companies in controlling content published by their current (or potential) employees is quite complex, the risk for businesses is real. For example, hackers could use information left on a social network by the employees of a particular company to try to gain access to the information systems of the company; information such as date of birth or the first and last names of children may in fact enable hackers to figure out passwords. Even worse, clumsy system administrators could, for example, by asking their peers for help on a web site, post information on the configuration of the
operating system, which would be very beneficial to any hackers. Thus, there must always be a compromise made by employees between their behavior and the interests of the companies that employ them.

**Advertising harassment/spam**—In 2011, Facebook achieved advertising revenues of US $4 billion, according to its chief operating officer, Sheryl Sandberg. Of course, companies display commercial advertisements on the site, but they also, and above all, use the private information that is published to better target their communication. This is also the case with Twitter, which, through its “sponsored tweet” concept, provides advertisers with detailed statistics on user profiles. This system allows them to find out more about potential customers and to obtain substantial revenue sources. Spam is a real nuisance, and the worst is that the operators of these sites are just as much victim to it as the public. For example, in mid-November 2011, Facebook was victim to a campaign of pornographic spam that appeared in users’ news feeds.

There are yet further dangers associated with the protection of privacy on networks: phishing facilitated by information left on social networks, spying by government agencies and ideological manipulation (e.g., terrorism, racism). The risk is exacerbated by the business model of social networks, which is an obstacle to the development of a serious private information security policy.

**Terms of Use and Privacy of Social Networks**

“The era of privacy is over.” This statement is not that of a hacker on the lookout for accounts to hijack, but that of Mark Zuckerberg, founder and chief executive of Facebook. And, although it provoked a public outcry, it does reflect what little importance social networks grant to user privacy.

Thus, although the Facebook conditions of use make a point of respecting and protecting the information of site members, a clause further specifies: “We do everything we can to make Facebook a safe service, but cannot guarantee its absolute security. To do this, we need your help, which includes the following obligations…” A series of recommendations then follows.

In short, social networks’ conditions of use are in no way capable of guaranteeing the safety of Internet users and are purposely written in such a way that will discourage users from browsing them properly. Sites basically have no interest in users finding certain clauses that give them full control over all the information published. Thus, in 2009, Facebook was claiming lifetime ownership of all user information even after users unsubscribed from the site. The site was then forced to abandon this quietly introduced clause, faced with the veritable outcry provoked by this decision.

Due to the ambiguous behavior of operators of the sites, each consumer must be informed about current legislation and then act responsibly to protect themselves.

**BUSINESS MODEL AND PRIVACY POLICY**

**Business Model**

The business model of social networks is based primarily on building huge databases of Internet users’ information on which companies and government agencies are willing to pay an awful lot of money. In this context, it goes without saying that respect for privacy is not the main concern of the operators of these sites.

They are constantly creating more applications that are a potential threat to protection of privacy, and sometimes installed by default on each profile. Such is the case with “Places,” a geolocation system, or “Timeline,” a kind of biography of users generated with all their publications on their Facebook profiles. These facts prompt us to look more closely at the conditions of use and privacy of social networks.

**LEGISLATION**

In February 2009, Alex Turk, president of France’s National Commission for Information Technology and Civil Liberties (CNIL), pointed the finger at a crucial issue. “The American companies that dominate the Internet do not feel bound by European regulations…” In fact, it is virtually impossible at this time to establish binding global legislation on the regulation of social networks. As the majority of servers for these networks are located in the US, American law applies and, unfortunately, it is relatively deficient with regard to security of Internet users’ private information.

Failing a more effective means of pressuring network administrators, the European Commission has adopted two strategies for the moment:

- Awareness, through advertising campaigns aimed particularly at minors
- Self-regulation, relying on voluntary action by social networks
However, it must be noted that in light of the facts mentioned previously, these networks are reluctant to assume social responsibility for obvious reasons of financial and strategic interests. This is evidenced by the recent reprimand of Facebook in the US by the Federal Trade Commission (FTC), concerning the violation of users’ privacy rights. The FTC’s criticisms are as follows: “The social network Facebook has accepted the criticisms of the FTC in the sense that it has disappointed users by telling them that they could protect the privacy of their personal information, and then on the other hand regularly sharing and making public this same information.” Of course Mark Zuckerberg says that he is working to ensure that these “mistakes” do not happen again. However, it is clear that, at the moment, users are extremely vulnerable to all sorts of abuse and to violation of their fundamental right to respect for their privacy, but that public authorities have no real means of enforcement.

This inability of governments to implement coercive global legislation led a coalition of experts in privacy protection in 40 countries to publish a statement in 2009. It requires governments to implement and enforce effective legislation on privacy.

HOW TO PROTECT YOURSELF?

Privacy protection on the Internet in general and on social networks in particular is becoming increasingly necessary. Vigilance continues to spearhead the security and, thus, the privacy of the information. It can be broken down into a few techniques that are simple but could make all the difference:

- **Choice of “friends” and contacts**—Users should be extremely careful in their choice of friends on these networks. It is common practice to accept contact from friends of friends, who are frequently complete strangers. This can lead to one’s private life being exposed to potentially harmful individuals.

- **Restricting private content to close friends and family only**—Social networking sites are increasingly allowing their users to configure restrictions on access to their information. It is, therefore, important to use these restrictions and to ensure that they are properly configured, given that our information is public by default.

- **Careful choice of information to be broadcast**—The key to the protection of privacy is in fact what information one broadcasts. Name, surname, date of birth, place of birth, photos, videos, comments and opinions should be carefully screened prior to being posted. Keep in mind that information posted on a network may one day be used against its author.

**ENDNOTES**

5. Le Monde Newspaper, 28 May 2010, p.16
Competition can be tough...

Gain the upper hand.

Register today!

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

ISACA members save US $150 off exam registration.

www.isaca.org/certification-Journal
Meeting PCI DSS When Using a Cloud Service Provider

With the advent of new technologies, cloud computing has the potential to be the next major driver of business innovation, as it is likely to change the provision of IT services across almost all industries, including finance, telecommunications, health care and government. This means that exploitation will change from systems to web. Due to these changes, today's business needs demand that applications and data move across physical, international borders as well as the cloud, and are accessible by third parties. This loss of control is significant for security teams, which must not only keep data safe, but also comply with the necessary security standards, e.g., the Payment Card Industry Data Security Standard (PCI DSS).

The number of data breaches involving consumer credit card information has been growing at an incredible rate. Major retailers have experienced unauthorized intrusions into the computer systems that process and store information related to customer transactions, resulting in the theft of millions of credit card numbers and other sensitive customer data. With today's online and cashless world, financial institutions, credit card service providers and retailers must make every effort to enable adequate privacy and data protection of credit card information, provide and share information securely across multiple systems and facilities, monitor and evaluate the security of their information, and enhance the value of their IT resources.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model promotes availability and is composed of three service models and four deployment models.

- **SaaS**—The capability provided to the consumer is to use the provider’s applications running on

PCI DSS requirements (see figure 1) apply to a cloud provider with environments that store, process or transmit cardholder data as well as other environments that handle cardholder data. When a cloud service provider says that it has been validated as PCI DSS-compliant, it means that it has been validated against specific PCI requirements; it does not mean that an enterprise is automatically PCI DSS-compliant if it is a tenant of that provider. Where cloud solutions and virtualization technologies are in use, the questions are about how to implement these technologies in a PCI DSS-compliant manner, rather than about which requirements apply.

The only way a customer could become automatically compliant is if a PCI-compliant cloud provider actually managed all the way up the application stack and had a Software as a Service (SaaS) offering that is specific around one application that does a specific function. The cloud service provider (CSP) would have to ensure that every single customer, whether the customer is on physical or virtual servers, has the same level of security and separation. Compliance also requires quarterly scans and, for certain customers, the ability to provide onsite audits.

This article contains the results of implementing PCI DSS at a CSP.

**WHAT CLOUD COMPUTING IS ALL ABOUT**

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model promotes availability and is composed of three service models and four deployment models.

The service models are:

- **SaaS**—The capability provided to the consumer is to use the provider's applications running on

Adesanya Ahmed, CRISC, CGEIT, ACMA, ACPA, is an IT security and connectivity consultant. Ahmed was the first to provide a CerebusServer broadband billing authentication for hotspot Wi Fi and WiMAX Internet service providers (ISPs) in Nigeria. Ahmed is a partner in Oogwave Inc., a web-based collaboration that provides a secure, reliable space on the cloud to share and access data, discuss ideas, and communicate on a single platform in real time. Ahmed can be reached at owos2001@yahoo.co.uk.

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:
### Figure 1—PCI DSS Requirements for Cloud Service Providers

<table>
<thead>
<tr>
<th>Activities</th>
<th>PCI DSS Requirements</th>
<th>Addressing the Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and maintain a secure network.</td>
<td>1. Install and maintain a firewall configuration to protect data; this includes firewall on client.</td>
<td>The purpose of this is to continually remove malicious traffic before damage occurs without creating productivity hits caused by false positives. Attacks covered include targeted application server attacks, worms, viruses and Trojans. Implement physical network segmentation to isolate any systems hosting public-facing or untrusted systems and networks from systems that host virtual components within or connected to the cardholder data environment (CDE). Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the CDE. Provide web application, database and other application protection with specific application vulnerability filters (including Oracle, SQL and MySQL). Prohibit direct public access between the Internet and any system component in the CDE.</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters.</td>
<td>Always change vendor-supplied defaults (wired or wireless) before installing a system on the network, including but not limited to passwords and Simple Network Management Protocol (SNMP) community strings. Eliminate unnecessary accounts. Do not locate both high-security and low-security on the same host or hypervisor. Encrypt all nonconsole administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access. Secure management protocols and traffic enforcement to block unauthorized protocols.</td>
</tr>
<tr>
<td>Protect cardholder data.</td>
<td>3. Protect stored cardholder data.</td>
<td>Frequently update security management system to provide comprehensive protection for network components, including encryption of terminal points against traffic anomalies, process table floods and distributed denial-of-service (DDoS) attacks. Do not store sensitive authentication data after authorization (even if encrypted). If key management functions are virtualized, do not house virtual components that perform key management functions or store cryptographic keys on the same hypervisor or host as virtual components that store or access data protected by those keys. Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions and do not store the personal identification number (PIN) or the encrypted PIN block.</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data and sensitive information across open public networks.</td>
<td>Use strong cryptography and security protocols (e.g., SSL/TLS, IPSEC, SSH) to safeguard sensitive cardholder data during transmission over open, public networks (Internet, wireless technology, GSM and GPRS). Protect against transmission of unencrypted data (customer filter that allows the intrusion protection system [IPS] to detect the application data type and apply the appropriate policy).</td>
</tr>
<tr>
<td>Maintain a vulnerability management program.</td>
<td>5. Use and regularly update antivirus software.</td>
<td>Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers). Ensure that all antivirus programs are capable of detecting, removing and protecting against all known types of malicious software. Ensure that all antivirus mechanisms are current, actively running and generating audit logs.</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications.</td>
<td>Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Develop a software application with capabilities of providing fast, accurate, reliable protection from internal and external cyberattacks.</td>
</tr>
<tr>
<td>PCI DSS Requirements</td>
<td>Addressing the Requirements</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Implement strong access control measures.</td>
<td>Virtualization technologies must be able to separate administrative access to the host or hypervisor from administrative access into individual hosted virtual components. This could result in preventing unauthorized or unnecessary assignment of privileged access within the hosted components.</td>
<td></td>
</tr>
<tr>
<td>7. Restrict access to data by business on a need-to-know basis.</td>
<td>Limit access to system components and cardholder data to only those individuals whose job requires such access.</td>
<td></td>
</tr>
<tr>
<td>7. Restrict access to data by business on a need-to-know basis.</td>
<td>Establish an access control system for system components with multiple users that restricts access based on a user’s need to know, and is set to deny all unless specifically allowed.</td>
<td></td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access.</td>
<td>Assign all users a unique ID before allowing them to access system components or cardholder data.</td>
<td></td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access.</td>
<td>Due to the potential impact of unauthorized hypervisor access, additional authentication controls may be needed, e.g., restricting all remote access to the hypervisor to defined source systems, management interfaces and consoles.</td>
<td></td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access.</td>
<td>Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators and third parties. For example, remote authentication and dial-in user service (RADIUS) with tokens, terminal access controller access control system (TACACS) with tokens, or other technologies that facilitate two-factor authentication.</td>
<td></td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access.</td>
<td>Dormant or offline virtual components could also contain cardholder data and may also require strong access controls.</td>
<td></td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access.</td>
<td>Ensure proper user identification and authentication management for nonconsumer users and administrators on all system components.</td>
<td></td>
</tr>
<tr>
<td>9. Restrict access to cardholder data.</td>
<td>Use appropriate facility entry controls to limit and monitor physical access to systems in the CDE.</td>
<td></td>
</tr>
<tr>
<td>9. Restrict access to cardholder data.</td>
<td>Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data are accessible.</td>
<td></td>
</tr>
<tr>
<td>9. Restrict access to cardholder data.</td>
<td>Due to the potential impact of unauthorized physical access, additional authentication and monitoring of physical access may be needed, e.g., requiring dual-factor authentication and a supervised escort for all physical access to the data center.</td>
<td></td>
</tr>
<tr>
<td>9. Restrict access to cardholder data.</td>
<td>Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access. Retain this log for a minimum of three months, unless otherwise restricted by law.</td>
<td></td>
</tr>
<tr>
<td>Regularly monitor and test networks.</td>
<td>Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.</td>
<td></td>
</tr>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data.</td>
<td>Secure audit trails so they cannot be altered.</td>
<td></td>
</tr>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data.</td>
<td>Do not locate audit logs on the same host or hypervisor as the components generating the audit logs.</td>
<td></td>
</tr>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data.</td>
<td>Review logs for all system components at least daily. Log reviews must include servers that perform security functions such as an intrusion detection system (IDS) and authentication, authorization and accounting (AAA) protocol servers (e.g., RADIUS).</td>
<td></td>
</tr>
</tbody>
</table>
a cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, including networks, servers, operating systems, storage and individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- **Platform as a Service (PaaS)**—The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (including network, servers, operating systems or storage), but has control over the deployed applications and possibly application-hosting environment configurations.

- **Infrastructure as a Service (IaaS)**—The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources under which the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over the operating systems, storage and deployed applications, and possibly limited control over select networking components (e.g., host firewalls).

The deployment models are:

- **Private cloud**—The cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party, and it may exist on-premise or off-premise.

- **Community cloud**—The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be managed by the organizations or a third party, and it may exist on-premise or off-premise.

- **Public cloud**—The cloud infrastructure is made available to the general public or a large industry group and it is owned by an organization selling cloud services.

- **Hybrid cloud**—The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing among clouds).

---

**Figure 1— PCI DSS Requirements for Cloud Service Providers (cont.)**

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Addressing the Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regularly monitor and test networks. (cont.)</td>
<td>Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). Use IDS, and/or intrusion prevention systems (IPSs) to monitor all traffic at the perimeter of the CDE as well as at critical points inside of the CDE, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines and signatures up to date.</td>
</tr>
<tr>
<td>11. Regularly test security systems and processes.</td>
<td>Develop daily operational security procedures that are consistent with requirements in this specification (e.g., user account maintenance procedures, log review procedures). Include details outlining specific controls and assigned responsibilities in written agreements with service providers in which cardholder data or security controls are under the control of a third-party service provider in a virtual environment. Develop usage policies for critical technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], email usage, Internet usage), and define proper use of these technologies. Establish, document and distribute security policies and procedures.</td>
</tr>
<tr>
<td>Maintain an information security policy.</td>
<td>Develop daily operational security procedures that are consistent with requirements in this specification (e.g., user account maintenance procedures, log review procedures). Include details outlining specific controls and assigned responsibilities in written agreements with service providers in which cardholder data or security controls are under the control of a third-party service provider in a virtual environment. Develop usage policies for critical technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], email usage, Internet usage), and define proper use of these technologies. Establish, document and distribute security policies and procedures.</td>
</tr>
</tbody>
</table>

PCI DSS

In today’s complex business environment, every organization across the globe, regardless of its size or industry, faces security issues pertaining to new and evolving threats, vulnerabilities, risk or regulatory/compliance landscapes. As such, there arises a need for organizations to make stringent efforts to ensure that their security and enterprise risk management (ERM) programs address multiple compliance requirements. PCI regulation applies globally and focuses on ensuring integrity and reliability of systems that participate in handling and storing cardholder data.

PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. It applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers and service providers, as well as all entities that store, process or transmit cardholder data.

SECURITY AND RISK OF OUTSOURCING CLOUD COMPUTING

The risk frequently associated with outsourcing cloud computing is not new, and it can be found in many organizations today. Well-planned risk management activities are crucial in ensuring that information is simultaneously available and well protected. Business processes and procedures need to account for security, and information security managers may need to adjust their enterprises’ policies and procedures to meet the needs of the business. Given the dynamic business environment and focus on globalization, there are few organizations that do not outsource some part of their business. Engaging in a relationship with a third-party cloud computing services provider means that the business is not only using the services and technology of the provider, but also must understand the way the provider runs its organization—the planning the provider has in place in its organizational culture and policies.

The risk involved in outsourcing cloud computing includes:

- **Loss of governance**—Just as in traditional IT outsourcing, using the services of a cloud provider requires organizations to give up control over their IT infrastructure. To make it easier for customers that take this step, cloud providers should make management and maintenance more transparent and auditable by customers. This should include recording logs and complete administrative sessions that affect the part of the cloud infrastructure used by customers and, if requested, making these records accessible to customers. There must be strong authentication and authorization for the staff of the CSP and the customers. This includes strong and possibly multifactor authorization methods, such as tokens or one-time passwords, on the one hand, and strong authorization methods, such as four-eyes authorization, on the other. Ideally, customers should be able to authorize and possibly monitor access to the system for the key systems they use. Such monitoring could be as simple as following the logs on an online interface or as sophisticated as watching a real-time audit trail of the administrator’s actions on the system—be it on a specific virtual machine or the hypervisor of the entire system. Allowing access to the audit trails of the hypervisor or providing four-eyes authorization to customers may initially seem excessive, but it may be necessary for compliance reasons.

- **Cloud provider selection**—Public clouds allow high-availability systems to be developed at service levels often impossible to create in private networks, except at extraordinary costs. Compliance with regulations and laws in different geographical regions can be a challenge for organizations. At this time, there is little legal precedent regarding liability in the cloud. It is critical to obtain proper legal advice to ensure that the contract specifies the areas in which the CSP is responsible and liable for ramifications arising from potential issues. Organizations could leverage the global compliance requirements that are becoming stricter and go for a CSP that can meet these requirements and is able to offer hard evidence of its compliance.
• **Compliance requirements**—For compliance requirements such as PCI DSS, today’s cloud computing services can challenge various compliance audit requirements currently in place. Data location and cloud computing security policy transparency are challenging issues in compliance auditing. Also, CSP do not want to be audited by all of their clients for compliance.

• **Weak user authentication**—Access to highly sensitive information often requires only simple password authentication, and does not take into account other contextual information (e.g., the user’s location) that might raise the risk of breach due to an unsecure network connection.

• **Data protection**—Data protection and data abuse prevention are traditionally handled via authorization and strong access control as well as by using an IDS and a data loss prevention (DLP) system. Authorization can be handled by strong and possibly multifactor authentication, and access control and authorization can be enhanced by four-eyes authorization methods. However, for obvious reasons, users must access a remote cloud using secure connections, which makes the use of an IDS and a DLP system increasingly difficult. Thus, a solution that can share the traffic of the encrypted channels with a client’s IDS/DLP system is highly beneficial.

• **Ineffective management of privileged users**—All IT environments have privileged users (e.g., admin, root) who have total access to key systems, applications and information. This is not only a security risk, but it can also make compliance much more difficult. Sharing administrator passwords is another common problem that could lead to inappropriate access to the organization’s systems and information and to an inability to identify who performed which action on each system.

  PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risk. The results of implementing PCI DSS by a CSP are presented as follows:

  • **PCI DSS compliance made easy**—While compliance with PCI DSS is mandatory for organizations that process financial transactions through payment cards, its scope is to protect cardholder data. CSPs that deal with cardholder data must also comply with the standard.

  • **Implementing secure control and encryption over the network**—The CSP must be capable of implementing the necessary protection and alerting locally in line with PCI DSS. External vulnerability scans must be conducted by an approved scanning vendor (ASV) every quarter of the year. The service provider may have an environment with public-facing Internet protocols (IPs) in certain cases, such as access through multiprotocol label switching (MPLS) environments and end-to-end connectivity; it may have none. An ASV audit is applicable only in the former. It is recommended that virtual private networks (VPNs) be used even with MPLS environments, since the transmissions are not encrypted.

  CSPs should provide more flexibility to merchants in terms of using a suitable method for detecting unauthorized access. Methods that can be used are wireless network scans, physical/logical inspection of system components and infrastructure, network access control (NAC), and a wireless IDS/IPS.

  • **Information protection and control**—CSPs that are planning to implement PCI DSS can easily manage, measure and provide evidence of satisfying compliance requirements through a single unique set of controls. CSPs have to ensure that every customer, whether on a physical or virtual server, has the same level of security and separation. Compliance also requires quarterly scans and, for certain customers, the ability to provide onsite audits. Protection of sensitive customer and corporate information, including intellectual property, is essential to avoiding the financial and reputational damage that might result from a public breach.

  • **Privileged user management**—Privileged users pose a significant risk of information disclosure, either through inadvertent or malicious actions. Access control provides granular control of systems and information across heterogeneous server platforms, thereby helping to protect assets from improper action. It also supports privileged user password management, which helps eliminate the challenge of sharing administrative passwords through the issuance of passwords on a temporary, one-time use basis. Access control can help ensure that privileged users have access only to the resources they require for their job role. And, given that many successful insider intrusions have been perpetrated by
administrators, access control is a crucial first building block in the foundation against insider threats.

- **Maintain information security policy**—A strong security policy tone must be set for the whole entity as it informs personnel about what is expected of them in compliance with PCI DSS. It is crucial to ascertain implementation of strong access control measures, and access to cardholder data should be restricted by business on a need-to-know basis. This is the difficult part of achieving PCI DSS compliance. In an outsourcing relationship, access control should be defined by the outsourcer. Practices such as role-based access control on the principle of least privilege are robust for securing sensitive information. It is mandated that access be based on white lists, denying all other access requests. All employees should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

- **Enforcement of four-eyes authorization**—The enforcement of four-eyes authorization with real-time monitoring and auditing capabilities effectively creates a strong auditing layer above the superuser layer that is accessing the devices, with the possibility to greatly increase the security of the cloud. For every security-aware customer, or for customers with special security needs such as those resulting from PCI DSS, it is possible to require a representative of the customer to authorize cloud administrators, making the maintenance of the cloud's infrastructure that is relevant to the customer completely transparent, auditable and reviewable.

**CONCLUSION**

PCI DSS compliance is mandatory for banks, merchants and providers who process, transmit or store cardholder data. The risk of noncompliance is substantial, including fines, potential security breaches and loss of business. However, organizations must remain vigilant in assessing the security and risk in virtual and cloud environments by appointing a CSP that is able to deliver robust and secure cloud-based services in line with PCI DSS requirements.

**REFERENCES**

PCI Security Standards Council, [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

Ponemon Institute Research, [www.ponemon.org](http://www.ponemon.org)


IT Policy Compliance, [www.itpolicycompliance.com](http://www.itpolicycompliance.com)

The benefits of cloud computing (specifically Software as a Service [SaaS]) over in-house development are clearly articulated and well known, and they include rapid deployment, ease of customisation, reduced build and testing effort, and reduced project risk. Similarly well known are Infrastructure as a Service (IaaS) benefits, which include reduction in cost, movement from capital expenditure to operational expenditure and agility.1 A consensus on the risk of cloud computing is, however, more difficult to achieve because the industry is lacking a structured framework for risk identification and assessment. In addition, businesses struggle with identifying and following a road map for cloud implementation. Paradoxically, from a small to medium-sized enterprise perspective, migrating to the cloud may in fact mitigate risk.2 For example, the likelihood of server misconfiguration or poor patch management leading to a successful attack is greatly reduced, as is the risk of data loss due to less use of portable media.

Recent high-profile outages and security breaches serve to further confuse businesses as they attempt to correlate their current internal control environment and proposed controls for the cloud with the external incidents chronicled in the press. For example, in April/May 2011, cloud risk came to widespread attention with the consecutive failures of Sony, VMware and Microsoft cloud-based services.3

**LITERATURE REVIEW**

Over the last few years, a plethora of documents have been written containing risk exposure, ad hoc guidance and control checklists to be consulted when considering cloud computing. Most of these are deep on security concerns but narrow across the breadth of IT risk where a comprehensive framework for assessment is needed.

Having said that, the International Organization for Standardization (in particular ISO/IEC JTC 1/SC 27) is embarking on the development of a series of standards that aims to formally address risk management of cloud computing services. The risk profile for cloud migration itself is also in a state of flux, as existing offerings are maturing and new offerings are emerging. Examples include new cloud offerings such as Data as a Service (DaaS) and the emergence of cloud service brokers, who provide intermediation, monitoring, transformation/portability, governance, provisioning and integration services in addition to existing cloud services.

In 2009, the European Network and Information Security Agency (ENISA) produced a document titled ‘Cloud Computing: Benefits, Risks and Recommendations for Information Security’. This document collates 35 types of risk identified by 19 contributors, and identifies eight top security risks based on ENISA’s view of indicative likelihood and impact.4 In March 2010, the Cloud Security Alliance (CSA) published ‘Top Threats to Cloud Computing V1.0’, which includes the top seven threats as identified by the Open Web Application Security Project (OWASP) released a ‘pre-alpha list’ of its top 10 cloud security risks derived from a literature review of other publications and sources.5 In May 2011, the National Institute of Standards and Technology (NIST) released a draft titled ‘Cloud Computing Synopsis and Recommendations (Special Publication 800-146)’, which provides a deep analysis of risk, but again no coherent framework. **Figure 1** gives a comparison of the top types of risk identified by the CSA, OWASP and ENISA, showing the variation in both content and ranking.

**Figure 1**

Cloud Risk—10 Principles and a Framework for Assessment

David Vohradsky, CGEIT, CRISC, is a principal consultant with Tata Consultancy Services and has more than 25 years of experience in the areas of applications development, program management, information management and risk management. He has worked in senior management and consulting across multiple industries, adapting, implementing and utilising industry frameworks and ensuring compliance with regulatory requirements. Vohradsky specialises in governance, risk and compliance within TCS’s Global Consulting Practice, is a member of the ISACA CGEIT Test Enhancement Subcommittee, and an external thesis examiner for the Doctor of Business Administration at Charles Sturt University (Australia).
Abuse and nefarious use of cloud computing—Due to the often anonymous nature of some cloud services, they attract use by criminal elements.

Insecure interfaces and application programming interfaces (APIs)—Due to the open nature of cloud services, interfaces and APIs often use anonymous access, cleartext authentication or content transmission.

Malicious insiders—Cloud providers offer little transparency into their supply chain, human resources, security management or incident management processes.

Share technology (multitenancy/isolation) risk—one tenant can deliberately or inadvertently interface with the security or performance of another tenant.

Data ownership (governance) and accountability—Data ownership, encryption, transmission, operational failure, data disposal/data deletion and availability are all challenges in a cloud environment.

Account or service hijacking (including management interface)—Using social engineering, phishing, fraud or vulnerability exploits, attackers can compromise confidentiality, integrity and availability.

Unknown risk profile—Cloud providers offer little transparency into compliance, security procedures, configuration management, logging and monitoring, leaving customers with an unknown risk profile.

User identity federation—Use of multiple cloud offerings can result in islands of identities that need to be maintained.

Regulatory compliance—Regulatory environments differ across countries and regions, particularly with regard to privacy.

Business continuity and resilience—These are delegated to the cloud provider and may not be appropriate. Pricing pressure results in commoditisation that de-emphasises this.

Service and data integration/protection—Data handling or data protection fails during transmission between end user and data centre, or between federated clouds.

Non-production environment exposure—A cloud provider is used for design, development and test activities, which are typically less controlled.

Lock in—Minimal tools, procedures, standards or interfaces are in place to guarantee data, application, service or business process portability.

In July 2011, ISACA released IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, which provides a comprehensive guide to cloud controls taken from COBIT, Val IT and Risk IT. The ISACA publication critiques a number of standards, certifications or frameworks, including COBIT, ENISA, CSA, NIST, ISO 27001, the American Institute of Certified Public Accountants (AICPA) Service Organisation Control (SOC) 1 Report, AICPA Trust Services (SysTrust), CSA’s Cloud Security Matrix, FedRAMP, Health Information Trust Alliance (HITRUST), BITS Shared Assessment Program and Jericho Forum® Self-assessment Scheme (SAS). In doing so, the publication highlights both the need for a consistent and broadly accepted risk assessment framework and the fact that its existence still remains elusive.

A FRAMEWORK FOR ASSESSMENT

The ISO/IEC 9126 standard (Information technology—Software product evaluation—Quality characteristics and guidelines for their use), when used in conjunction with a deep security assessment, is valuable for putting more structure and
coherence around assessing the suitability of new vendors and new technologies, including cloud offerings. The objective of this international standard is to provide a framework, comprising six quality characteristics, for the evaluation of software quality. However, it also appears to be useful for SaaS, Platform as a Service (PaaS) and IaaS cloud assessments.

The types of risk identified in the reviewed literature can map directly to ISO/IEC 9126 (as shown in figure 2). In addition, the standard can be used to derive a superset of risk that is currently not coherently articulated in the industry. The example shown in figure 2 is based on an assessment by Force.com conducted by the author several years ago, and may not reflect the current offering from Salesforce.com.

<table>
<thead>
<tr>
<th>ISO 9126 Characteristic</th>
<th>Subcharacteristic</th>
<th>Cloud Risk</th>
<th>Force.com Example Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>Suitability (for business requirements)</td>
<td>Development/solution does not meet business requirements. (New)</td>
<td>Data model, screen layouts and business logic meet only basic business requirements. Heavy customisation is required.</td>
</tr>
<tr>
<td></td>
<td>Accurateness</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Interoperability (with internal systems)</td>
<td>Development/solution does not meet IT architecture requirements (e.g., interfaces, data migration). (New)</td>
<td>All integration through Web API requires ETL tools, and performance is unknown. Import/export via Apex Data Loader, which has execution limits. Sales Force Object Query Language (SOQL) does not have aggregate functions (e.g., sum, count, average) or joins.</td>
</tr>
<tr>
<td>Compliance (with regulations and policies)</td>
<td>OWASP (3)—Regulatory Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td>See figure 3.</td>
<td>Web API uses a generic account; security needs to be enforced by an external application.</td>
</tr>
<tr>
<td>Reliability</td>
<td>Maturity (of the offering)</td>
<td>Lack of quality in system/service (e.g., existing usage and support) (New)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fault tolerance (service level agreements [SLAs] and expected downtime)</td>
<td>OWASP (4)—Business Continuity and Resilience</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recoverability (business continuity ([BC])/disaster recovery ([DR]) arrangements)</td>
<td>Inability to recover services in line with business requirements (e.g., what is the backup, BC and DR strategy?) (New)</td>
<td></td>
</tr>
<tr>
<td>Usability</td>
<td>Understandability (technical and user)</td>
<td>Service/system is not operated as intended (e.g., lack of understanding of architecture, resilience, performance). (New)</td>
<td>Staff needs to learn Visualforce framework, Web Services API and APEX programming language.</td>
</tr>
<tr>
<td></td>
<td>Learnability (technical and user training required)</td>
<td>Staff has inadequate skills to perform roles and responsibilities. (New)</td>
<td>Requires expert level to achieve same look and feel in custom development as that which appears in out-of-the-box product.</td>
</tr>
</tbody>
</table>
### Figure 2—Risk Mapped to ISO 9126 (cont.)

<table>
<thead>
<tr>
<th>ISO 9126 Characteristic</th>
<th>Subcharacteristic</th>
<th>Cloud Risk</th>
<th>Force.com Example Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usability (cont.)</td>
<td>Operability (technical and user effort required)</td>
<td>There are inadequate people to support the solution (e.g., both at cloud provider and cloud subscriber).</td>
<td>Will require support for new ETL and reporting tools required, as well as support for customisations required.</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Time behaviour (response and processing times)</td>
<td>OWASP (6)—Service and Data Integration ENISA R26—Network Management</td>
<td>Web API integration is dependent on user machine memory (minimum 1GB) and browser.</td>
</tr>
<tr>
<td></td>
<td>Resource behaviour (multitenant impacts)</td>
<td>ENISA R8—Resource Exhaustion—Under/Over Provisioning (e.g., resource usage by another tenant)</td>
<td>Script execution limits (200 record batching/5,000 API call per 24-hour limit) offer protection, but require complex programming to perform some business reporting functions.</td>
</tr>
<tr>
<td>Maintainability</td>
<td>Analysability (technical transparency)</td>
<td>CSA (7)—Unknown Risk Profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Changeability (change and configuration management processes)</td>
<td>Release of changes negatively impacts the business (e.g., segregation of duties, centralised/decentralised changes, compliance with change management policies, configuration management tools).</td>
<td>Source code control and separate environments are provided, but there is only one production to test environment refresh per month. There are up to 15 developer instances, but only one application layer (cannot refresh from production).</td>
</tr>
<tr>
<td></td>
<td>Stability (how easy it is to break)</td>
<td>CSA (4)—Shared Technology Issues ENISA R25—Network Breaks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Testability (including available test environments)</td>
<td>Release of IT change negatively impacts the business (e.g., test processes, test environments, test data sanitisation).</td>
<td>See Changeability entry.</td>
</tr>
<tr>
<td>Portability</td>
<td>Adaptability (to technical business variations)</td>
<td>OWASP (2)—User Identity Federation (may need multiple user accounts)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installability (effort to migrate to)</td>
<td>Implementation project risk (e.g., scope, time, cost, quality)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conformance (standards supported)</td>
<td>Lack of quality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Replaceability (ability to migrate to alternative)</td>
<td>ENISA R1—Lock In</td>
<td>Import/export capabilities are limited and subject to execution limits.</td>
</tr>
</tbody>
</table>
The security-related risk can be assessed in a similar structured approach by assessing against selected ISO 2700x, COBIT and NIST 800-53 controls that are applicable to the exposures within cloud computing. As an example, figure 3 shows a cross-reference of the security-related risk (identified in the literature reviewed) to COBIT 4.1 DS5 Ensure systems security.

Figure 3—Security-related Risk and COBIT DS5

<table>
<thead>
<tr>
<th>COBIT Control Objective</th>
<th>Controls</th>
<th>Cloud Risk</th>
<th>Force.com Example Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS5.1 Management of IT security</td>
<td>Management (ISO 27002–6)</td>
<td>ENISA R2—Loss of Governance</td>
<td>Will maintain appropriate safeguards; liability limited to US $500,000 or amount paid in preceding 12 months.</td>
</tr>
<tr>
<td>DS5.2 IT security plan</td>
<td>Compliance (ISO 27002–15)</td>
<td>ENISA R3—Compliance Risks ENISA R22—Risk from Changes in Jurisdiction Hosted in Singapore with replication to North America; will be considered material outsource by financial industry regulators.</td>
<td></td>
</tr>
<tr>
<td>DS5.3 Identity management/DS5.4 User account management/ISO 27002–11</td>
<td>Unique ID</td>
<td>OWASP 2—User Identity Federation</td>
<td>Individual and role-based restrictions at system, component, object, record and field level.</td>
</tr>
<tr>
<td></td>
<td>Generic accounts</td>
<td>CSA 3/ENISA R10 and R28—Malicious Insiders Unknown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Account security</td>
<td>CSA 6—Account or Service Hijacking Logins are restricted to IP range and time of day. Service is monitored for security violation attempts. Login data are retained for six months and can be downloaded and reviewed.</td>
<td></td>
</tr>
<tr>
<td>DS5.5 Security testing, surveillance and monitoring</td>
<td>Security logging (ISO 27002–10)</td>
<td>OWASP 8—Incident Analysis and Forensic Support Audit trails can be defined; may have performance impact.</td>
<td></td>
</tr>
<tr>
<td>DS5.6 Security incident definition</td>
<td>Incident management (ISO 27002–13)</td>
<td>ENISA R18—Malicious Probes or Scans ENISA R30 and R31—Loss or Compromise of Logs</td>
<td></td>
</tr>
<tr>
<td>DS5.7 Protection of security technology</td>
<td>Technology controls</td>
<td>OWASP 7/ENISA R9—Multitenancy and Physical Security ENISA R24—Licencing Risks Each database consists of static tables that store data from thousands of customers all mixed together. Control and access are managed by metadata.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vulnerability management</td>
<td>OWASP 9—Infrastructure Security ENISA R20—Cloud Hardening ENISA R15—Distributed Denial of Service (DDoS) Unknown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Utility program access</td>
<td>OWASP 10—Non-production Environment Exposure ENISA R11 and R19—Service Engine/Interface Compromise Unknown</td>
<td></td>
</tr>
</tbody>
</table>
THE TEN PRINCIPLES OF CLOUD COMPUTING RISK

The ten principles of cloud computing risk help to give context to the frameworks for assessment previously discussed, and they can be used as an overall road map for migration to cloud computing. The road map is based on four guiding principles:

1. Vision—What is the business vision and who will own the initiative?
2. Visibility—What needs to be done and what are the risks?
3. Accountability—Who is accountable and to whom?
4. Sustainability—How will it be monitored and measured?

The ISACA Business Model for Information Security (BMIS) (figure 4) was used as an overarching framework for risk and security.

Based on BMIS, these 10 principles of cloud computing risk provide a framework for cloud computing migration which is presented here in a case study.
This case study considers moving a risk management business function (e.g., a home loan mortgage insurance calculation) to the cloud. The business function is part of the decision-making process within the end-to-end home loan business process shown in *Figure 5*. In this process, an application is received and acknowledged, various calculations are performed, and a decision is made regarding whether to lend money.

The business benefit of placing this function in the cloud is that it will allow branches, call centres, brokers and other channels to use the same code base and avoid replicating the calculations in multiple places. The use of the cloud will also reduce paper handling and host system access and the associated security required. There is also a potential business driver for allowing customers access to their own data if placed on the public cloud.

The first step in the framework is to formulate and communicate a vision for the cloud at an enterprise and business-unit level. The first two principles relate to this vision:

1. **Executives must have oversight over the cloud**—The business as a whole needs to recognise the value of the cloud-based technology and data. There must be constant vigilance and continuous monitoring of risk to these information assets, including ensuring compliance with appropriate laws, regulations, policies and frameworks. This is related to the governance dimension of BMIS. In the case study, the head of the retail banking department obtains briefings from internal and/or external business and technical experts to understand the technology and its alignment to the business objectives. The individual then sets a ‘tone from the top’, mandating policies and structures to ensure that this alignment is maintained within industry standards and regulatory constraints.

2. **Management must own the risks in the cloud**—The management of the relevant business unit must own the risk associated with its use of cloud services, and must establish, direct, monitor and evaluate commensurate risk management on an on-going basis. This is related to the organisation dimension of BMIS. In the case study, the business decides to assign ownership of the complete (business and IT) risk of the initiative to the retail bank operational risk manager, who works with the departmental IT risk manager to plan actions covering both the business and technical risk involved.

   Once the vision is articulated and the risk management organisation is in place, the next step in the road map is to ensure visibility of what needs to be done and the risk of doing it. There are three principles related to ensuring visibility:

3. **All necessary staff must have knowledge of the cloud**—All users of the cloud should have knowledge of the cloud and its risk (commensurate with their role in the organisation), understand their responsibilities and be accountable for their use of the cloud. This is related to the human factors dimension of BMIS. In the case study, the home lending line-of-business owner and the IT manager work together to ensure that the involved business and technology staff have the appropriate skills to embark on the cloud initiative or that the needed expertise is obtained externally.

4. **Management must know who is using the cloud**—Appropriate security controls must be in place for all uses of the cloud, including human resources practices (e.g., recruitment, transfers, terminations). This is related to the people dimension of BMIS. In the case study, the home lending line of business owner must ensure that the necessary background checks, segregation of duties, least privilege and user access review controls are in place in the business, IT and cloud service provider. This will require working with the IT manager and the possible engagement of external assessment organisations.

5. **Management must authorise what is put in the cloud**—All cloud-based technology and data must be formally classified for confidentiality, integrity and availability (CIA) and must be assessed for risk in business terms, and best practice business and technical controls must be incorporated and tested to mitigate the risk throughout the asset life cycle. This is related to the technology dimension of BMIS, and it is where the ISO 9126-based framework for assessment is used in this road map.
In the case study, the home loan mortgage insurance calculation process uses sensitive data such as customer identity, date of birth and taxable income. The CIA rating of the business data is an average of high, based on the assessment provided in figure 6.

A more complete CIA analysis might also consider detailed business requirements, data retention requirements, and privacy and regulatory requirements.

Once this assessment is completed, the asset can be mapped to potential cloud deployment models. Based on the profile of high concern in the case study, management decided that the process should be considered for migration to a private cloud. In this type of deployment, the calculation can be made accessible to the various stakeholders with their heterogeneous client devices, but still provide an acceptable level of security over the data. A key consideration would be the limited scalability or agility that a private cloud would offer compared to a public cloud. In this case, the retail banking executive decides to deploy to a private cloud until customer access becomes a compelling requirement.

As the next step, the risk associated with a cloud implementation must be assessed against the risk associated with the incumbent in-house system, and also against the option of acquiring a new internally operated system. The framework for assessment could be used for each of these options, to assess risk areas such as deficient vendor or internal support, application complexity, and application reliability. In the case study, an assessment of the existing loan mortgage insurance application identified an aging application with overreliance on a single vendor and limited disaster recovery.

---

**Figure 6—Confidentiality, Integrity and Availability Assessment**

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Public</th>
<th>Internal use</th>
<th>Confidential X</th>
<th>Highly restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>Low (archival)</td>
<td>Moderate (routine)</td>
<td>High (relied on) X</td>
<td>Maximum (very high reliance)</td>
</tr>
<tr>
<td>Availability</td>
<td>Tolerance &gt; 14d</td>
<td>Tolerance 1-14d</td>
<td>Tolerance &lt; 24 hours</td>
<td>Tolerance &lt; 4 hours</td>
</tr>
</tbody>
</table>

---

**Figure 7—Risk Profile for the Process in the Current In-house System**

<table>
<thead>
<tr>
<th>Impact/Likelihood</th>
<th>Insignificant (&lt;AU $100,000)</th>
<th>Minor (AU $100,000–$500,000)</th>
<th>Significant (AU $500,000–$1 million)</th>
<th>Serious (AU $1 million–$10 million)</th>
<th>Catastrophic (&gt; AU $10 million)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely 30/year</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50/50 chance</td>
<td>Loss of customer due to data leakage (data loss)</td>
<td>Missing functionality (suitability)</td>
<td>Loss of business due to poor stakeholder access</td>
<td>Fine from regulator (compliance)</td>
<td></td>
</tr>
<tr>
<td>Unlikely 1/3 year</td>
<td>Operational error (usability)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very unlikely 1/30 year</td>
<td>Fine from regulator (compliance)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The current risk assessment may have identified a value-at-risk (VaR) of US $20 million per year and a need to spend approximately US $1 million–$2 million, stabilising and securing the existing system. The as-is risk profile for the current in-house system (using the risk associated with deficient characteristics from the ISO 9216 framework) is shown in figure 7. The risk profile for the business process after moving it to a private cloud (using the combined ISO 9126 and COBIT assessment framework) is shown in figure 8. A similar risk assessment (as well as an assessment of relative business value) should be conducted on the other option—an internally operated and hosted system.

Movement of the business function to a private cloud reduced the VaR to around US $2 million per annum by removing the exposure to aging, poor-performing technology, and removing the user and data security risk of having multiple copies of the system and data in circulation. At a more detailed level, an organisation may have an overall scorecard covering the combined ISO 9126 and COBIT frameworks; a detailed control assessment of applicable preventive, detective and impact controls; and a risk assessment for each risk showing inherent (prior to control) and residual (after control) impact and likelihood.

The third step in the cloud computing road map is accountability. In the case study, the business owner works

<table>
<thead>
<tr>
<th>Impact/Likelihood</th>
<th>Insignificant (&lt; AU $100,000)</th>
<th>Minor (AU $100,000–$500,000)</th>
<th>Significant (AU $500,000–$1 million)</th>
<th>Serious (AU $1 million–$10 million)</th>
<th>Catastrophic (&gt; AU $10 million)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely 30/year</td>
<td>Loss of business due to poor end-customer access</td>
<td>Operational error (usability)</td>
<td>Business disruption (reliability)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely 3/year</td>
<td>50/50 chance</td>
<td>Missing function (suitability)/security breach (user)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely 1/3 year</td>
<td>Backlog processing (time behaviour)</td>
<td>Business disruption (reliability)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very unlikely 1/30 year</td>
<td>Loss of customer due to data leakage (data loss)</td>
<td>Fine from regulator (compliance)/security breach (technical)</td>
<td>Business disruption due to disaster (reliability)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Unit Owner</th>
<th>Business Delegate (Operational Risk Manager)</th>
<th>Risk and Security Consulting and IT Risk Manager</th>
<th>Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective setting</td>
<td>Determine risk appetite for business.</td>
<td>Accept risk on behalf of owner or escalate.</td>
<td>Deliver IT services including security.</td>
</tr>
<tr>
<td>Event identification</td>
<td>Approve incident management process.</td>
<td>Monitor and escalate incidents within business.</td>
<td>Identify and manage threats and incidents.</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Approve risk and control profile.</td>
<td>Compile and monitor risk and control profile.</td>
<td>Identify and assess risk and controls.</td>
</tr>
<tr>
<td>Risk response</td>
<td>Oversee significant remediation work.</td>
<td>Oversee remediation work.</td>
<td>Execute remediation activities.</td>
</tr>
<tr>
<td>Control activities</td>
<td>Approve controls within the business and provider.</td>
<td>Operate business controls.</td>
<td>Design, integrate and operate controls.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Provide legal oversight of control assessment and testing.</td>
<td>Oversee control assessment and testing.</td>
<td>Maintain evidence of control effectiveness.</td>
</tr>
</tbody>
</table>
with the operational risk manager to develop a matrix of roles and responsibilities, shown in figure 9.

This accountability extends to process, architecture and culture through the next three principles:

6. **Mature IT processes must be followed in the cloud**—All cloud-based systems development and technical infrastructure processes must align with policy, meet agreed business requirements, be well documented and communicated to all stakeholders, and be appropriately resourced. This is related to the process dimension of BMIS. In the case study, the retail bank operational risk manager ensures that relevant policies are in place and communicated, and that a mapping of policy clauses to the assessment framework is included. A gap analysis is then performed against IT development and support processes and included in the risk and control profile.

7. **Management must buy or build management and security in the cloud**—Information risk and security, as well as its monitoring and management, must be a consideration in all cloud investment decisions. This is related to the architecture dimension of BMIS. In the case study, the departmental IT risk manager is involved in all aspects of the initiative, including vendor evaluation and management, technology review, security assessment and design, and the final investment decision.

8. **Management must ensure cloud use is compliant**—All providers and users of the cloud must comply with regulatory, legal, contractual and policy obligations; uphold the values of integrity and client commitment; and ensure that all use is appropriate and authorised. This is related to the culture dimension of BMIS. In the case study, the retail banking operational risk manager works with the compliance manager to ensure that all policies, regulations and employee codes of conduct are in place; training is performed; and compliance is periodically reviewed. The operational risk manager works with the IT risk manager and vendor manager to ensure that processes are in place to similarly assess compliance within the cloud service provider.

The final phase in the cloud computing road map is sustainability, and there are two related principles:

9. **Management must monitor risk in the cloud**—All cloud-based technology developed or acquired must enable transparent and timely reporting of information risk and be supported by well-documented and communicated monitoring and escalation processes. This is related to the enabling and support dimension of BMIS. In the case study, the retail banking operational risk manager and departmental IT risk manager work together to develop an ongoing cloud risk and security monitoring, reporting and escalation process. Ideally, this process includes regular information and escalations from the cloud service provider.

10. **Best practices must be followed in the cloud**—All cloud-based systems development and technical infrastructure related processes must consider contemporary technology and controls to address emerging information risk identified through internal and external monitoring. This is related to the emergence dimension of BMIS. In the case study, the departmental IT risk manager and IT resources involved in the cloud initiative undertake continuing education on cloud technology and related risk through formal education, industry contacts and associations such as ISACA.

**CONCLUSION**

This article has reviewed some of the existing guidance to keep in mind when considering cloud computing, suggested ISO 9126 as a valuable standard for a more structured and coherent assessment of cloud offerings, and proposed ten principles of cloud computing risk loosely based on BMIS and cloud assessment road map consisting of four guiding principles: vision, visibility, accountability and sustainability.

The framework suggested is not a panacea, as variations occur in each of the different service models (SaaS, PaaS or IaaS) and deployment models (public, community, private, or hybrid). Variations also occur depending on whether the private/community clouds are onsite, outsourced or virtual (virtual private clouds). A cloud-consuming business needs to be aware of risk variations within each cloud model and remain accountable for risk and security regardless of the cloud model or the contractual obligations of the cloud service provider.

The proposed framework could be tailored to map to these various cloud models, and it could be expanded by mapping to detailed controls within ISO 27001, COBIT, NIST and other guidance and regulatory requirements in various industries. Another area of development is an expansion of the trade-offs between the various quality characteristics (in particular, functionality, reliability and efficiency) and the ways that various cloud offerings address the issue of consistency vs. availability vs. partitioning.
ENDNOTES
1 Wei, Yi; M. B. Blake, ‘Service-Oriented Computing and Cloud Computing: Challenges and Opportunities’, IEEE Internet Computing, November/December 2010
7 ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, USA, 2011, www.isaca.org/cloud
8 The ten principles of cloud computing risk arose from a client engagement. The chief executive officer (CEO), overwhelmed with security issues, asked the chief information security officer (CISO) and his consultant (the author) to provide a list of the six principles that he should ask everyone in the organisation to follow regarding cloud computing. The author took this on as a challenge, but could not keep the list to six.

EDITOR’S NOTE
Guidance for BMIS is now incorporated in COBIT 5, www.isaca.org/cobit
How Strong Is Strong User Authentication?

Many companies (ranging from commercial to multimedia and financial sectors) have moved or are moving their services to the Internet, including critical processes such as payments. As a result, the issue of ensuring the identity of the accessing counterpart becomes critical.

Multifactor authentication (also widely known as strong authentication) has gained general consensus in the IT field as a fitting solution for such critical services. However, taking a closer look, this is true only if the basic concept is fully understood and the implementation details are designed accordingly.

This article focuses on the security of the authentication procedure set up by a service provider (SP) using a solution/tool obtained by a technical security provider (TSP). The Internet user (IU) uses the solution to access an online service by means of a personal access device (AD) equipped with a web browser (e.g., PC, smartphone, tablet). This article aims to provide organizations that are planning to introduce a strong authentication procedure with useful guidelines and warnings in view of achieving a higher level of protection.

RAISING SECURITY OF AUTHENTICATION PROCEDURES

According to current best practices and standards (e.g., ISO 27002 and COBIT® 5), adequate information security can be ensured only via a holistic approach, i.e., through a risk analysis, considering all available protection measures (including nontechnical ones) with respect to all relevant threats. However, it can be recognized that among all security measures applicable to the provision of Internet services, the authentication procedure plays a fundamental role in mitigating the insidious risk of identity theft by cyberintruders and fraudsters.

Strong authentication is generally defined as an authentication procedure requiring the combination of multiple authentication factors, including at least two of the following:

1. Knowledge—Something the user knows, e.g., a password, a personal identification number (PIN)
2. Ownership—Something the user has, e.g., token, smart card, mobile phone/SIM
3. Inherence—Something the user is, e.g., fingerprint

The rationale is that the combination of factors, which are different in nature, prevents the chance that a single vulnerability in the technical solution could undermine the security of the whole authentication procedure allowing intruders to impersonate legitimate users (i.e., identity theft). It can be viewed as a specification of the security principle, borrowed from military strategy, of defense-in-depth, in which the breach of one defense line is caught by the second line. This implies the following considerations:

• Two or more security factors can be combined to yield a strong multilayered solution, but only if they are all sound. Indeed, combining a weak factor with a stronger factor does not add much to the security provided.
• The selected factors, as used in the envisaged solution, must be mutually independent so that the compromising of one does not impact the protection level offered by the other(s).

It is worth highlighting that the aforementioned requirement of having mutually independent factors could be difficult to match. In fact, in the context of access to Internet services, when using ownership and inherence factors as well as when inputting a PIN or password, the user transmits digital data to the verifying counterpart (i.e., authentication codes), so that regardless of the generating factor, susceptibility to interception is a common vulnerability.

INDEPENDENCE AND QUALITY CHARACTERISTICS

As a consequence of the aforementioned considerations, an organization should seek a solution that entails:

• The independence of generation and transmission means of the different factors’
authentication codes. If the use of an independent channel is not viable, it is advisable to adopt ownership/inherence factors that generate short lifetime, non-reusable authentication codes, so that the risk of misuse of an intercepted or stolen code is mitigated.

- Authentication factors that are designed and managed to be uniquely bound to the legitimate user.

The latter principle can be translated to the relevant quality characteristics to be applied. In figure 1, these key characteristics are listed indicating the relevant authentication factors (knowledge, ownership and inherence—referred as K, O and I respectively) applicable to each one of them, together with explanatory notes as needed.

In addition to the characteristics listed in figure 1, whenever secrets that can be helpful in guessing passwords are stored, adequate systems and procedures should be in place for their treatment. In particular, it is recommended not to store reusable authentication codes (e.g., passwords) in the SP’s systems unless they are properly encrypted.

In regard to the ownership factors with, for example, token-generating one-time passwords (OTPs), it is advisable to evaluate solutions not involving the storage of secret codes at the TSP’s premises.

In addition to the discussed properties of quality and independence of the authentication factors, other controls need to be adopted, including factor management (e.g., tool initialization, provisioning, renewal procedures) and account management (e.g., retry limits, unblocking procedures) for which reference can be made to suitable standards/frameworks (e.g., ISO 27002, COBIT).

**Implementations in Use**

Having outlined the fundamental requirements of a strong authentication solution, this article will now discuss common cases of implementation to determine whether they meet the standards for strong authentication. In some cases, the article highlights (see items one to four of the following list) implementation mismatches with respect to the proposed independence and quality characteristics. In other cases

<table>
<thead>
<tr>
<th>Figure 1—Quality Characteristics for Authentication Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Characteristic</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>The factor is not forgeable.</td>
</tr>
<tr>
<td>The authentication codes generated are not guessable.</td>
</tr>
<tr>
<td>A common means to enforce this requirement for the knowledge factor is linked to a properly defined password policy for the authentication system. In particular, the knowledge of previously generated codes must be no use in deriving other usable values.</td>
</tr>
<tr>
<td>The factor is unfeasible to replicate.</td>
</tr>
<tr>
<td>Since inherence ensures that the authentication factor cannot be lost, the requirement could be narrowed to be applied only to the case of a non-consenting legitimate user.</td>
</tr>
<tr>
<td>The factor is not prone to be surreptitiously stolen via the Internet.</td>
</tr>
<tr>
<td>The factor is tamper-resistant.</td>
</tr>
<tr>
<td>In particular, in case of physical connection to, or integration into the access device, the code generators must be tamper-resistant against malware and network attacks. For inherence, the requirement applies to the transducer device.</td>
</tr>
</tbody>
</table>
(see items five and six), there are some possible vulnerabilities to be taken into account. The following list does not include the use of inherence factors since they are not widespread allegedly due to drawbacks and other inconveniences:

1. **The use of a password plus a grid card**—Since a grid card can be easily replicated, it cannot be considered a viable ownership factor. In addition, legitimate users in general have no way to detect if fake copies of their cards have been made, thus they will continue using the system at the same time as the fraudster.

2. **The use of a password plus a secret stored on the access device (e.g., software digital certificates, smartphone applications, embedding authentication codes)**—As long as secrets stored in the AD can be surreptitiously stolen via the Internet (e.g., through the use of malware) and used many times by the fraudster, their use together with the user password cannot be considered a sound implementation of strong authentication.

3. **A hardware token-generating OTP to be used together with the IU customer identifier (e.g., banking account number)**—Since a customer identifier is not designed and managed to be known only by the legitimate user, this is a single-factor solution and, as such, it does not provide strong authentication.

4. **A PIN-protected card used together with a card reader to obtain a OTP to access the SP site**—In this case, a knowledge factor and an ownership factor are used, but the first PIN is used only to enable the card reader and only the OTP is transmitted to the verifying entity (the SP); therefore, a possible vulnerability of the OTP would affect the security of the whole solution, likely setting aside the protection offered by the PIN. As a result, since the security of the knowledge factor is dependent on that of the ownership, this case should not be regarded as a strong authentication solution.

5. **The use of a password plus an OTP generated and transmitted to the SP by an application stored on the IU’s mobile**—Since the OTP is generated and transmitted via a second channel, this arrangement bears the features needed to provide strong authentication. However, viruses have been detected that are able to transmit from a smartphone to a PC (or vice versa) when they are connected (e.g., to synchronize their data). Therefore, specific measures to strengthen the independence of the two channels should be considered, if it is deemed opportune on the basis of the relevant risk analysis.

6. **The combination of a password with an OTP generated by a (disconnected) hardware token**—Given that these two authentication factors fulfill the requirements listed previously for knowledge and ownership factors (including, in particular, a very limited lifetime for the OTP), this widespread solution can provide an effective strong authentication. However, since the two authentication codes are put in the same device and interface, they are still vulnerable to real-time man-in-the-browser (MITB) attacks, usually via sophisticated malware. Hence, for operations requiring strict protection (e.g., high amount payments), this strong authentication can be complemented with even more advanced measures, such as the e-signature of the transaction.

---

**IS THE OTP ALONE SAFE?**

To explain why sending just an OTP as the authentication code could be risky, a significant example that can be considered a variation of the classic brute-force attack is discussed hereafter. In this example, an SP adopts a solution like those mentioned in number three or four in the previous list, making use of a six-digit OTP and allowing up to three consecutive incorrect attempts before blocking the account. An attacker knowing the username or ID of a customer (which generally is not confidential) and using a fixed number of six chosen digits—assuming that at least one successful access is made by the average legitimate user in a week—may try to enter the relevant account only three times per week. In one year, the attacker’s chances of success can be calculated using the formula in figure 2 (with $K = 3 \times 52 = 156$; $N = 1,000,000$), having assumed that the algorithm is sound and the generated numbers appear evenly random, is about one out of one thousand ($1/1,000$).

---

**Figure 2—Formula**

\[
P_N(K) = 1 - \left(\frac{N-1}{N}\right)^K
\]

$K = \text{number of attempts}$

$N = \text{possible OTP values}$

While that does not seem alarming, it can be calculated that for a massive similar attack targeted to a big SP, the
probability of success increases dramatically. For example, in a case in which the attacker knows the user ID of some 300,000 customers (e.g., by knowing the algorithm the SP has adopted to generate them), with only three tries on them all (executed by means of an automated tool), the likelihood of entering at least one of the accounts (putting $K = 3 \times 300,000$) is nearly 60 percent. Therefore, unless longer OTPs and/or other compensative measures are implemented, such a solution cannot be trusted; moreover, this example shows that a whole group of user IDs (and their formulation) should not be made publicly available.

CONCLUSION
Multifactor authentication can be deemed strong only if the choice of the technical solution and its implementation are achieved in light of sound principles and criteria, including the substantiated independence of the selected authentication factors. The stronger security of solutions not properly taking into account these requirements is questionable.

ACKNOWLEDGEMENTS
The author wishes to thank Pietro Franchini and Ravenio Parrini for their review of this article and their feedback.

DISCLAIMER
The views expressed in this article are those of the author and are not necessarily those of Banca d’Italia.

ENDNOTES
1 In spite of extensive use in the IT security sector, the notion of strong authentication has not been standardized yet in the security literature. For a basic definition, see Federal Financial Institutions Examination Council (FFIEC), “Authentication in an Internet Banking Environment,” and “FAQ,” 12 October, 2005 and 15 August, 2006.
2 Federal Financial Institutions Examination Council (FFIEC), “An authentication factor (e.g., PIN or password) is secret or unique information linked to a specific customer identifier that is used to verify that identity.”
3 As a more advanced measure, it should not be considered at all to process passwords in clear on the SP’s premises, given that the hash could have been performed at the IU client side.
4 It can be argued that using biometric characteristics such as fingerprints or irises for sensitive operations such as payments might put at risk the legitimate users of the service.
5 Besides a full-fledged e-signature, a typical solution provides for the customer to input into his/her token/card reader some transaction details so that the generated OTP is linked to the latter.
6 The formula is derived from the binomial distribution, summing the probability mass function from 1 to $K$ to yield the probability to have at least one successful try.
7 With respect to this kind of attack, an OTP can be assessed as less secure than an ordinary password with proper password policy and management. In fact, the information entropy $H$ of a randomly generated six-digit OTP (calculated by the formula $H = L\log_2N$ with $L = 6$ and $N = 10$) evaluates to about 20 bits, while according to the US National Institute of Standards and Technology (NIST) Electronic Authentication Guideline, a human-generated eight-character password using mixed case numbers and symbols can be accredited of an entropy of about 24 bits.
A Little Bit of History Repeating Itself—Nolan’s Stages Theory and the Modern IS Auditor

One of the key aspects of an information systems (IS) audit is ascertaining the maturity of the technologies in use within an organisation or department. In reality, some areas of the business’s use of IT are more mature than others, and this is particularly true of companies that have undergone recent mergers or acquisitions.

The Stages of Growth Model for IT systems was developed by Richard L. Nolan in the 1970s. Though modified over time and subject to criticism in some quarters, it is still used to discuss the growth of IT within an organisation and is used by many companies and consultants to categorise the evolution of what was originally known as data processing departments.

In this article, the six (originally four) stages are discussed, along with their direct relevance to the IS auditor. Nolan’s theory can provide a useful framework for an audit engagement, especially for the less-experienced auditor who may not have had extensive exposure to a wide range of IT organisational systems.

The Creation and Evolution of Nolan’s Theory

When Richard L. Nolan first published his theory in 1973, there was no such thing as the microcomputer. The smallest configuration available was a minicomputer, such as the DEC PDP-7. Mainframe computers were the norm, dominating large air-conditioned data centres. Expensive to buy and expensive to run, these computers mostly operated in batch mode, with jobs submitted to be run overnight. While some real-time systems were available, the expensive communication links required made these viable only for particular niche areas, such as airlines and banking.

Within this context, however, Nolan provided a vision for what could happen within an organisation if the costs of data processing were reduced. Prophetic in his approach, many of his predictions came true—first for large corporations and then for much smaller businesses.

The Stages of Growth Model has not remained static. In 1979 Nolan added two further stages as the model tried to keep up with the dramatic developments in technology at the time. Over time there have been criticisms of the theory, including the assumption that an organisation leaps from one state to another and the perception that an organisation must always strive to be benchmarked against the higher stages (i.e., data administration and maturity). Furthermore, other models have been developed that build on the work of Nolan, but attempt to alleviate what are seen by some as shortcomings. For example and perhaps in a nod to controlled risk self-assessment, the Data Management Practice Maturity Model is an approach that closely matches the original thinking of Nolan, but the theory is discussed in the context of 2012 rather than the 1970s.

Stage I—Initiation

This stage is concerned with the first introduction of technology into an organisation. While it may be hard to conceive for those who work in corporate IT, many small businesses thrive without a large IT infrastructure—consider the number of small businesses that need only a mobile phone and diary to complete their work.

The initiation stage in an organisation was identified by Nolan as being the point at which an organisation first purchases technology. In the 1970s, this was inevitably a minicomputer; now, with laptop costs tumbling and the use of smartphones for many day-to-day business functions, this starting point is much harder to determine. Personal devices are frequently being repurposed for the needs of the business. In this way, the starting point can very easily become blurred, and the increasing reliance upon IT goes unnoticed. For many small businesses, information assurance may not be a major concern, but as everyone who has lost a phone is aware, an effective backup (even of phone contacts/diary entries) is critical.
Within larger organisations, a base level of IT infrastructure is now certain to be found. However, stage I can also be applied to any emerging technologies. It is highly unusual for an innovative technology to be introduced by policy. Rather, the introduction is usually by small initial successes in pockets of the organisation’s employees acting individually. For example, consider the initial deployment of smartphones within organisations. Originally, these were purchased by the individuals who saw the potential of these devices for their personal productivity, but then expected to be able to connect these to the corporate network—frequently with little concern for the security issues surrounding mobile devices.

The internal IS auditor has a role in identifying these early accesses. They can identify best practice and suggest adoption by other areas. While this may be a good way of disseminating information, it may also inadvertently lead to many of the problems discussed in stage II.

Conversely, internal audit could identify new technologies and work with the organisation to promote the development of regulation and control. If this happens in parallel with the adoption of the technology rather than after implementation, the difficulties of stage II could be greatly reduced.

STAGE II—CONTAGION

This is a critical stage of IT growth and is identified by the proliferation of systems within the organisation. Different technologies may compete to be dominant within the organisation, e.g., the decades-old Mac vs. PC dispute. Today debates ensue, for example, about whether information itself must be held within the organisation or whether cloud computing and storage are appropriate.

In the early days of data processing, vendors were keen to ensure that their customers were ‘locked in’ to their systems and data file formats. Even agreements on the sequence for alphanumeric sorting and storage of data were proprietary, with ASCII (DEC) and EBCDIC formats used by ICL and IBM. Many of us have experienced the frustrations of different data formats, but nowadays data can often be converted between systems. Extensible Markup Language (XML) schemas and improved data quality standards have helped significantly within this area.

The danger of this stage stems from lack of control, spiralling costs, and errors that arise through the need for manual data input to transfer information among systems or incorrect controls when transferring data between systems. This growth frequently occurs at the same time as the company expands. IT can be a facilitator of growth and, at the same time, can become a victim of its own success.

Again, using the smartphone as an example, after seeing early adopters benefit from their use, more individuals and departments adopted them, but still not within a corporate framework. Hence, there has been a proliferation of models and operating systems, leading to incompatibilities and additional support demands.

The role of internal audit at this stage can be that of a sheepdog or cattle herder, providing assurance that numerous disparate systems have appropriate controls. Frequently, the internal IS auditor is uniquely placed to recognise where synergies may be possible due to their wider organisational scope. This may be particularly relevant for integrated audits that ‘combine both financial and operational audit steps’. By identifying these synergies, the internal IS auditor can assist the organisation’s progress through this chaotic stage and into stage III. If an organisation fails to do this, there are significant risks for the long-term success of both the IT within an organisation and the organisation itself.

STAGE III—CONTROL

From a management perspective, having seen the proliferation of systems present in stage II (and their usefulness), a need to introduce controls can be identified, not only on the number of systems, but also on the budgets associated with these systems. The need for this control may possibly be recognised through an internal audit, identifying that despite the early successes of stage I and the mass (but uncontrolled) proliferation of stage II, the technology is now becoming a behemoth. For example, a disaster recovery or business continuity incident may occur, which demonstrates an intolerable risk to the organisation of simply having too many systems to attempt to recover in a limited time. Recovery time objectives (RTOs) and recovery point objectives (RPOs) become impossible to achieve, as a lack of standardisation of procedures means that recovery becomes overly complex and the interruption window becomes too large for the business to tolerate.
On initial inspection, it may be considered that this stage is where internal audit should enter the process. This is not the case; internal audit may have already proposed controls that now have to be formalised and, more important, applied and monitored. If an organisation does not enforce control (with the assurance of internal audit), not only will it not progress, but it can easily slip back to stage II, as individual areas once again implement disparate IT solutions without corporate authority.

Continuing the smartphone example, at this stage internal IS auditors should identify the issues associated with the multitude of different devices in use. They may well recommend control over the devices’ use or suggest an organisational purchase policy. These recommendations should not only be directed at the actual device, but also at its use, thereby moving the technology onwards to stage IV.

**STAGE IV—INTEGRATION**

After getting the systems under control in the previous stage, the organisation may wish to further develop the maturity of the IT systems and begin to consolidate the systems and the data that underlie the core functionality of the organisation. It is at this point that the organisation-wide experience of the internal IS auditor begins to come to the forefront in an advisory role rather than in monitoring and control, further developing this role in stage V. It may be that the internal IS auditor is the only individual who has the holistic view of all levels of the organisation, particularly if a decentralised management structure (such as a matrix structure) exists.

Nowadays, integration inevitably leads to the consideration of enterprise resource planning (ERP) systems. The market for these has grown rapidly in the last 20 years, and many vendors offer services for small and medium-sized enterprises (SMEs). It is feasible, therefore, that an organisation that experiences brisk growth may be able to leaptfrog from stage I to stage IV without the plethora of systems associated with stages II and III, and with a tighter control of costs, which is particularly necessary in SMEs.

Internal audit may be tempted to rely solely upon standard reports generated by the ERP systems themselves. It is essential that the auditor’s independence, including independence from the systems themselves, is maintained. Internal IS auditors now have the potential to access vast repositories of data, this makes it essential that they consider the use of automated tools (e.g., computer-assisted audit techniques [CAATs]) to analyse the data available. The difficulty may now reside in identifying and obtaining the data sets necessary and deriving the tests to be applied upon them, rather than in assuring the relevance and accuracy of the data.

**STAGE V—DATA ADMINISTRATION**

The data administration stage is less of a technological shift, and more of a philosophical culture change within the organisation. The issue of data ownership (DO) is at the forefront at this stage. Rather than the data being owned by the IT department (or outsourced provider), the users take ownership of the data. Internal audit can help define the concept of DO within the specific context of the organisation and the allocation of a responsible person for the ownership, access and protection of the information asset.

The data within the ERP system can be opened up to a wider user base, and the organisation needs confidence (through role-based access) that the individuals know how to use the information to which they are granted access.

By this stage, the role of the internal IS auditor has shifted from that of an IT policeman to that of ensuring data and information resources are being used effectively and correctly by an organisation, complying with both external regulatory frameworks and best practice.

Continuing the mobile device example, there is a need for the internal IS auditor to ensure that individual users appreciate the issues of data being removed from the organisation and the importance of synchronisation of data, thereby ensuring integrity across the organisation. The emergence of cloud storage may help at this level, allowing clear demarcation of the data custodian, the data owner and the data user—regardless of their location and access device.

**STAGE VI—MATURITY**

The final stage identified by Nolan is achieved when all systems within an organisation are developed to their optimum state and can be said to have reached both a technological maturity and system stability commensurate with the business’s reliance upon those systems. While external benchmarking can provide some level of reassurance, it is also possible for the organisation to become complacent, in which case strategic drift could ensue. Therefore, the role of the internal IS auditor is to ensure that complacency is avoided or eliminated.

In reality, the pace of technological and business change means that systems need to be constantly developed. This could be to maintain competitive advantage, enter a new market or take advantage of (for instance) falling IT architecture costs.
Hence, although seemingly impossible to achieve, the IT maturity stage is something to which the organisation should continually strive, and the charter for the IT steering committee could identify the realisation of this stage as an ongoing and organic strategic objective.

CONCLUSION

As demonstrated, IT technologies undergo a series of incremental stages. At each stage internal and external factors will drive change forward, and overall the role of the internal IS auditor is to ensure that this occurs in a controlled manner. By associating an organisation or department with a particular stage of the model, an auditor can identify the necessary actions to drive the technology onto the higher levels, tending toward maturity. Therefore, Nolan’s model offers a useful tool to the auditor when discussing long-term strategic planning as part of an institution’s IT audit function, ensuring that senior management recognise the risk of uncontrolled IT adoption and seize the opportunities of moving forward with a coherent and structured IT strategy.

ENDNOTES

5 ISACA, CISA Review Manual 2011, USA, 2010

Register today to attend ISACA’s premier North America conference for security, risk, governance and compliance professionals 14-16 November 2012! This event combines ISACA’s Security and Governance conferences—ISRM and IT GRC—into one fantastic experience to deliver a wider range of session offerings while increasing your return on investment.
A factor to evaluate when considering using cloud storage
Facilitate, in a way
Potentially disastrous event that can be caused by viruses, data breach, or accidental deletion (2 words)
Refusing to make a statement
Web address
Social media interactions can affect a company's _____
Non-registered users
Over eight hours' work
Text messaging service, abbr.
Mark Zuckerberg: “The ____ of privacy is over”
Voice
Brown color
Chess term relating to pawn moves, abbr.
DHS campaign to help reduce cybersecurity threats: “____, Think, Connect”
What an individual seeks to live by
Creep into
World Wide Web
False front
Moral ____ (inner sense of right and wrong)
Not make an income target, for example
Excuse or overlook an ethical lapse
Recognition code
Outline
Systematic training actions
Agree
Word that appears twice in COBIT 4.1 and 23 times in COBIT 5
That is
Computers linked into a network
Code ____ in “A Few Good Men”
Atomic number 21, symbol
Gan Subramaniam, CISA, CISM, CCNA, CCSSA, CIA, CISSP, ISO 27001 LA, SSCP, is the global IT security lead for a management consulting, technology services and outsourcing company’s global delivery network. Previously, he served as head of IT security group compliance and monitoring at a Big Four professional services firm. With more than 16 years of experience in IT development, IS audit and information security, Subramaniam’s previous work includes heading the information security and risk functions at a top UK-based business process owner (BPO). His previous employers include Ernst & Young, UK; Thomas Cook (India); and Hindustan Petroleum Corp., India. As an international conference speaker, he has chaired and spoken at a number of conferences around the world.

Q  I am planning to audit one of our subsidiaries, a company that develops software and sells packaged applications. Our organisation also buys certain software that we use as tools/platforms for development. I would like to know the key clauses in licensing agreements that ought to be in place when licensing software to buyers. I am also keen to know the software licensing terms that we must have in place with our software providers.

A  Ideally, you should consult a legal expert regarding this question. However, I am responding to this from an auditor’s point of view. As always, this is an indicative list:

- Many contracts have key preambles called ‘recitals’. Recitals outline the reasons behind the signing of the contract. On many occasions, recitals explain the background and expertise of the parties involved. For example, a recital may state: ‘The licensor has expertise and experience in providing software solutions for the health care industry’. This clause is advantageous from a buyer point of view. The buyer can sue the seller should something go wrong, as the buyer can claim that he placed reliance on the expertise claimed in the recital section of the contract. It is important that recitals be clear and concise.

- The granting of the licence for use is one of the fundamental clauses in any licensing agreement. The grant-related clause describes the terms of use or the rights of the buyer with respect to the software licensed. This section must also outline the restrictions placed on the licensee in terms of the licensed software use. Rights or privileges not granted expressly must not be assumed as available. Any rights granted must be explicitly stated, for example:
  - The license should explicitly prohibit any attempts to reproduce or make or distribute by sales, lease, loan, rental, gift or sublicense by the buyer to any other third party. Users can, however, make one copy for backup purposes.
  - There can be geographical limitations. For example, the licence terms can dictate that the software be used in one particular site only.
  - The duration of the license is the next most important provision. The duration can be for a set period (post which it will be renewed at a cost), can be perpetual or can be unspecified.
  - The number of copies licensed is very important. However, the number of copies is irrelevant if the software is licensed for unlimited use.
  - The user should have no right to further modify the licensed software unless granted so.
  - The licensor should have a responsibility to release patches and fixes on a periodic basis.
  - If the licensor has hot-site or cold-site arrangements for disaster recovery purposes, the license must permit usage of such sites.

- Cost or price of the software and the terms of payment must be in the licensing agreement.

- Escrow arrangement is one of the key clauses in any software licensing arrangement. Escrow relates to the voluntary retention of a copy of the software with a mutually agreeable third party. The buyer can invoke the escrow clauses and gain access to the software source code if the seller were to go bust or shut down business operations.

The next two important clauses relate to warranty and any potential liability that may arise.

- The software must perform and meet the objectives for which it has been purchased. The buyer will obviously seek a warranty on the product. No software provider can guarantee that a product will be free of bugs or glitches. At the same time, from a buyer’s point of view, who would want to buy software that malfunctions repeatedly?

- Liability relates to the compensation due to the buyer from the seller in the event of any major incident or damage caused due to the software. The buyer usually insists on unlimited liability, but the seller must be prudent enough to limit
or cap the liability to an acceptable and reasonable fixed amount. The seller must be careful in ensuring that he does not agree to recompense any consequential loss incurred by the buyer. For example, if an airline, suffers operational loss because the ticketing software malfunctions, it would be unwise on the part of the buyer to recompense such loss. Consequential loss also includes the software company recompensing the passengers of the airline, with whom it does not have a relationship.

Again, this is just an auditor’s indicative checklist. An intellectual property (IP) lawyer would be able to advise better on the terms and conditions for an ideal licensing arrangement. There have been multiple cases in various international courts, and judgements have appeared in favour of both software sellers and buyers.

---

**Q&A**

**Start at the top. Then work your way up.**

You want to work for one of the top Internal Audit departments. We want the best and the brightest for ours.

Humana is looking for highly qualified Internal Auditors, Business Consultants, IT experts, and CPAs to join our team. We have a tradition of excellence that has helped us win prestigious awards and raise the industry bar. We’ll give you the tools and freedom to unlock your full potential and pursue a rewarding career. If you have what it takes to help us maintain these high standards, the sky’s the limit.

Find out more about careers with Humana at Careers.Humana.com

**Keyword search: IA001**
1. In the case of Infrastructure as a Service (IaaS), a cloud provider’s responsibilities usually cover the security platform configuration and maintenance, log collection, and security monitoring.

2. Standards such as ISO 27001 usually lead to organizational and technical changes, whereas specific requirements such as the Payment Card Industry Data Security Standard (PCI DSS) for credit card data define very detailed requirements, which can lead to more time-consuming and cost-consuming efforts.

3. SOC 2 and SOC 3 examinations and reports consider specific trust principles, namely security, availability, processing integrity, confidentiality and/or privacy of data and systems.

4. Among the various service organization reports, the basic difference between a Type I report and a Type II report is that a Type I report considers the design of controls at a single point in time, while a Type II report further considers the operating effectiveness of those controls over a specified period of time.

5. SOC guidance allows service auditors to rely on prior-year controls as a means of assessing controls in the current reporting period.

6. Effectively, a service organization cannot freely distribute the SOC report, including via a publicly displayed SOC 3 seal linked on its web site.

7. First and foremost, the SOC 3 report must consider the design and operating effectiveness of controls over a period; unlike SOC 1 and SOC 2, a Type I report option, in which controls may be attested to on a particular date, does not exist.

8. Service organizations must either operate the key controls relevant to the report or they must include any key controls that have been outsourced to subservice organizations.

9. Internal audit was originally expected to go beyond a static and cyclical approach, to a state of continuously optimizing the use of technology on an as-needed basis.

10. CA/CM requires a small degree of data analytics, as auditors are not to audit the whole population but only a sample of the transactions.

11. Although an increasingly larger part of organizational development takes place in projects, only one out of five development projects succeeds.

12. Project portfolio management (PPM) is the management of an organization’s development projects as a totality that systematically and consistently implements an organization’s strategy.

13. At times, it may be necessary for the executive group to prioritize programs and suspend or terminate a program or project before the date originally scheduled.

14. The table is a flexible tool, but its simultaneous use by the user and organization requires special arrangements.

15. The steering group tracking the progress of the entire portfolio can intervene in the progress of a project if its implementation begins to deviate from the original plan.

16. The risk posed by each threat agent is a monotone, increasing function of both the impact of the attacks and the probability that these attacks are successfully implemented.

17. Haruspex deals with the aforementioned problem (risk evaluation in IT security) by applying a divide-and-conquer approach that decomposes the probability of interest in its components and deals with each of them separately.
ISACA Journal
CPE Quiz
Based on Volume 3, 2012—Audit Process

Quiz #144 Answer Form

(Please print or type)

Name __________________________________________

__________________________________________________

Address _________________________________________

__________________________________________________

__________________________________________________

CISA, CISM, CGEIT or CRISC# _______________________

Quiz #144

True or False

RUHSE AND BATUROVA ARTICLE
1. __________
2. __________

VAZZANA ARTICLE
3. __________
4. __________
5. __________
6. __________
7. __________
8. __________

VASARHELYI, ROMERO, KUENKAIAEW AND LITTLEY ARTICLE
9. __________
10. __________

HEISKANEN ARTICLE
11. __________
12. __________
13. __________

BAIARDI, TELMON AND SGANDURRA ARTICLE
14. __________
15. __________
16. __________
17. __________

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

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

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

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

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

Answers—Crossword by Myles Mellor
See page 50 for the puzzle.
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 provides multiple levels of guidance.

- **Standards** define mandatory requirements for IT audit and assurance.
- They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession’s expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.

- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

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

Links to current guidance are posted on the standards page, www.isaca.org/standards. Please note that the standards are being updated and links to the exposure draft and questionnaire will be posted on www.isaca.org/standardsexposure after notice has been emailed to all ISACA members and CISAs.

The titles of issued standards documents are:

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

**IT Audit and Assurance Guidelines**
- G1 Using the Work of Other Experts Effective 1 March 2008
- G2 Audit Evidence Requirement Effective 1 May 2008
- G3 Use of Computer-assisted Audit Techniques (CAATS) Effective 1 March 2008
- G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
- G5 Audit Charter Effective 1 February 2008
- G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
- G7 Due Professional Care Effective 1 March 2008
- G8 Audit Documentation Effective 1 March 2008
- G9 Audit Considerations for Irregularities Effective 1 September 2008
- G10 Audit Sampling Effective 1 August 2008
- G11 Effect of Pervasive IS Controls Effective 1 August 2008
- G12 Organisational Relationship and Independence Effective 1 August 2008
- G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
- G14 Application Systems Review Effective 1 October 2008
- G15 Audit Planning Revised Effective 1 March 2010
- G16 Effect of Third Parties on an Organisation’s IT Controls Effective 1 March 2009
- G17 Effect of Non-audit Audit on the IS Auditor's Independence Effective 1 May 2010
- G18 IT Governance Effective 1 May 2010
- G19 Withdrawn 1 September 2008
- G20 Reporting Effective 16 September 2010
- G21 Enterprise Resource Planning (ERP) Systems Review Effective 16 September 2010
- G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
- G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
- G24 Internet Banking Effective 1 August 2003
- G25 Review of Virtual Private Networks Effective 1 July 2004
- G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
- G27 Mobile Computing Effective 1 September 2004
- G28 Computer Forensics Effective 1 September 2004
- G29 Post-implementation Review Effective 1 January 2005
- G30 Competence Effective 1 June 2005
- G31 Privacy Effective 1 June 2005
- G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
- G33 General Considerations for the Use of the Internet Effective 1 March 2006
- G34 Responsibility, Authority and Accountability Effective 1 March 2006
- G35 Follow-up Activities Effective 1 March 2006
- G36 Biometric Controls Effective 1 February 2007
- G37 Configuration and Release Management Effective 1 November 2007
- G38 Access Controls Effective 1 February 2008
- G39 IT Organisation Effective 1 May 2008
- G41 Return on Security Investment (ROI) 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) Reviews 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 2003
- P7 Irregularities and Illegal Acts Effective 1 December 2003
- P8 Security Assessment—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
- P9 Evaluation of Management Controls Over Encryption Methodologies Effective 1 January 2005
- P10 Business Application Change Control Effective 1 October 2005
- P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

**Standards for Information System Control Professionals**
- 510 Statement of Scope
  - .010 Responsibility, Authority and Accountability
  - .020 Professional Independence
  - .020 Organisational Relationship
- 520 Professional Ethics and Standards
  - .010 Code of Professional Ethics
  - .020 Due Professional Care
  - .040 Competence
  - .050 Skills and Knowledge
  - .020 Continuing Professional Education
  - .030 Planning
  - .010 Control Planning
  - .060 Performance of Work
    - .010 Supervision
    - .020 Evidence
    - .030 Effectiveness
  - .070 Reporting
    - .010 Periodic Reporting
    - .080 Follow-up Activities
    - .010 Follow-up

**Code of Professional Ethics** Effective 1 January 2011
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.

**FEATURED...**

www.isaca.org/featuredbooks

<table>
<thead>
<tr>
<th>Book Title</th>
<th>Member Price</th>
<th>Nonmember Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COBIT 5 for Information Security</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td>$35.00</td>
<td>$175.00</td>
</tr>
<tr>
<td><strong>COBIT 5 Implementation</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td>$35.00</td>
<td>$150.00</td>
</tr>
<tr>
<td><strong>Cybersecurity: The Essential Body of Knowledge</strong>&lt;sup&gt;10-IT&lt;/sup&gt;</td>
<td>$81.00</td>
<td>$91.00</td>
</tr>
<tr>
<td><strong>Effective Project Management: Traditional, Agile, Extreme, 6th Edition</strong>&lt;sup&gt;50-WPM6&lt;/sup&gt;</td>
<td>$60.00</td>
<td>$70.00</td>
</tr>
<tr>
<td><strong>The Essential Guide to Internal Auditing, 2nd Edition</strong>&lt;sup&gt;92-WIA&lt;/sup&gt;</td>
<td>$55.00</td>
<td>$65.00</td>
</tr>
<tr>
<td><strong>Implementing Service Quality Based on ISO/IEC 20000</strong>&lt;sup&gt;10-ITSQ&lt;/sup&gt;</td>
<td>$25.00</td>
<td>$35.00</td>
</tr>
<tr>
<td><strong>Information Security Policies Made Easy, Version 12</strong>&lt;sup&gt;1-BS12&lt;/sup&gt;</td>
<td>$795.00</td>
<td>$805.00</td>
</tr>
<tr>
<td><strong>Information Security Roles &amp; Responsibilities Made Easy, Version 3.0</strong>&lt;sup&gt;2-PS3&lt;/sup&gt;</td>
<td>$405.00</td>
<td>$505.00</td>
</tr>
<tr>
<td><strong>IT Governance: Policies &amp; Procedures, 2012 Edition</strong>&lt;sup&gt;5-AS12&lt;/sup&gt;</td>
<td>$245.00</td>
<td>$255.00</td>
</tr>
</tbody>
</table>

**NEW BOOKS...**

www.isaca.org/newbooks

Audit, Control and Security—Essentials

<table>
<thead>
<tr>
<th>Book Title</th>
<th>Member Price</th>
<th>Nonmember Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT Ethics and Security in the 21st Century: New Developments and Applications</td>
<td>$180.00</td>
<td>$190.00</td>
</tr>
<tr>
<td>Security Metrics: A Beginner’s Guide</td>
<td>$40.00</td>
<td>$50.00</td>
</tr>
</tbody>
</table>

Internet and Related Security

<table>
<thead>
<tr>
<th>Book Title</th>
<th>Member Price</th>
<th>Nonmember Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking Exposed 7: Network Security Secrets &amp; Solutions, 7th Edition</td>
<td>$50.00</td>
<td>$60.00</td>
</tr>
<tr>
<td>Web Application Security: A Beginner’s Guide</td>
<td>$40.00</td>
<td>$50.00</td>
</tr>
</tbody>
</table>

* 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
Caroline Wong

Learn how to communicate the value of an information security program, enable investment planning and decision making, and drive necessary change to improve the security of the enterprise. Security Metrics: A Beginner’s Guide explains, step by step, how to develop and implement a successful security metrics program.

This practical resource covers project management, communication, analytics tools, identifying targets, defining objectives, obtaining stakeholder buy-in, metrics automation, data quality, and resourcing. The reader will also get details on cloud-based security metrics and process improvement. Templates, checklists, and examples give the reader the hands-on help needed to get started right away.

2011, 432 pages. 28-MSM

Member $40.00 | Nonmember $50.00

ICT Ethics and Security in the 21st Century: New Developments and Applications
Marian Quigley

The rapid, global growth of technology necessitates a continued review of issues relating to privacy and security, as well as studies on the adoption of and access to new products, tools, and software.

ICT Ethics and Security in the 21st Century: New Developments and Applications highlights ethical dilemmas and security challenges posed by the rise of more recent technologies along with ongoing challenges such as the digital divide, threats to privacy, and organizational security measures. This book comprises a valuable resource for ICT researchers, educators, students, and professionals along with both employers and employees of large organizations searching for resolutions to the everyday ethical and security dilemmas grappled with in a highly globalised and technologized world. Topics covered include:

- Copyright and ethical issues in emerging models for the digital media reporting
- Critical infrastructure protection
- ICT and health
- Monitoring employee actions in the workplace
- Organizational and strategic Information Security Management (ISM) frameworks
- Privileged information handling in an eHealth context
- Security of personal information
- Social networks and students’ ethical behavior
- Trust in virtual communities

2011, 378 pages. 5-IGI

Member $180.00 | Nonmember $190.00
Hacking Exposed 7: Network Security Secrets & Solutions, 7th Edition
Stuart McClure, Joel Scambray, George Kurtz

Hacking Exposed 7: Network Security Secrets & Solutions is filled with all-new information on today’s most devastating attacks and proven countermeasures. The book covers: advanced persistent threats; infrastructure hacks; industrial automation and embedded devices; wireless security; the new SCADA protocol hacks; Microsoft Windows Server 2010; Web 2.0; Ubuntu Linux; hardware; Cisco; RFID; malware; and more! The 7th Edition also features a new “5 Deployments” approach for the first time that provides five key actions for every countermeasure—focused on five areas of expertise:

- Network Security
- Server Security
- Mobile Security
- Endpoint Security
- Web Security

Hacking Exposed 7 applies the authors’ computer security methodologies, technical rigor, and from-the-trenches experience to making computer technology usage and deployments safer and more secure for businesses and consumers. It uncovers new, cutting-edge computer security issues.

2012, 768 pages. 2-MCG7

Member $50.00 Nonmember $60.00

Web Application Security: A Beginner’s Guide
Bryan Sullivan, Vincent Liu

Secure web applications from today’s most devious hackers. Web Application Security: A Beginner’s Guide helps the reader stock a security toolkit, prevent common hacks, and defend quickly against malicious attacks.

This practical resource includes chapters on authentication, authorization, and session management, along with browser, database, and file security—all supported by true stories from industry. The reader will also get best practices for vulnerability detection and secure development, as well as a chapter that covers essential security fundamentals. This book’s templates, checklists, and examples are designed to help the reader get started right away.

2011, 352 pages. 29-MWAS

Member $40.00 Nonmember $50.00

Inventory Reduction Sale

Books offered in the ISACA Bookstore Special Sale may contain dated material, overall these books are still of value. Sales prices effective while quantities are available.

Visit www.isaca.org/salesbooks for available titles and pricing.
To prepare for the December 2012 CISA exam, order
www.isaca.org/cisabooks

To prepare for the December 2012 CISM exam, order
www.isaca.org/cismbooks

To prepare for the December 2012 CGEIT exam, order
www.isaca.org/cgeitbooks

To prepare for the December 2012 CRISC exam, order
www.isaca.org/criscbooks

Certified Information Security Manager (CISM®) Review Questions, Answers & Explanations Manual 2012*
### 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>CISM-12</td>
<td>CISA Review Manual 2012*</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CISM-12C</td>
<td>Chinese Simplified Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CISM-12F</td>
<td>French Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CISM-12I</td>
<td>Italian Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CISM-12J</td>
<td>Japanese Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CISM-12S</td>
<td>Spanish Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
</tbody>
</table>

### CISA Review Questions, Answers & Explanations Manual 2012 Supplement*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDB-12S</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>225.00</td>
<td>190.00</td>
</tr>
<tr>
<td>CDB-12W</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>185.00</td>
<td>155.00</td>
</tr>
<tr>
<td>CRM-12S</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>135.00</td>
<td>105.00</td>
</tr>
</tbody>
</table>

### CISA Review Questions, Answers & Explanations Manual 2011*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CQA-11E</td>
<td>English Edition</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>CQA-11C</td>
<td>Chinese Simplified Edition</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>CQA-11I</td>
<td>Italian Edition</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>CQA-11J</td>
<td>Japanese Edition</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>CQA-11S</td>
<td>Spanish Edition</td>
<td>130.00</td>
<td>100.00</td>
</tr>
</tbody>
</table>

### CISA Practice Question Database v12 (1,100 Questions)*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDB-12S</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>225.00</td>
<td>190.00</td>
</tr>
<tr>
<td>CRM-12S</td>
<td>E-Book—PDF format (purchase online only)</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>CM-12</td>
<td>CISM Review Manual 2012*</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CM-12J</td>
<td>Japanese Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CM-12S</td>
<td>Spanish Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
</tbody>
</table>

### CISM Review Questions, Answers & Explanations Manual 2012*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CQA-12</td>
<td>English Edition</td>
<td>90.00</td>
<td>70.00</td>
</tr>
<tr>
<td>CQA-12J</td>
<td>Japanese Edition</td>
<td>90.00</td>
<td>70.00</td>
</tr>
<tr>
<td>CQA-12S</td>
<td>Spanish Edition</td>
<td>90.00</td>
<td>70.00</td>
</tr>
</tbody>
</table>

### CISM Review Questions, Answers & Explanations Manual 2012 Supplement*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CQA-12S</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>CQA-12J</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>CQA-12S</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>130.00</td>
<td>100.00</td>
</tr>
</tbody>
</table>

### CISM Practice Question Database v12 (800 Questions)*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM-12</td>
<td>E-Book—PDF format (purchase online only)</td>
<td>160.00</td>
<td>120.00</td>
</tr>
<tr>
<td>MDM-12W</td>
<td>Download—English Edition</td>
<td>160.00</td>
<td>120.00</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>CGD-11</td>
<td>CGEIT Review Questions, Answers &amp; Explanations Manual 2011 (80 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CGA-11</td>
<td>Candidate’s Guide to the CGEIT Exam and Certification</td>
<td>15.00</td>
<td>5.00</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</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CRQ-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>CACR*</td>
<td>Candidate’s Guide to the CRISC Exam and Certification</td>
<td>15.00</td>
<td>5.00</td>
</tr>
</tbody>
</table>
### AUDIT, CONTROL AND SECURITY—ESSENTIALS

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>48-CRC</td>
<td>Access Control, Security, and Trust: A Logical Approach</td>
<td>190.00</td>
<td>90.00</td>
</tr>
<tr>
<td>1-IT9</td>
<td>Accounting Information Systems, 5th Edition</td>
<td>258.00</td>
<td>246.00</td>
</tr>
<tr>
<td>93-WAAS</td>
<td>Auditing and Assurance Services: Understanding the Integrated Audit</td>
<td>223.00</td>
<td>213.00</td>
</tr>
<tr>
<td>6-PL</td>
<td>Auditing IT Infrastructures</td>
<td>105.00</td>
<td>95.00</td>
</tr>
<tr>
<td>76-WGL</td>
<td>Build Your Own Security Lab: A Field Guide for Network Testing</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>43-CRC</td>
<td>Building an Effective Information Security Policy Architecture</td>
<td>94.00</td>
<td>84.00</td>
</tr>
<tr>
<td>31-CRC</td>
<td>Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI</td>
<td>140.00</td>
<td>130.00</td>
</tr>
<tr>
<td>79-WCAF</td>
<td>Computer-Aided Fraud Prevention and Detection: A Step by Step Guide</td>
<td>74.00</td>
<td>64.00</td>
</tr>
<tr>
<td>4-IGI</td>
<td>Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions</td>
<td>110.00</td>
<td>100.00</td>
</tr>
<tr>
<td>51-CRC</td>
<td>Data Protection: Governance, Risk Management, and Compliance</td>
<td>86.00</td>
<td>76.00</td>
</tr>
<tr>
<td>50-WPMI</td>
<td>Effective Project Management: Traditional, Agile, Extreme, 3rd Edition</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-ABEES</td>
<td>Enterprise Security for the Executive: Setting the Tone from the Top</td>
<td>45.00</td>
<td>35.00</td>
</tr>
<tr>
<td>92-WA</td>
<td>The Essential Guide to Internal Auditing, 2nd Edition</td>
<td>65.00</td>
<td>55.00</td>
</tr>
<tr>
<td>71-WCF</td>
<td>Essentials of Corporate Fraud</td>
<td>58.00</td>
<td>48.00</td>
</tr>
<tr>
<td>82-WACL</td>
<td>Fraud Analysis Techniques Using ACL</td>
<td>221.00</td>
<td>211.00</td>
</tr>
<tr>
<td>11-IT</td>
<td>Guide to Firewalls and VPNs, 3rd Edition</td>
<td>165.00</td>
<td>155.00</td>
</tr>
<tr>
<td>5-IGI</td>
<td>ICT Ethics and Security in the 21st Century: New Developments and Applications</td>
<td>190.00</td>
<td>180.00</td>
</tr>
<tr>
<td>7-ART</td>
<td>Implementing the ISO/IEC 27001 Information Security Management System Standard</td>
<td>105.00</td>
<td>95.00</td>
</tr>
<tr>
<td>2-ABA</td>
<td>Information Security and Privacy: A Practical Guide for General Executives, Lawyers and Technologists</td>
<td>106.00</td>
<td>96.00</td>
</tr>
<tr>
<td>83-WIS</td>
<td>Information Storage and Management: Storing, Managing, and Protecting Digital Information</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>4-CRC</td>
<td>Information Technology Control and Audit, 3rd Edition</td>
<td>100.00</td>
<td>90.00</td>
</tr>
<tr>
<td>95-WASA</td>
<td>Information and Application of International Standards on Auditing IT, Audit, and Security</td>
<td>115.00</td>
<td>105.00</td>
</tr>
<tr>
<td>90-WACS</td>
<td>IT Audit, Security, and Privacy</td>
<td>95.00</td>
<td>85.00</td>
</tr>
</tbody>
</table>

### IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>WITCOC*</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>50.00</td>
<td>FREE</td>
</tr>
<tr>
<td>ICTOC*</td>
<td>Print Format</td>
<td>60.00</td>
<td>35.00</td>
</tr>
<tr>
<td>STPRA*</td>
<td>IT Standard and Guidelines of Standards and Tools and Techniques for Audit and Control Professionals</td>
<td>20.00</td>
<td>15.00</td>
</tr>
<tr>
<td>WITAF*</td>
<td>ITAF: A Professional Practices Framework for IT Assurance e-book—PDF (purchase online only)</td>
<td>45.00</td>
<td>FREE</td>
</tr>
<tr>
<td>15-MT2</td>
<td>IT Auditing Controls to Protect Information Assets, 2nd Edition</td>
<td>80.00</td>
<td>70.00</td>
</tr>
</tbody>
</table>

### IT Control Objectives for Basel II

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>WITCOB*</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>35.00</td>
<td>FREE</td>
</tr>
<tr>
<td>ICTOCB*</td>
<td>Print Format</td>
<td>50.00</td>
<td>20.00</td>
</tr>
</tbody>
</table>

### IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>22-MSM</td>
<td>IT Security Metrics: A Practical Framework for Measuring Security &amp; Protecting Data</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>6-ITSO</td>
<td>IT Strategic and Operational Controls</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-IA</td>
<td>A New Auditor’s Guide to Planning, Performing, and Presenting IT Audits</td>
<td>80.00</td>
<td>70.00</td>
</tr>
<tr>
<td>7-5NY9</td>
<td>PCI Compliance, Second Edition</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-PIA</td>
<td>Practical IT Auditing with current Supplement</td>
<td>445.00</td>
<td>435.00</td>
</tr>
<tr>
<td>12-IT</td>
<td>Principles of Information Security, 4th Edition</td>
<td>152.00</td>
<td>142.00</td>
</tr>
<tr>
<td>2-SAPP</td>
<td>SAP Security and Risk Management, 2nd Edition</td>
<td>80.00</td>
<td>70.00</td>
</tr>
<tr>
<td>28-MSMG</td>
<td>Security Metrics: A Beginner’s Guide</td>
<td>50.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

### AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-MAO</td>
<td>Applied Oracle Security: Developing Secure Database and Middleware Environments</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>4-DC</td>
<td>Audit Guidelines for DB2</td>
<td>80.00</td>
<td>70.00</td>
</tr>
<tr>
<td>53-CRC</td>
<td>FSIWA Principles and Best Practices: Beyond Compliance</td>
<td>90.00</td>
<td>80.00</td>
</tr>
<tr>
<td>10-ART</td>
<td>Identity Management: Concepts, Technologies, and Systems</td>
<td>110.00</td>
<td>100.00</td>
</tr>
</tbody>
</table>

### Linux: Security, Audit and Control Features

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLN*</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>30.00</td>
<td>15.00</td>
</tr>
<tr>
<td>PUN*</td>
<td>Print Format</td>
<td>50.00</td>
<td>35.00</td>
</tr>
</tbody>
</table>

### INTERNET AND RELATED SECURITY TOPICS

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>19-M24</td>
<td>24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>45-CRC</td>
<td>Cloud Computing: Implementation, Management, and Security</td>
<td>90.00</td>
<td>80.00</td>
</tr>
<tr>
<td>11-EL</td>
<td>Cyber Attacks: Protecting National Infrastructure</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-CAPS</td>
<td>Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 3rd Edition</td>
<td>48.00</td>
<td>38.00</td>
</tr>
<tr>
<td>2-SCC</td>
<td>Cybercrimes: A Multidisciplinary Analysis</td>
<td>199.00</td>
<td>189.00</td>
</tr>
<tr>
<td>10-IT</td>
<td>Cybersecurity: The Essential Body of Knowledge</td>
<td>91.00</td>
<td>81.00</td>
</tr>
<tr>
<td>90-MG9</td>
<td>Gray Hat Hacking: The Ethical Hackers Handbook, 3rd Edition</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>15-MME</td>
<td>Hacking Exposed Web Applications, 3rd Edition</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>33-MCG7</td>
<td>Hacking Exposed 7: Network Security Secrets &amp; Solutions, 7th Edition</td>
<td>60.00</td>
<td>50.00</td>
</tr>
</tbody>
</table>

### NON-MEMBER RESOURCES

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>2012 Nonmember Price</th>
<th>2012 Member Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-TCA</td>
<td>Administration de la Seguridad de Información</td>
<td>55.00</td>
<td>45.00</td>
</tr>
</tbody>
</table>

### CISA Examination Reference Material

- Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the December 2012 CISA exam—see page 55

### CISM Examination Reference Material

- Study aids available in Japanese and Spanish for the December 2012 CISM exam—see page 55

### COBIT 3rd Edition

- Available at the following web site

### COBIT 4.1 Edition

- Available at the following web sites

### Meyco CBBIT Suite

Meyco CBBIT es un software completo e integrado para la implementación de COBIT como una herramienta para el Buen Gobierno de la TI, Seguridad de la TI e Aseguramiento de la TI según COBIT 4.1. (see www.isaca.org/nonenglishbooks para descripción y precios)
<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>94-WIERS</td>
<td>An Executive Guide to IFRS: Content, Costs and Benefits to Business</td>
<td>50.00</td>
<td>40.00</td>
</tr>
<tr>
<td>3-PAGE</td>
<td>7 Steps to Better Written Policies and Procedures</td>
<td>30.00</td>
<td>20.00</td>
</tr>
<tr>
<td>4-PAGE</td>
<td>Best Practices in Policies and Procedures</td>
<td>36.00</td>
<td>20.00</td>
</tr>
<tr>
<td>1-ITG</td>
<td>Board Briefing on IT Governance, 2nd Edition</td>
<td>7.00</td>
<td>7.00</td>
</tr>
<tr>
<td>6-SYN</td>
<td>Business Continuity and Recovery Planning for IT Professionals</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>BMFS*</td>
<td>The Business Model for Information Security</td>
<td>60.00</td>
<td>45.00</td>
</tr>
<tr>
<td>54-WDO2</td>
<td>CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition</td>
<td>75.00</td>
<td>65.00</td>
</tr>
<tr>
<td>WCCS*</td>
<td>Creating a Culture of Security (e-book)</td>
<td>50.00</td>
<td>FREE</td>
</tr>
<tr>
<td>11-ITDG</td>
<td>The Data Governance Imperative</td>
<td>50.00</td>
<td>40.00</td>
</tr>
<tr>
<td>37-CRC</td>
<td>Digital Privacy: Theory, Technologies, and Practices</td>
<td>90.00</td>
<td>60.00</td>
</tr>
<tr>
<td>89-WEG</td>
<td>Empowering Green Initiatives with IT: A Strategy and Implementation Guide</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>9-ART</td>
<td>Enterprise Information Security and Privacy</td>
<td>109.00</td>
<td>99.00</td>
</tr>
<tr>
<td>13-IT</td>
<td>Ethics in Information Technology, 4th Edition</td>
<td>101.00</td>
<td>91.00</td>
</tr>
<tr>
<td>23-WIT</td>
<td>The Executive’s Guide to Information Technology, 2nd Edition</td>
<td>110.00</td>
<td>100.00</td>
</tr>
<tr>
<td>10-VH</td>
<td>Foundations of IT Service Management Based on ITIL® V3</td>
<td>65.00</td>
<td>55.00</td>
</tr>
<tr>
<td>3-VH</td>
<td>Frameworks for IT Management</td>
<td>65.00</td>
<td>55.00</td>
</tr>
<tr>
<td>85-WF10</td>
<td>Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition</td>
<td>65.00</td>
<td>55.00</td>
</tr>
<tr>
<td>64-WURC</td>
<td>Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and Informational Guidance and Best Practices</td>
<td>173.00</td>
<td>163.00</td>
</tr>
<tr>
<td>7-ITGR</td>
<td>Green in IT, 2nd Edition</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>20-MHE</td>
<td>Hacking Exposed Malware and Rootkits: Malware &amp; Rootkits Secrets &amp; Solutions</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>67-WHF</td>
<td>Human Face of Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation</td>
<td>62.00</td>
<td>52.00</td>
</tr>
<tr>
<td>1-IBM</td>
<td>The IBM Data Governance Unified Process</td>
<td>35.00</td>
<td>25.00</td>
</tr>
<tr>
<td>WIGUA</td>
<td>Identifying and Aligning Business Goals and IT Goals</td>
<td>35.00</td>
<td>20.00</td>
</tr>
<tr>
<td>4-ID</td>
<td>Implementing Information Technology Governance: Models, Practices and Cases</td>
<td>110.00</td>
<td>100.00</td>
</tr>
<tr>
<td>46-CRC</td>
<td>Implementing the Project Management Balanced Scorecard</td>
<td>90.00</td>
<td>90.00</td>
</tr>
<tr>
<td>19-ITSG</td>
<td>Implementing Service Quality Based on ISO/IEC 20000</td>
<td>35.00</td>
<td>25.00</td>
</tr>
<tr>
<td>2-ITGO</td>
<td>Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition</td>
<td>7.00</td>
<td>7.00</td>
</tr>
<tr>
<td></td>
<td>Information Security Governance: Guidance for Information Security Managers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-ITG</td>
<td>Information Security Governance: Guidance for Information Security Managers</td>
<td>50.00</td>
<td>25.00</td>
</tr>
<tr>
<td>W3STG*</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>45.00</td>
<td>FREE</td>
</tr>
<tr>
<td>WSH*</td>
<td>Information Security Harmonisation: Classification of Global Guidance (E-book—PDF format purchase online only)</td>
<td>40.00</td>
<td>FREE</td>
</tr>
<tr>
<td>1-BS12</td>
<td>Information Security Policies Made Easy, Version 12</td>
<td>805.00</td>
<td>795.00</td>
</tr>
</tbody>
</table>

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

Order online at www.isaca.org/bookstore

Mail completed form with payment:

ISACA/ITGI
1055 Paseo Sphere Circle
Chicago, IL 60674-1055 USA

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

Phone: +1.847.660.5650

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/V A T charges levied by the country of destination. See www.isaca.org/shipping for further information.
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 ________________________________________________________________

Phone Number ( ) ______________________ Fax 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 of Cardholder ____________

Shipping & Handling Rates for Orders

All orders outside the US are shipped Federal Express Priority.

<table>
<thead>
<tr>
<th>For Orders Totaling</th>
<th>Outside US</th>
<th>Within US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to $30.00</td>
<td>US $10.00</td>
<td>US $5.00</td>
</tr>
<tr>
<td>$30.01 to $50.00</td>
<td>US $15.00</td>
<td>US $7.00</td>
</tr>
<tr>
<td>$50.01 to $80.00</td>
<td>US $20.00</td>
<td>US $8.00</td>
</tr>
<tr>
<td>$80.01 to $150.00</td>
<td>US $26.00</td>
<td>US $10.00</td>
</tr>
<tr>
<td>Over US $150.00</td>
<td>17% of Total</td>
<td>10% of Total</td>
</tr>
</tbody>
</table>

No shipping charges apply to Myecor COBIT.
No shipping charges apply to CISA Practice Question Database v.12—download.
No shipping charges apply to CISM Practice Question Database v.12—download.

Subtotal __________________________

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.

TOTAL __________________________

Shipping & Handling Rates for Orders

International customers are solely responsible for paying all custom duties, service charges, and taxes levied by their country.

Shipping details www.isaca.org/shipping

All purchases are final. Pricing, shipping and handling, and tax are subject to change without notice.
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.
UNEQUALLED INFORMATION SECURITY RISK PROFILING AND ASSESSMENT SYSTEM TO MONITOR AND REPORT AGAINST PRIMARY REGULATIONS AND STANDARDS FOR ALL OF YOUR KEY INTERNAL AND EXTERNAL SYSTEMS

- TOUCH OF A BUTTON STATUS REPORTING — BY REGION, BY REGULATION, BY FUNCTION, BY RISK, ...
- BUILT-IN PROCESS AUTOMATION TO INCREASE PRODUCTIVITY AND MASSIVELY REDUCE ADMINISTRATION EFFORT
- ‘ASK ONCE/SATISFY MANY’ DESIGN TO ENSURE A LEAN BUT APPROPRIATE EXPERIENCE BY YOUR CUSTOMER AND STAKEHOLDER GROUPS

OUR UNIQUE GRC DATA WAREHOUSING CAPABILITIES CAN ALSO UNLOCK THE VALUE FROM YOUR EXISTING SECURITY AND COMPLIANCE APPLICATIONS

AdaptiveGRC — Stay Ahead, Way Ahead

"WHAT I REALLY LIKE ABOUT THIS SOLUTION IS THAT IT COMBINES CONTROL MATERIAL AND FUNCTIONALITY THAT YOU DON’T FIND ANYWHERE ELSE"

— HEAD OF TECHNOLOGY AUDIT & ASSESSMENT FROM A FORTUNE 50 COMPANY

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.

SUPERIOR BUSINESS TECHNOLOGY SOLUTIONS, DELIVERED FASTER