Volume 2, 2015

ISACA® Journal

OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGY

Featured articles:

Internet of Things Offers Great Opportunities and Much Risk

Strategic Alignment and E-health Governance

Cloud Insecurities

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

FIND THE **RIGHT TALENT**. FIND THE **RIGHT JOB**.

EITHER WAY, YOUR SEARCH CAN END **RIGHT HERE**.

CONNECT MORE

Whether you are searching for a job or looking for that perfect candidate for your open position, **ISACA's Online Career Centre** is *the* source for IS/IT audit and information security professionals.

EMPLOYERS:

Designations and experience are highlighted providing a special opportunity for those interested in hiring CISA®, CISM®, CGEIT® or CRISC™ holders and applicants with COBIT experience.

JOB SEEKERS:

Take advantage of advanced search features, job alerts, career advice and much more!

More than **450** new jobs posted

350+ new employers posted jobs

735 searchable resumes on average

240,000+ unique page views in 2014

Nearly **50,000** new visitors in 2014

ISACA®

Trust in, and value from, information systems

Visit our Career Centre today at *www.isaca.org/CareerCentre* to learn more.

infosecurity®
EUROPE
• 02-04 June 2015 • Olympia • London •

Securing the connected enterprise

Join Europe's biggest free-to-attend information security conference & exhibition

www.infosecurityeurope.com

Collect **CPE/CPD** credits

REGISTER YOUR INTEREST NOW

www.infosecurityeurope.com

- **98.1%** of 2014 visitors, were satisfied to completely satisfied
- **84.1%** of visitors are very likely to recommend participating in Infosecurity Europe to a colleague
- **96.6%** of 2014 visitors are more than likely to attend in 2015
- **97.2%** of exhibitors were satisfied in 2014 and 80% have already rebooked to participate in 2015
- **£447.5m** of future orders expected to be placed with exhibitors as a direct result of Infosecurity Europe 2014

CELEBRATING 20 YEARS

02-04 JUNE15
OLYMPIALONDONUK

Managed by: infosecurity GROUP

Part of: Reed Exhibitions

VOLUME 2, 2015

ISACA® Journal

Columns

Features

Plus

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

Online-Exclusive Features

Do not miss out on the *Journal's* online-exclusive content. With new content weekly through feature articles and blogs, the *Journal* is more than a static print publication. Use your unique member login credentials to access them at *www.isaca.org/journal.*

Online Features
The following is a sample of the upcoming features planned for March and April.

Book Review: Cybersecurity: The Essential Body of Knowledge
Reviewed by Dauda Sule, CISA

ERP Implementation in the Education Sector
Manas Tripathi and Arunabha Mukhopadhyay, Ph.D.

Book Review: Fraud Prevention and Detection
Reviewed by Upesh Parekh, CISA

IS Audit Basics: Auditor: About Yourself (And How Others See You)
Ed Gelbstein, Ph.D.

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

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

Follow ISACA on Twitter: *http://twitter.com/isacanews;* Hash tag: #ISACA

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

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

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

The **projected growth rate** for the information security analyst profession between 2012 and 2020

SOURCE: BUREAU OF LABOR STATISTICS, 2014

Do you have what it takes to answer the call?

Elevate your information security career with one of Capella's new MS in Information Assurance and Security options: **Digital Forensics** | **Network Defense**

Your future is waiting. Start now. CAPELLA.EDU/ISACA OR 1.866.670.8737

See graduation rates, median student debt, and other information at www.capellaresults.com/outcomes.asp.

Capella University

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

Cyberwhatsit

I did a Google search on the word *cyber* and was told there are 467 million references to that term. This seems to me an awfully exact number, but I guess we can agree there are a lot of references. But references to what exactly? Cyber*crime*? Cyber*attacks*? Cyber*threats*? Cyber*security*? For fun, I looked at the 20th page of the Google search and found cyberrisk, cybercareer and cybercafe. Languages (well, English anyway) have an enormous capacity for newspeak through the combination of an adjective and a noun. This little linguistic interlude would be an interesting aside, except that I think it points to a genuine obstacle to progress in countering the problems connoted as cyber. We need targeted countermeasures to the targeted threats posed by Internet-enabled terrorists, state-sponsored spies and saboteurs, misguided political activists, and criminals. A lack of verbal clarity is not going to help.

There is, I believe, a correlation between fuzzy speech and fuzzy thinking. If we are not clear about what we consider the problem to be, we are more likely to be off-target in developing the necessary solutions. Objectives matter. No matter how great the risk of directed misuse of information resources, budgets for mitigating those risk factors are limited and those responsible for safeguarding those resources can ill afford applying the allocated money inappropriately.

CYBERTHEFT

Donn Parker, perhaps the earliest chronicler of crimes committed by computers, suggested many years ago that even automated murder was possible.[1] And indeed, if a life-support system is computerized, would not disabling its system constitute the ultimate felony? However, in the current usage, the term cybercrime is generally applied to stealing information. And, even that takes several forms. The one that seems to make it into the headlines most often is the theft of personally identifiable information (PII), especially information that can be readily monetized, i.e., credit card numbers and authenticators. Target and Home Depot have been recent and well-publicized victims of such crimes, which are, in actuality, privacy violations. As such, I propose that the tools of privacy protection, such as encryption, compartmentalization and disposal, are best applied to stop this sort of theft.

There is another type of cybercrime that I consider even more insidious: theft of proprietary information. Gen. Keith Alexander, director of the US National Security Agency (NSA) and commander of the US Cyber Command, has said that the loss of industrial information and intellectual property through cyberespionage constitutes the "greatest transfer of wealth in history."[2] He ought to know. Once again, encryption is probably the tool of choice, but since the information needs to be decrypted to be used, encryption is an incomplete solution. If the information is as valuable as Gen. Alexander implies, perhaps it should be kept on separate, classified systems as is done in the military.

Criminals do have another way of making cybercrime pay, by stealing information assets that have intrinsic value. Sony has recently been victimized in this way.[3] The only sure way to protect valuable property is to lock it in a vault. In computer terms, this means not storing information resources that are valuable in themselves on Internet-accessible devices.

CYBERATTACKS

To my way of thinking and speaking, an attack—cyber or otherwise—implies intent to harm a person or organization. Stealing information is harmful, to be sure, but it does not undermine an organization's essential business functions. I reserve the word *cyberattack* for cases in which an organization is prevented from carrying out its intended mission. Cyberattacks threaten the integrity or the very existence of information and have the potential to bring a business to a halt. When Saudi Aramco and RasGas were attacked in 2012, up to 30,000 computers were wiped clean, replacing their contents with the image of

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:

a burning American flag. These attacks were linked to Iran.[4] Such destructive attacks can only be combatted, to my way of thinking, by adopting zero-trust architectures based on next-generation firewalls.[5]

A variant on destructive attacks is one in which the integrity of a system is violated. Perhaps the most notorious of these was Stuxnet, malware originated by Israel and the US, according to many sources, including Edward Snowden, formerly of the NSA.[6] He ought to know. This attack was designed to "physically damage the facility's infrastructure by throwing off automated systems and cover its tracks so that even if engineers were monitoring those systems, everything would appear normal."[7] I have previously advocated frequent validation of the integrity of software,[8] which might have arrested the damage of Stuxnet. One might say that all cyberattacks on software or information integrity are failures of change management, so strengthening these controls is also a tool against cyberattacks.

> We can only win if we fight the right fights with the right tools against the right enemies.

CYBERTHREATS AND CYBERSECURITY

We live in threatening times that these malefactors of great stealth have bestowed upon us. It is what Thomas Friedman of *The New York Times* calls "the struggle between 'makers' and 'breakers' on the Internet."[9] I have confidence that we who make and protect information systems will win out in the end. But let us not overlook the depth of resources, talent and time that the breakers have at their disposal.

We can only win if we fight the right fights with the right tools against the right enemies. **Figure 1** summarizes the cybertaxonomy (aha, another cyberneologism…and another!) discussed above.

It demonstrates that the cyberthreats are not all the same; they come from different sources, each with different impacts and safeguards. We set back the cause of the makers by treating cybersecurity as a monolith. One size fits nobody. The breakers are not all alike and the response by the makers must be nuanced as well. If we are clear in our minds as to whom and what we are fighting, we are a great deal more likely to win.

Figure 1—Different Types of Cyberthreats

Types of Assault	Intended Effects	Probable Sources	Recent Victims	Selected Countermeasures
Stealing PII	Credit card fraud; blackmail	Criminals	Target, Home Depot	Encryption, compartmentalization, disposal
Theft of intellectual property	Industrial espionage	Governments, hacktivists	Sony	Encryption, classified systems
Theft of valuable information resources	Piracy	Criminals	Sony	Segregation, air gap
Destructive attack	Destruction of information	Governments, terrorists	Saudi Aramco, RasGas	Zero-trust architecture, next-generation firewalls
Integrity attack	Manipulation of systems or data	Governments, terrorists	Iranian nuclear program	Software validation, change management

ENDNOTES

[1] Kearns, Helen; "The Dawn of Computer Crime: Theft Today…Is Murder Next?," *Montréal Gazette*, 17 May 1978, *http://news.google.com/newspapers?nid=1946&dat=19780517&id=_DgyAAAAIBAJ&sjid=b6QFAAAAIBAJ&pg=4051,330681*. This article quotes Donn Parker, the bald eagle of information security and someone I consider a friend and a mentor. He was talking about cybercrime before most of us could spell cyber.

[2] Rogin, Josh; "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy*, 9 July 2012, *http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/*

[3] Barnes, Brooks; Nicole Perlroth; "Sony Films Are Pirated, and Hackers Leak Studio Salaries," *The New York Times*, 2 December 2014, *www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html?module=Search&mabReward=relbias%3Ar*

[4] Perlroth, Nicole; "Report Says Cyberattacks Originated Inside Iran," *The New York Times*, 2 December 2014, *www.nytimes.com/2014/12/03/world/middleeast/report-says-cyberattacks-originated-inside-iran.html?module=Search&mabReward=relbias%3Ar*

[5] Beck, Eric J.; "How Zero-trust Network Security Can Enable Recovery from Cyberattacks," *ISACA Journal*, vol. 6, 2014, p. 14-18, *www.isaca.org/journal*. Full disclosure: Eric Beck is my business partner at Risk Masters.

[6] Ferran, Lee; "Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet," *ABC News*, 9 July 2013, *http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/*

[7] *Ibid*.

[8] Ross, Steven J.; "CyberCERT," *ISACA Journal*, vol. 5, 2014, *www.isaca.org*

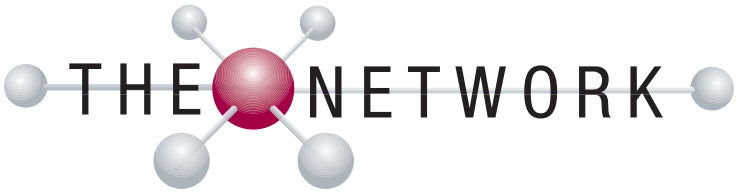
[9] Friedman, Thomas; "Makers and Breakers," *The New York Times*, 8 November 2014, *www.nytimes.com/2014/11/09/opinion/sunday/thomas-l-friedman-makers-and-breakers.html?module=Search&mabReward=relbias*

The center of cybersecurity knowledge and expertise.

CSX™
CYBERSECURITY NEXUS

Created by the leading minds in the field, Cybersecurity Nexus™ (CSX) brings you a single source for all things cybersecurity. From certification, education and training—to webinars, workshops, industry events, career management and community—you'll find everything you need to take your career to the next level. And, we've designed CSX to help you every step of the way, no matter what your level of experience. Connect with the resources, people and answers you need... visit us today at www.isaca.org/cyber2015

ISACA®



Lilia Liu Chung, CRISC, CFE, COBIT 5 Foundation

Lilia Liu Chung has more than 20 years of experience in information technology with emphasis on implementing of industry best practices. She has a background as an advisor in computer crime, white-collar crime and corporate fraud, and security of IT; a chief information officer; an information systems auditor; and a legal advisor.

Q: *How do you think the role of the IS auditor is changing or has changed? What would be your best piece of advice for IS auditors as they plan their career paths and look at the future of IS auditing?*

A: The role of the auditor has evolved as new technologies have emerged and become part of our daily activities. As we integrate new technologies, using them makes organizations vulnerable to new risk, not only technological, but reputational, operational, etc. As auditors, we must be prepared for any kind of associated risk. Mostly, we find organizations that upload data to the cloud or use social networks, big data, or wireless devices, such as cell phones, tablets, USB sticks and others, have fragile security procedures that are capable of being impaired by any internal or external attack. The lack of policies, periodic reviews, adequate supervision or continuous monitoring may cause problems for organizations. My best advice for auditors as they plan their futures is to discuss what they want to be, where they want to go, what scope they want in their career and what contribution they want to provide to society with their work. The advantage of auditors is that they can work in any company regardless of industry or sector. Though as a result, the auditor must document, study and tap into a broad knowledge base.

Q: *Your experience ranges from computer crime and corporate fraud consulting to IT security to IS audit. Please describe the adjustments you have made in your career to complete these transitions and how you have used your experiences in each role to better you for the next.*

A: I had to make adjustments throughout my career because I have seen that a technical degree in computer systems engineering, while very comprehensive, falls short. By supplementing that degree with a master's in business administration with an emphasis in finance, I came to understand that technology goes hand in hand with business objectives, how to determine which way is the north of the organization, possible financial problems, and how the economy is moving regionally and globally.

Today, computer crime is the order of the day. Thus, I've drawn my attention to the study of crime and I also participate with a number of associations in the fight against fraud. As a lawyer specializing in technology issues, I have had the opportunity to review contracts on service level agreements, prepare contracts, see and prepare intellectual property issues, and participate as an expert on issues of cybercrime. It is never too late to study and train. We must be continuously learning to keep up with the always evolving technology race.

Q: *As an entrepreneur, what unique challenges have you encountered in beginning your own consultancy?*

A: As an entrepreneur, one of the biggest challenges I found was marketing the firm. It is quite simple when you work in a larger organization with a structure, a management body and many employees. The biggest challenge I've had has been to start from the ground up; even when you know and have familiarity with clients, there is much work of evangelization. One of my biggest secrets to overcome this has been volunteering and networking through associations such as ISACA® and the Association of Certified Fraud Examiners (ACFE).

Q: *How has volunteering with a leading industry association, such as ISACA, helped and advanced your career and professional life?*

A: Volunteering has raised my professional experience—increasing my knowledge on many subjects beyond auditing, allowing me to exchange ideas with people from other countries, improving my exposure to the public, sharing with and teaching others what I have learned—and it has provided me with ongoing development.

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

A: My biggest workplace challenge was when I was appointed chief information officer at a recognized insurance company in my country. With the appointment, I moved from being an auditor to being the executor. With the support of the management body and the board of the company, I was able to successfully transition. The most important thing I learned from that experience is the importance of working together with other people to meet the goals of the organization—one person cannot do it alone.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

WHAT ARE YOUR THREE GOALS FOR 2015?

1. Advising boards of directors in companies
2. Strengthening the firm's personnel in the use of forensics tools for research
3. Increasing networking with other unions

WHAT'S ON YOUR DESK RIGHT NOW?

- Two audit reports for review
- My computer
- A glass of water

HOW HAS SOCIAL MEDIA IMPACTED YOU PROFESSIONALLY?

Social networks allow for ease of communication. If used wisely, they can be a strong means of communication and a way to spread awareness.

WHAT'S YOUR NUMBER-ONE PIECE OF ADVICE FOR OTHER RISK PROFESSIONALS?

Be sure to check thoroughly before expressing an opinion in writing to avoid misunderstanding.

WHAT'S YOUR FAVORITE BENEFIT OF YOUR ISACA MEMBERSHIP?

Staying up to date on the latest issues facing audit and security professionals

WHAT DO YOU DO WHEN YOU'RE NOT AT WORK?

I like gardening and working on feng shui.

Successful Audits Do Not Just Happen

Ed Gelbstein, Ph.D., has worked in IS/IT in the private and public sectors in various countries for more than 50 years. He did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late 60s and early 70s, and managed projects of increasing size and complexity until the early 1990s. In the 90s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi)retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. He also teaches postgraduate courses on business management of information systems.

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:

An online search for "audit success criteria" reveals few articles or books specific enough to be useful. Several reflected an audit function perspective and did not discuss the views of other stakeholders.

Let us assume here that organizations have a unique environment defined by their corporate culture, their choices of technical and audit standards and guidelines, their governance processes, the criticality of their information systems and data to their business, supply chains, vendors, and so much more. Thus, a one-size-fits-all approach to audit will not automatically lead to success.

PART 1: HOW TO ENSURE YOUR AUDIT IS A FAILURE

First, there are five key ways to waste your organization's time and money:

1. **Poor audit planning**—It should go without saying: Fail to plan sufficiently and you have already planned to fail!
2. **Ignoring changing risk**[1]—This is the easiest way to fail—both internally (e.g., a significant business change) and externally (e.g., a key vendor discontinuing support for a product critical to your organization, an attack with weapons-strength malware)—and, instead, repeat past audits. Thereby, you potentially fail to focus on the most important *current* technology risk factors.
3. **Not thinking in terms of value added**—Avoid the mindless pursuit of perfection (MPP), i.e., pushing the auditee to do things simply because the standards, guidelines and good practices state these are good things to do. Audits that do not focus on risk having significant impact to the organization, its customers or stakeholders will be certain to have missed opportunities, represent poor value and reflect adversely on the internal audit function.
4. **Auditor bias**—We all have biases. The key is to be aware that they exist and appropriately manage them. Two commonly found biases are:
   - Negativity bias, which gives more weight or attention to negative observations and findings than to positive results
   - Overconfidence bias, which is based on the belief that one's knowledge and answers to questions are always correct
5. **Not working *with* the auditees**—It is important not to forget that an audit is not the objective in itself, but a process that has as one of its objectives adding value to the work of IS/IT providers, so that IS/IT operates securely and effectively and supports the organization's business and operations.

PART 2: WHAT DOES SUCCESS LOOK LIKE TO THE VARIOUS STAKEHOLDERS?

To answer this question, let us consider this from the different perspectives.

The Internal Audit Perspective

The internal audit perspective is almost certain to be based on six essential criteria. The audit:

- Adheres to audit standards and quality assurance guidelines[2]
- Is conducted in an impartial manner and supported by evidence
- Addresses critical and high-risk areas pertinent to the individual organization
- Answers the objectives set out in a clearly defined and agreed scope
- Provides timely findings and actionable recommendations
- Is completed on time and on budget

In turn, these six criteria depend on:

- The availability of sufficiently up-to-date and of good-enough-quality business risk assessments and related prioritized and resourced mitigation plans
- The availability of any self-assessments already conducted by the appropriate functions, including metrics to support them
- The availability of competent auditors with a mix of audit skills, experience and soft skills leading to effective interactions with auditees
- The agreement of the auditees to the scope, timing and timescales proposed
- The process for validating the accuracy of the audit findings and the value added by the report

- The process for quantifying the estimated cost of any recommendations and the value added by implementing them

The Audited Party Perspective

Those being audited would be expected to support the previously noted criteria and add the following:

- The audit identifies domains of significant risk not previously recognized by the auditees or their management.
- The audit identifies areas of cost-effective improvements not previously identified by the auditees or their management.
- The audit report gives credit for initiatives and actions identified and initiated by the auditees.
- The schedule for the audit and its related activities does not result in significant disruption to the day-to-day work.
- There is adequate coordination with other oversight bodies' plans to avoid back-to-back audits without a suitable break between them.
- The scope of the audit is maintained throughout the process—no scope creep.
- The entry meeting sets out clear audit objectives, a well defined scope and a method of work.
- The auditors keep the auditees informed of their progress and ensure that their findings are accurate as the audit progresses.

The Audit Committee Perspective

An audit committee can be expected to support all the previously noted criteria and possibly add:

- An audit strategy focusing on information assurance and information security that describes the specific objectives for a multiyear audit plan in which the audit universe is segmented into several areas, ranked by impact and risk
- Inclusion of root-cause analysis (RCA)[3] that supports the recommendations
- Confirmation from management that the audit includes analyses that were not previously available and descriptions of actions and options that had not yet been considered
- A statement of the standards, guidelines, tools and metrics used in conducting the audit
- An inventory or list of risk domains that cannot be audited for contractual or legal reasons (e.g., a cloud service provider or Internet service provider)
- Clear understanding of the status of past audit recommendations, including those that have been implemented and validated as effective by further audit and those that have not been implemented and whether the reasons why are valid and justified

The Management Perspective

Management, from the functional managers of the entities being audited to the executive suite, need to be satisfied that audits meet three criteria:

1. The audits planned and conducted are aligned with the needs of the business/organization.
2. The actions recommended by the auditors represent a good return on expenditure.
3. The results of audits over time lead to a demonstrable reduction in business risk.

CONCLUSION

Everybody wants an audit to be successful. Given that success may mean different things to the parties involved, due attention needs to be given to their criteria.

Future columns will explore the many factors that may conspire to make success harder than it need be.

ENDNOTES

[1] ISACA, IS Audit and Assurance Guideline 2202, Risk Assessment in Planning, September 2014, *www.isaca.org/standards*

[2] ISACA, *ITAF, 3rd Edition*, September 2014

[3] Mind Tools, "Root Cause Analysis: Tracing a Problem to Its Origin," *www.mindtools.com/pages/article/newTMC_80.htm*

Information Technology and Innovation Ethics

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

Entrepreneurship and small business are at the core of economic growth. After all, new giants such as Google and Facebook germinated from humble beginnings, much like the launch of Hewlett-Packard in a garage. While entrepreneurship has always been a key segment of the economy, there has been a huge surge in this sector since the 1990s. For technology start-ups, the biggest innovation boost came from the increasing reliability of access to, and the speed of, the Internet.

Whereas the failure rate of small businesses is alarmingly high, the ambition to "make it happen" has never dissipated. Now there are university degrees, incubators, business-academia collaborations, television and media shows such as *Shark Tank*, crowd-funding, and the community of angel investors—all ready to feed this passion. One of the most powerful influences behind this tidal wave seems to be wealth creation at an unprecedented rate and in a few short years. Names we have had barely a chance to get acquainted with have gone through the roof in share price and market caps in a short period of time. Innovation deserves big applause!

Before we explore the ethics of technology-based innovation, let us recognize that innovation *generally* is an ethical thing to do. As Chris Fabian and Robert Fabricant suggest in their blog, innovation is humanistic.[1] It likely improves the ecosystem, creates more wealth that can be used to do more good, enhances lifestyle and contributes to material happiness. And it could help greatly in reducing pain and discomfort, hunger, sickness and ignorance worldwide. The Gates Foundation is just one example of how doing well leads to doing good. So ethics and innovation are *generally* not on a collision course. While the net impact of some innovations on society is either debatable or not yet known,[2] generally, innovation has infused positive energy in the economy over time.

TECHNOLOGY-BASED INNOVATIONS

We classify technology-based innovations into two categories: technology-enabled and technology-centric. The former involves technology as a lever to make a traditional business model more open source, virtual and efficient. An example is the Lending Club, an online platform that matches borrowers with money from individuals and institutions. Borrowing and lending are two parts of the same transaction, traditionally dominated by financial institutions, now getting a virtual treatment from the Lending Club.

In contrast, more dynamic initiatives of wealth creation involve technology-centric innovation. An example is Instagram. The platform allows you to take a picture or video, choose a filter to transform its look and feel, and post it to Instagram for sharing with friends and family. While sharing is not new, a business model with a new way of sharing in the virtual environment presents tremendous potential for its stakeholders. It is fast, virtual and efficient; it works in a one-to-many relationship. In this realm, we are looking at needs that may not have been previously examined in terms of an entirely new business model. For decades, perhaps centuries, we have lived with photo film and snail-mail to share our memories. Instagram made a technology-centric model feasible by ignoring traditional media and channels of communication. This, in turn, improved the quality of experience with impressive gains in efficiency as well.

Since technology-enabled innovation transforms an existing value creation model, ethical codes of conduct, policies and practices in place may provide a starting point for the new business. The Lending Club, for example, could lean on the history of the mortgage lending sector to begin to determine its dos and do nots. For technology-centric models, the challenges might be significant because they have no history on which to draw. Instagram's innovators, for example, had to create their own code to support their business model. In sum, any innovative use of technology warrants a careful examination of ethical implications. We discuss this in three parts aligned to the developmental stages of innovations: initiation, launch and postlaunch.

INITIATION

At the initiation stage, innovators are focused typically on making their idea come alive; they are almost exclusively consumed by the journey from thought to implementation. At this early stage of innovation, they have little time to think about anything else; no one is going to question them if they do not yet have a written code of ethics. However, innovators should think about ethical implications of the idea as far into the future as they can project. And this should be imparted to others in the small group that the entrepreneur recruits to work on the idea. Such recruitment is likely driven by urgency of delivering the product, process or platform on which the innovation is expected to thrive. However, this should not be enough; after all, the culture and values of the business entity being born hinges upon the entrepreneur and the few people who are first to arrive. This group often establishes an unwritten code of ethics that guides the group during the initiation phase and beyond.

> "Innovators are focused typically on making their idea come alive."

Bitcoin, a form of virtual currency, serves as a context for issues leading to ethical dilemmas at the initiation stage. One can trade bitcoins across national and regional boundaries with one currency and with few transaction costs. It is safe and protects the anonymity of transactions. However, the birth of bitcoin suffers from an inherent limitation of no backing from any currency regulatory agency and, thus, severely limits the amount of trust in the currency, currently treated by many as a commodity. Anonymity defies transparency, which is a necessary attribute for many things fiduciary in nature and, therefore, central to currency management. The secrecy of identity could have side effects; for example, it nurtures an environment of illegal trading, criminal behavior and underground economy. Although laudable, the bitcoin initiative suffers from inherent ethical dilemmas. If these could not be addressed at the initiation stage, the trust in ecosystems built around bitcoin currency will be limited. Some businesses seem to support transactions in bitcoins; however, there is no overwhelming outburst to get on the bandwagon. And most important, leadership of this innovation seems scattered, perhaps not even traceable to one or a few leaders. No wonder, the hiccups in the journey of electronic currency suggest fundamental problems with the idea itself.

Yik-Yak and its peers (e.g., Whisper and Secret) have adopted a business model that supports messaging apps for anonymous posting of content. Yik-Yak, the leader in this push, ranked in the top 10 of all social networking apps in the Apple store in 2014.[3] It is popular among college students and catching up with high school students as well. The problem is that students often post immature content, including bullying threats and trash talking. Anonymity breeds unwarranted heroics, leading only to greater risk to the communities, including schools. To counter abuse of the app, the company uses a geo-fence around physical school campuses to block the use of the app in schools. But students easily circumvent this at the end of the school day when they leave school grounds.

An ethically flawed idea may suffer from correctable deficiencies, but it could also be downright incurable. Entrepreneurs should engage in an early assessment of ethical dilemmas that may surface from any innovation under consideration. The entrepreneurial plate is currently quite full, with issues lurking to be examined in the case of drones, robotics and artificial intelligence, for example. In each opportunity space, doing the right thing is more critical than doing the thing right.

LAUNCH

If there are no fundamental issues of ethical nature inherent in the idea, the next stage of innovation risk surfaces at the launching stage. No matter how impressive the technology, ultimately, the idea meets the human user. This invariably happens at the launching stage where human experience with the innovation is confirmed.[5] Equally important, such experience in the Internet era happens on a large scale. Everything can go just right, or much can fall apart at this stage, not because the idea is inherently flawed, but because it now puts human trust to the test.

Uber, an app-based ride services business, provides an example. Companies, even families or groups, can authorize rides for others (e.g., employees, children) and pay directly, without requiring the employee to seek reimbursement or the child to pay directly. The Uber ride itself may be a matter of pride if Uber could develop a brand name that stands out for a unique experience (e.g., reliability, on-time service, rider safety, well-maintained cars, courteous drivers). Upon launch

in many nations, Uber has run into a crisis of confidence, not because of the technology behind the business model, but rather because of the human interaction with it.

It seems Uber is aware of rider safety issues as a potential risk. The company's web site discusses rider safety and claims that it screens drivers. However, problems suggesting systemic failures ensued as soon as people were introduced to the service on a massive scale. A case of alleged rape by an Uber taxi driver in India has induced the government to ban all app-based taxi services. Thailand has barred all app-based taxi service operators who use personal vehicles. A lawsuit has been filed in California against Uber for allegedly misleading customers with an assertion that they screen drivers.[6] While similar app-based services have appeared on the scene, Uber has gained the most attention on issues of rider safety, something that its technology-enabled model does not address.

In a thought-provoking piece, Christopher Mims equates Uber to a "logical endpoint of the gradual transformation of the tech industry into something new."[7] He asserts that the emphasis of early tech companies was on "being an enabling force, on improving life first and perhaps changing the world in the process." Sure enough, Google strives to live up to such ambitions and so do several other tech companies. Mims suggests that the new tech companies play a zero-sum game. The focus of innovation has shifted from sustaining communities to making owners wealthy.

> "Ethical leadership has an obligation to manage innovation."

Uber's growth seems impressive, but its launch has shown significant vulnerabilities. One wonders what happens when a technology is embedded within communities. As Schneier puts it, the society thrives on trust and when such trust is violated, issues of ethics, security and control, and regulation arise.[8] Without trust, people would not use Uber, or any, services. Ethical leadership has an obligation to manage innovation. For Uber, putting trust back into the business will remain a formidable challenge; how it addresses the dilemma will define its destiny.

POSTLAUNCH

Fabian and Fabricant discuss UNICEF's Innovation Labs, which provide a good example of a value-based approach to problem solving that effectively bridges technology and development.[9] One idea is to create a translation layer between start-up thinking (Would people use my product?) and development thinking (Will the change become institutionalized over time?). Ensuring widespread adoption of the innovation is the key to impactful and lasting innovation. Without it, the world gets left out of the benefits of innovation.

Over time, some innovations successfully cross the bridge from start-up thinking to development thinking. Such innovative businesses become major players in world economies. By one estimate, five US tech firms—Apple, Amazon.com, Facebook, Google and Microsoft—are valued at a combined US $1.8 trillion, compared to a combined US $1.3 trillion for all 30 blue-chip companies in the German DAX index. For one thing, each is relatively new on the economic scene and each has successfully navigated the initiation and launch phases, managing effectively any and all challenges along the way. For example, on the privacy front, Facebook faces a similar challenge to Uber, but it has managed to nurture the trust of its users well, barring occasional mishaps. And even at the advanced stage of proving its worth, Google still has to respond to challenges of privacy; the battle continues, but there is more trust and greater willingness of people to use Google services.

In the postlaunch period, the role of IT innovation firms changes from that of an adversary to an ally. With the amount of influence they wield on the private and work life of individuals, it is clear that in some respect they are more powerful than even the national governments of some countries. More important, their influence cuts across national boundaries and varied cultures across the globe. For these established companies with abundant influence and resources, the accountability shifts toward shaping the policies and practices, regulations, and conventions that make the world a better place.

CONCLUSION

Technology inherently is neither good nor bad; what matters is how it is introduced to a purpose. While its downside should be contained to mitigate risk, its upside potential must be explored fully. And all this requires that trust is kept in balance so as not to cause anticipated benefits to prematurely vanish. The world has gained a great deal from information technology, and it appears, on balance, the associated risk is worth taking. And yet, one should expect bumpy rides in the future, while the greater good is achieved.

> "Technology inherently is neither good nor bad; what matters is how it is introduced to a purpose."

ENDNOTES

[1] Fabian, Chris; Robert Fabricant; "The Ethics of Innovation," Stanford Social Innovation Review, 5 August 2014, *http://www.ssireview.org/blog/entry/the_ethics_of_innovation*

[2] An example is the mapping of the human genome. It is unclear what negative side effects this project would produce.

[3] Rusli, Evelyn M.; Jeff Elder; "Behind the App's Rise, Dark Side Looms," *The Wall Street Journal*, 26 November 2014, p. B1-B4

[4] Marcus, Gary; "Artificial Intelligence Isn't a Threat—Yet," *The Wall Street Journal*, 13-14 December 2014, p. C3

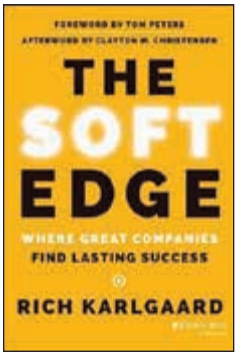
[5] Innovators are typically seeking feedback from prospective customers at an early stage. However, this may not always be culturally holistic or globally complete.

[6] Sugden J.; A. Malhotva; D. Macmillan; "Uber Under Attack Around Globe," *The Wall Street Journal*, 9 December 2014, p. B1

[7] Mims, Christopher; "Uber and a Fraught New Era for Tech," *The Wall Street Journal*, 25 November 2014, p. B1-B5

[8] Schneier, Bruce; *Liars and Outliers*, Wiley, 2012

[9] *Op. cit*., Fabian and Fabricant, p. 4



By Rich Karlgaard

Reviewed by Dino Ippoliti, CISA, CISM, an expert consultant at inspearit. He has been a practitioner in information and computer security, IT system auditing, and software and system engineering process improvement for more than 17 years in multiple industries. He is a member of the ISACA Publications Subcommittee and a mentor in ISACA's Pilot Mentoring Program.

The Soft Edge: Where Great Companies Find Lasting Success

How many times has it been asked if an initiative (e.g., a start-up, a new project, an audit, a security assessment) will be successful or, more generally, whether it would be possible to predict the future performance of a company?

According to the author of *The Soft Edge: Where Great Companies Find Lasting Success*, to be successful, an enterprise needs not only to be good at the strategic basis (understanding their market, customers and competitors) and the hard edge (the execution of the strategy), but also needs to be good at the human factor, the so-called soft edge. These are the three sides of the health triangle of an enterprise, which the author suggests could help predict the long-term success of a company, just as in biology the health triangle—composed of physical, social and mental/emotional sides—is used to predict the survival chances of an organism.

The Soft Edge will not give the reader advice on how to cope with the new security risk posed by virtualization technologies or the growing use of bring your own device (BYOD), nor will it provide an auditor with any insight on how to leverage big data analytical techniques to perform financial audits. Rather, this book will help readers understand why the soft side is so vitally important and how anyone, not just the gifted few, can leverage it to reach higher peaks of performance and better results. Moreover, even individuals can make use of the soft edge to improve their working performance.

The soft edge is composed of five pillars and each of them is analyzed in a dedicated chapter that guides readers to answer crucial questions including:

- How does trust affect productivity and innovation? How can trust be built within a team and with external stakeholders, including customers?
- What does it mean to be smart in business today? Does it mean hiring the best graduates or the best experts, or does it have to do with hard work, perseverance and lateral thinking?
- The importance of teamwork is universally recognized, but what are the most important ingredients to build a high-performance team? What is the ideal number of team members and what kind of diversity should be sought?
- What makes a product or a service appealing when compared to others available on the market? To achieve a successful product, an aesthetic and emotional engagement needs to be included.
- To advertise a product, should only its functionalities be focused on or would it be necessary to narrate a story that might trigger the emotional side of the listeners, be it a customer or an employee? How can stories be created and told that contribute to the success of a brand?

Throughout the book, readers begin to understand soft-edge factors and their impact on enterprises' health and long-lasting success by reading real-life stories, well-formed arguments and references to external resources. Moreover, these stories come from different kinds of businesses (e.g., medical, technological, sports, logistics). The contribution of the new technology, such as data analytics, to build the soft edge is not neglected, and appropriate examples are provided.

Although the use of real enterprises' success stories might be perceived by some as promotional for the companies mentioned, this book offers important information for managers and enterprise owners, as well as any kind of professional, including IT auditors and security experts. Indeed, business success cannot be achieved without taking into account the human factor, without which businesses are hampered in delivering good results as a team and, most important, in making those results accepted by stakeholders so as to really make a difference.

It is important to consider that to successfully harden IT systems, it might be necessary to fully understand the importance of the soft edge in the business.

EDITOR'S NOTE

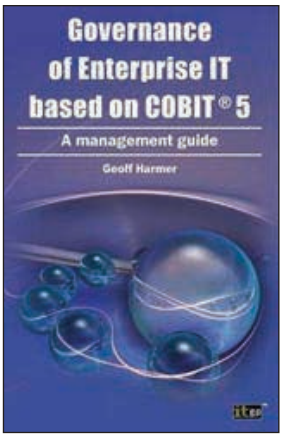
The Soft Edge is available from the ISACA® Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore,* email *bookstore@isaca.org* or telephone +1.847.660.5650.

Governance of Enterprise IT Based on COBIT 5: A Management Guide

Reviewed by Maria Patricia Prandini, CISA, CRISC, who has a long career as a public official in different positions related to information technology in the Argentine Government. Prandini was involved in the development of the National PKI and the foundation of ARCERT, the first governmental computer security incident response team (CSIRT) in Argentina. She is the immediate past president of the ISACA Buenos Aires (Argentina) Chapter.

When governance and management of enterprise IT (GEIT) is needed, COBIT® 5 is frequently the framework of choice for organizations all over the world. With an increased focus on business, COBIT 5 offers a major strategic change in how the framework is structured and organized.

However, the depth, innovation and extent of COBIT 5 could be somewhat overwhelming for anyone who has never come in contact with previous editions of the framework. With his book, *Governance of Enterprise IT Based on COBIT® 5: A Management Guide*, Geoff Harmer's goal is to fill this gap. And for those who are acquainted with previous versions of COBIT, this book also provides assistance to quickly gain access to the new concepts and characteristics of COBIT 5.



By Geoff Harmer

In fact, as the author states, the book is a guide to GEIT and, specifically, how it may be implemented using COBIT 5. Consequently, key concepts of COBIT 5, such as IT governance and management, the goals cascade, the five principles, and the seven enablers, are presented in an easy-to-understand way. The publication also includes several tables and figures that clarify the contents and main concepts of COBIT 5.

With text organized into nine chapters, the author successfully introduces the framework's key elements, the structure of the 37 processes, the implementation of GEIT using COBIT 5 and the COBIT Process Assessment Model (PAM). The first two chapters present the concept of IT governance and the main international frameworks and standards supporting it.

The next four chapters provide an overview of COBIT 5, its enablers and principles, and how domains and processes are organized. The following chapters describe the central aspects of the framework implementation and the PAM. The last chapter explains how COBIT 5 documentation is organized and the official COBIT 5 training courses and certifications available.

Professionals working in IT management, governance, assurance, security, risk and control roles could take advantage of this book as a shortcut to understanding COBIT, as this book helps readers gain quick access to COBIT 5's basic concepts.

This book provides a head start for anyone interested in using the framework. Readers working in a small enterprise or a large multinational corporation will increase their COBIT 5-related knowledge base and skill set. For newcomers to the framework who do not know where to start or those needing a quick overview of COBIT 5, this book offers a simple and clear way to learn about the characteristics of this unique framework.

EDITOR'S NOTE

Governance of Enterprise IT Based on COBIT® 5: A Management Guide is available from the ISACA® Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

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:

Internet of Things Offers Great Opportunities and Much Risk

Marcelo Hector Gonzalez, CISA, CRISC, supervises IT environment and internal control in banks operating in Argentina. He is also responsible for auditing cross-border data processing outside of Argentina for international financial entities. He is a member of the Commission of e-Banking in the Central Bank of the Republic of Argentina, which has published several booklets on e-banking best practices. Gonzalez can be reached at *marcelohgonzalez@gmail.com.*

Jana Djurica works at the National bank of Serbia as an IT supervisor of the Serbian financial sector. She is an IT expert with experience in auditing IT areas such as IT governance, risk assessment, internal IT audit, IT security, business continuity management, disaster recovery planning, IS development and IT outsourcing. She can be reached at *janadjurica@yahoo.com.*

Turkçesi de bulunmaktadır
www.isaca.org/currentissue

There are a number of definitions of Internet of Things (IoT), with all of them having slightly different meanings. Some define IoT as the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure; others say that IoT represents appliances connected to the Internet, and there are many more definitions. The definition that, for now, seems to make the most sense is: "IoT is a scenario in which objects, animals or people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT is a world where virtually everything is imbued with one or more tiny computers or smart sensors, all transmitting a flow of data onto the Internet."[1] Wikipedia.com defines IoT as the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure;[2] and Webopedia.com describes IoT as the ever-growing network of physical objects that feature an IP address for Internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.[3]

Keeping in mind the variety of definitions and the many differences between them, it can be concluded that IoT remains in its initial phase of evolution. Soon, cars, homes, major appliances and other basic objects from everyday life, even city streets, will have the capacity and the need to be connected to the Internet, creating a network of objects that will be able to control everything. This network will be made of millions of devices with sensors that can generate or capture constant streams of data. The potential appears endless.

THE POSSIBILITIES WITH IOT

IoT consists of three principal components:

- **The things themselves** that, in most cases, represent the devices or sensors with the ability to capture or produce data, and the time to create an effect on the environment in which they have some influence
- **The communications network** that interconnects the things (this network connectivity, in most cases, is wireless)
- **The computing systems** that process and use the data received and/or transmitted by the things, with, in most cases, a minimal computational capability

By using this infrastructure, things can communicate with each other and even optimize activities among each other based on the analysis of data streaming through the network.

These data can be personal data (which, if compromised, carries significant legal implications with regard to privacy) or environmental data, such as measurement of temperature, barometric pressure and wind activity, for example.

Imagine that someone is about to leave home to go to work or for a walk. The sky is somewhat cloudy and the person wonders, "Will it rain?" There is not enough time to go back inside and wait for the weather forecast on television or to turn on a computer to see the weather forecast. However, next to the front door is the umbrella stand and the handle of the umbrella has a red light, a warning that there is a chance of rain, so the person decides to bring the umbrella as a prevention when he/she leaves the house.

The purpose of IoT is for regular elements to perform the functions for which they were designed but at a higher intelligence rate, adding to their aggregate value. This is shown with the umbrella example where a simple device is connected to the Internet to obtain some useful data that will provide it with the ability to fulfill the same original function of protecting against the rain, but at an improved level because of additional valuable information. David Rose,

author and instructor at the Massachusetts Institute of Technology (Boston, USA) Media Lab, has the following vision: "IoT is technology that atomizes, combining itself with the objects that make up the very fabric of daily living."[4]

Examples of IoT are slowly becoming reality. A US company, Ambient Devices, already develops these kinds of devices, including an umbrella that connects to AccuWeather[5] and alerts the user of the need for an umbrella.

The imagination could take this much further. Imagine a water sprinkler that uses Internet forecasts, weather sensors and usage information to optimize water expenses and improve ecological behavior. What about a public trash can that can compact all the trash inside it and alert the city trash gatherers when it is full?

Home security systems already allow homeowners to remotely control door locks, lights and thermostats (**figure 1**), but what if they took proactive measures such as cooling the home and opening windows or turning lights on based on owner preferences, weather conditions, owner proximity to home or cost expectations?

Figure 1—Internet of Things All Around the Home

Source: Gonzalez and Djurica. Reprinted with permission.

POTENTIAL RISK

We are living in a continuously increasing smart world where not only personal computers, tablets and smartphones are connected to the Internet, but also an incredible amount of different devices—everything from pill bottles and umbrellas to refrigerators, watches and cars—are coming online. The only limitation seems to be the imagination.

This technological trend is remapping how the world and individuals interconnect with each other and everything else. This implies a higher immediate security risk for people, homes and enterprises than the risk caused by current consumer technologies.

The increasing trend of making buildings more energy efficient, green friendly, secure and responsive to changing environmental conditions is resulting in diverse Internet-enabled technologies. These building or home management systems are not only becoming increasingly more integrated with each other, they are also integrating into systems outside the perimeter of each edifice, creating a smart grid.

Many of the Internet-enabled intelligent devices embedded in modern homes and organizations have little security built into them, making them vulnerable to attacks that could disrupt normal use or operations and create safety concerns. This is a critical problem that must be resolved.

As the number of lamps, thermostats and sensors that can connect to mobile phones increases, so does the number of malicious hackers who will want to try to disrupt these devices, or make money by wreaking havoc. Weakly protected building management systems connected to the Internet could also provide a way for malicious attackers to break into systems connected to the same network, but outside the originally targeted one.

> "Security systems must develop in the same way and at the same pace as do all these new intelligent systems being created with the things around us."

Someone could take control of a home, a whole building or a town. Security systems must develop in the same way and at the same pace as do all these new intelligent systems being created with the things around us.

The threat is not only that someone could penetrate a home or a building system to cause serious disruptions. There is also a potential impact on technology infrastructure that could result in a loss of communications due to a system outage or unauthorized access to data because of poor segmentation between the automation network and the infrastructure security network.

> Establishing trust in a broad range of things across dispersed settings and on a massive scale is a challenge for information security experts.

Traditionally, home and building management systems have not been considered IT systems; they are not overseen by an information officer and have long been considered operational technology under the management of facilities designers. This will have to change with the emerging use of IoT in homes, buildings and cities. Facilities designers, administrators and IT experts will need to work together to identify and mitigate potential security risk. "The IoT offers a very appealing vision of harnessing technology today to lead to a better tomorrow. But focusing too much on the data and not enough on the beliefs and behaviors of the people attached to the 'things' can create major privacy and security risks."[6]

Several barriers exist that prevent mass prevalence of IoT as a part of smart buildings, at home or in an enterprise. Those are:

- Smart technology in IoT is still not cheap and becomes even more expensive if the technology is designed with strong security measures. In fact, the security of these systems is currently at a fairly low level.
- Smart technologies in IoT are not totally interoperable and at the moment do not exist in a unique architecture.

However, it is just a matter of time before these obstacles are overcome. Thus, information security and control experts need to begin adjusting to these possibilities now.

PRIVACY ISSUES RELATED TO INTERNET OF THINGS

The things in IoT, such as cars, toys and home appliances, can be used for unlawful surveillance. These Internet-connected things could allow attackers to obtain far more information than they could previously. For example, attackers may be able to monitor children through cameras installed in toys, monitor people's movements through Internet modules installed in a smart television, or monitor when a person enters or leaves his/her home by connecting to an Internet-connected door lock. Such threats are not merely speculative. Many of those present real vulnerabilities in Internet-connected modules installed in cars, medical devices, airplanes engines and children's toys, because not all of those devices were designed with privacy or security in mind.

Those Internet-connected modules could allow attackers not only to passively monitor their victims, but also to actively intrude into their private lives. This is because many of those things can be remotely controlled so an attacker can divert the signal in order to remotely stop the refrigerator, start the heater or unlock the door.

Another important issue is that IoT enables the creation, storage and sharing of enormous amounts of data about a person's habits, behaviors and preferences. As a result, regulatory bodies, including the US Federal Trade Commission and the European Commission, are turning attention toward the potential privacy and security issues that the IoT presents in citizens' everyday lives.

Needless to say, establishing trust in a broad range of things across dispersed settings and on a massive scale is a challenge for information security experts. The devices themselves are vulnerable to physical attacks, the networks over which they communicate are not always secured and the back-end systems and data repositories are attractive targets for thieves and terrorists. Opportunists, hacktivists, malicious insiders and even unscrupulous governments are all potential attackers with the ability to intercept critical data in transit or seize control of these devices.

With more and more things connected to the Internet, the potential privacy implications, the general false sense of security associated with design and the possibility of data compromise grow more critical. Thus, IoT needs to rely on two things: trust and control. These two concepts present an opportunity and a challenge at the same time for information security experts and IT auditors.

> It is an Internet-scale problem that will require an Internet-scale solution.

This leads to the same questions e-commerce posed 15 years ago when Amazon was interacting with millions of customers. The difference now with IoT is that, for example, a utility company can interact with millions of smart meters or

a transit center can interface with thousands of cars. Mutual authentication, secure communications and high-integrity messaging, all at an Internet scale, will become core security foundations for these systems, so it is an Internet-scale problem that will require an Internet-scale solution.

This is much more serious than a privacy issue; it is about rights to modify things that can then profoundly impact the security, health, environment, finances, relations and more of millions of individuals (**figure 2**).

If IoT use increases, as experts expect, millions and millions of devices will come online and managing security around a very large network of different kinds of devices will be a crucial, urgent and complex issue.

If a large, branded supplier of IoT devices implements a complete home or business IoT solution and an intruder manages to attack and steal personal health or financial data or physical belongings, it will be a disaster not just for the individual, but also for IoT device suppliers around the world. For example in the worst-case scenario, if an attacker modifies the parameters of when a medicine dispenser has to alert a pharmacy to refill it, this becomes a potential matter of life and death.

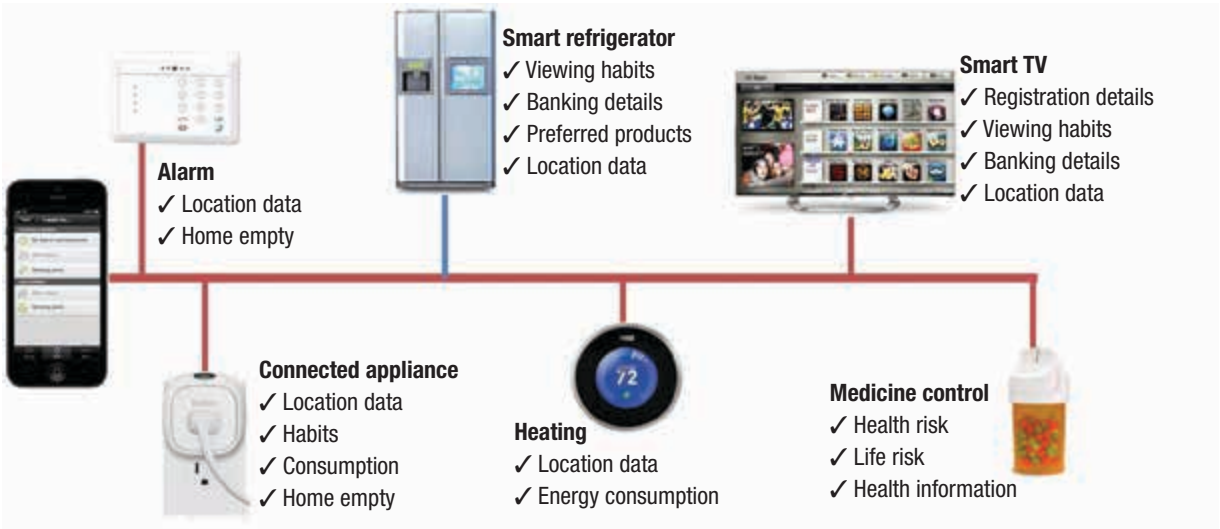
Attacks can also multiply in scale as one attack goes viral. For example, if a burglar hacks a door system in a home while the homeowner is out, this can escalate to a viral situation in minutes across a large territory in which the same door lock provider has installed similar systems.

SECURITY FOR IOT

Most of the devices in IoT are always connected and, thus, always vulnerable. Issues around Internet security and mobile devices' interrelations already present a challenge in this era of constant connectivity. In the scenario of a home or business owning numerous connected devices, those challenges will be even greater.

An ineffective or nonexistent plan for deploying security updates will be the single largest impediment for IoT. The reality is that vulnerabilities appear in all code from time to time, so a solid security life cycle that considers security throughout design and development will have notably fewer security issues. However, all software manufacturers must be ready to quickly respond to vulnerabilities and release patches to protect their users.

Figure 2—Personal Data at Risk



Source: Gonzalez and Djurica. Reprinted with permission.

As all these scenarios show, securing connected devices should be a major component of IoT, but security is not at the top of the to-do list for the companies that are manufacturing connected devices. Many of the engineers who develop the devices have more experience in design and the interconnection of devices, which may result in security not being considered in depth or worse: being totally overlooked.

Another cause for the lack of security in connected devices may be cost. To make these devices secure, manufacturers need to take extra steps, such as developing security models, creating patches to maintain secure devices and doing penetration testing for vulnerabilities. Because of these, some companies might opt out of security altogether. And further complicating matters is the fact that many of these devices use embedded software and cannot easily be patched.

To accelerate IoT development, some companies are developing technologies to address the security, interconnection and interoperability challenges and enable solutions. For example, Intel offers several versions of development kits with a combination of performance and software capabilities—the reason being that there are different types of developers, ranging from hobbyists and enthusiasts to professionals.

Unfortunately, every new technological development comes with a new set of security threats.

FACTORS TO CONTROL IN THE INTERNET OF THINGS.

Attention must be paid in order to achieve control and minimize the potential IoT risk and to:

- **Minimize collection of personal data.** Sensors such as smart meters are aimed at encouraging end users to shift electricity usage to off-peak hours or to control water usage with the goal of helping the planet and lowering costs. Those sensors are designed to collect consumption data in order to determine the usage of electricity, water or other utilities and set prices accordingly. These data are collected at the individual level, so one measure could be to control which data can be exposed to the Internet without an individual's consent.
- **Minimize connecting data with individuals.** It is important to assess whether devices or software need personal information or some other data that could be connected with individuals or their private information. For example, is it necessary to use Internet service provider (ISP) data or can static Internet Protocol (IP) data be provided? The optimal method is to collect data without connecting it to individuals. It is always preferable to aggregate data on a higher level rather than using data that could be connected to an individual person.
- **Minimize and secure data retention.** Sometimes, depending on the sensor or device brand or configuration, data are not only sent, but also stored inside the device or in several devices around the Internet, in the communication or with the utility provider. Therefore, one best practice is to make certain that data sent through the network are encrypted to prevent personal information leakage in transit. Also, if there is a connection with a utility provider, no additional data (apart from data that were agreed upon at the assumption of the service delivery contract) should be transmitted.

Additionally, traditional controls should not be forgotten:

- If something is connected to a home or business network, it can be accessed over the Internet and, thus, ensure that it is secured in relation to that which it is exposed.
- Review the security settings on any device installed. If it is remotely accessible, disable this feature if it is not needed. Change any default passwords to something difficult to guess. Do not use common or easily guessable passwords.
- Depending on the complexity of the IoT installation in a home or a business and the level of existing exposure, install a firewall to protect all of the resources inside it.
- Regularly check the manufacturer's web site to see if there are updates or patches to a device's software.

It is important to keep in mind that the requirements for connecting a car information system sensor are quite different than the security requirements for a home, business, corporation, or public safety or government entity. All of these unique requirements add complexity to the implementation and control of IoT security. There is no simple solution that would secure such a diverse collection of devices, and there is no single, effective security strategy because different devices from different manufacturers have different security risk profiles. Meanwhile, until a consolidated security solution is in place, IoT security's focus would be most effective if on the data, rather than on the devices. As such, when data are stored, in process or in transit, protections enable individuals and enterprises to provide security and privacy simultaneously.

> "There is no simple solution that would secure such a diverse collection of devices."

THE HUMAN PERSPECTIVE RELATED TO IOT

The Jetsons[7] was set in the sky-high Orbit City and the show featured a family living an average life in the future with flying space cars, instant transport tubes, robots and lots of technological gadgets that enabled them to get work done in a matter of seconds.[8]

In a not-too-distant future, the reality will be even more sensors, gadgets, micro devices, and perhaps robots that will do a lot of things that people used to do, a lot of things that people are not able to do and a lot of things that people do not like to do.

The future holds many uncertainties with regard to how IoT will affect people. Perhaps many people will have to learn different skills at home and at work, as some basic jobs will be replaced by devices that work together in collaboration with the Internet.

The Google Self-driving Car is an example. Imagine a world full of cars with no human drivers where people enjoy the car journey doing things such as resting, reading or playing. It sounds amazing and in many ways unimaginable, but to get there, many changes will have to take place beyond the simple creation of the technology. For example, such IoT technology may provide malicious hackers an opportunity to implant a virus in the network of traffic sensors and traffic controls, changing information about where traffic jams are located or where there are demonstrators.

> "IoT challenges should be met proactively with sound planning, good security strategies and frequent IoT audit assessments."

The industry must get prepared for profound changes to current cybersecurity strategies and operations as IoT introduces an avalanche of new devices, network traffic and protocols, physical and physiological risk, applications that demand data security improvements, and wider and deeper malware attack surfaces. IoT challenges should be met proactively with sound planning, good security strategies and frequent IoT audit assessments.

ENDNOTES

[1] TechTarget, WhatIs.com, "Internet of Things," *http://whatis.techtarget.com/definition/Internet-of-Things*

[2] Wikipedia, "Internet of Things," *http://en.wikipedia.org/wiki/Internet_of_Things*

[3] Stroud, Forrest; "Internet of Things," *Webopedia*, *www.webopedia.com/TERM/I/internet_of_things.html*

[4] Rose, D.; *Enchanted Objects*, Scribner, USA, July 2014

[5] AccuWeather is an American media company that provides for-profit weather forecasting services worldwide.

[6] Stroud, Robert; "The Convenience/Privacy Trade-off on the Internet of Things," *Wired* Innovation Insights Blog, 17 December 2013, *http://insights.wired.com/profiles/blogs/the-convenience-privacy-trade-off-on-the-internet-of-things?xg_source=activity#axzz3MNq2UmCe*

[7] Hanna-Barbera, *The Jetsons*, an animated US television series (sitcom) that aired from 1962-1963.

[8] Tucker, Jeffrey A.; "The Attempted Militarization of the Jetsons," Mises Daily, Mises Institute, 21 September 2005

Feature

Strategic Alignment and E-health Governance

Elena Beratarbide, Ph.D., CISA, is the e-health quality and governance manager and e-health researcher at the National Health Services (Scotland, UK). She is a former IT consultant and security auditor for Touché & Ross (Deloitte), KPMG and Fujitsu.

Thomas W. Kelsey, Ph.D., is senior lecturer in the School of Computer Science at the University of St. Andrews (Scotland). He is a renowned investigator and member of a number of research bodies, as well as a nonmedical fellow of the Royal Society of Medicine.

Hermenegildo Gil, Ph.D., is a full professor in the Business Management Department (DOE) at the Polytechnic University of Valencia (Spain) and the Ph.D. director for the Integration of Information Technologies Within Organisations Programme.

E-health is important because health is one of the most important things for every human being, current health care models are not sustainable, and, hence, there is a need to find more efficient ways to achieve better health across the entire population for years to come.

From the health care service perspective, e-health plays an essential role. It is perceived as crucial for high-quality and cost-effective health care. It is faster, provides more and better information (when and where it is needed), reaches remote areas of the population and is secure. In short, e-health promises to be a great solution to the current sustainability issue.

Conversely, getting the expected benefits from e-health has been difficult to demonstrate. This is the point where e-health governance can help in achieving expectations.

There has been rising interest in adopting e-health governance frameworks to obtain reassurance that investments return the expected results in health care. However, how e-health governance is implemented within health care is poorly understood; equally misunderstood is the actual impact e-health governance has on linking health care structures and resources with local and national health care strategies—in other words, in achieving strategic alignment.

This article introduces a recent comprehensive technical report on e-health governance. The report explores the application of well-known frameworks (e.g., COBIT® and ITIL) within the National Health Services (NHS) in Scotland and their impact on e-health governance maturity and strategic alignment with health care. The report mainly presents results of a longitudinal study conducted since 2008 within Scottish health care organisations, but also offers cross-national and cross-sectoral benchmarking.

As a result, it offers an adapted and simplified instrument to swiftly measure e-health governance and strategic alignment maturity levels.

The conclusions of the study suggest that there is a potential strong statistical correlation between e-health governance and strategic alignment; however, more data are required to confirm the initial findings. Thus, it is recommended that the longitudinal analyses continue over the coming years to determine the actual correlation ratio. Further research is also required to understand the influence the rest of the strategic alignment model (SAM) dimensions have and to determine how e-health governance influences strategic alignment in isolation of the rest of the SAM dimensions. For this purpose, a simplified and adapted method to monitor these trends in future health care organisations (HCOs) is also provided.

WHAT IS BUSINESS-TO-E-HEALTH STRATEGIC ALIGNMENT?

Business-to-e-health strategic alignment follows the model proposed by Henderson and Venkatraman.[1] This model has been extensively used in business management, including Luftman's experiences within Fortune 500 companies.[2]

Business-to-e-health strategic alignment refers to applying IT within health care in harmony with the HCO's strategies, goals and needs. Achieving alignment maturity involves IT and HCO strategies evolving jointly, in an integrated way and in harmony.

WHAT IS E-HEALTH GOVERNANCE?

There is not unanimous consensus on what e-health is, nor what governance entails; however, for the purpose of this article, e-health governance is defined as the act of governing e-health, which involves decision making as well as e-health management.[3] Beyond this concept, governance is also the art of assurance, which becomes relevant because of the need for greater results accountability in the best interest of all health care stakeholders.

The World Health Organization (WHO) defines e-health in terms of the efficiency of using information and communication technologies (ICT) in health care,[4] whilst the European Commission (EC) defines e-health more broadly as "the use of modern information and communication technologies to meet needs

of citizens, patients, healthcare professionals, health care providers, as well as policy makers."[5]

In a survey, 93 random individuals in a hospital were asked about how they identify themselves with five e-health vision statements.[6] Sixty-one percent identified e-health with empowering patients and health care professionals to link devices and technologies towards the personalised medicine of the future—integrating smarter, safer and patient-centred e-health services into the patient's life.

Nineteen percent thought of e-health as helping people realise their best possible health through digital technologies.

Ten percent suggested e-health will, through the active engagement of patients and health and social care professionals, provide innovative technology at the point of demand. With enthusiasm, e-health will support and deliver accessible solutions that will facilitate secure access to relevant and accurate information in order to provide the best quality of care and improved health.

Another 10 percent suggested e-health is a way for establishing innovative health care in the region (in this case, Scotland) for the 21st century.

E-health has different connotations, but for the purpose of this article, it is defined as presented by eHealth Industries Innovation Centre (eHI2) Swansea University (Wales, United Kingdom), because of the express mention to the association between e-health and people living in digital societies: E-health is a different way of pursuing healthy lives. E-health implies people living in digital societies using information and communication technologies in favour of better health: health care professionals, patients and care givers, as well as citizens involved in their own or their family's health care.[7]

THE VALUE OF E-HEALTH GOVERNANCE

Is it worth spending time, resources and efforts on e-health governance? For some, common sense suggests a clear yes as a response; for others, it is not as clear because implementing e-health governance good practices, frameworks and standards requires time, resources and huge transformational efforts in most HCOs.

The results of the study (available in the ISACA® Knowledge Center at *www.isaca.org/monitoring-progress-on-ehealth*) support conclusions on how immature organisations are in this matter.

As stated earlier, e-health is important as it is a potential solution for the sustainability of future health care systems. There is an expectation in digital societies that ICT will contribute to better health care. It is expected that e-health innovations contribute to providing quality and cost-effective solutions for 21st century health care challenges,[8] especially considering aging populations, increasing long-term conditions, obesity and alcohol-related issues, along with the costs of preventable hospital admissions if prescription medications were taken correctly.[9] Furthermore, e-health is considered key to achieving sustainable health care, especially in collaborative cross-border spaces.[10]

Despite e-health being considered key for sustainable health care, many e-health initiatives have failed,[11, 12] and HCOs commonly find themselves caught between the organisational pressures for delivering e-health and organisational resistance to new ways of functioning.[13]

Success with implementing e-health initiatives varies significantly according to experiences, as reported to the NHS.[14, 15] Some of the downsides are related to delays, over expenditures or budget deficits, poor quality of outcomes, and effectiveness on health care,[16] which are consistent with the average ICT project's implementation statistics.[17]

After a series of disappointing e-health implementations, there is rising interest in e-health/IT governance[18] as a vehicle to provide assurance to all stakeholders to whom e-health programmes deliver the expected benefits.[19] This interest also derives from the appearance of greater pressures in HCOs for compliance with best practices, standards and regulations.[20]

It is expected that interest will continue rising in the coming years since investments on e-health continue to grow at an average rate of 12-16 percent per year and a global e-health market worth an estimated US $23 billion is expected by 2017.[21] Despite this, and the expectations of successful e-health implementations at strategic levels in health care organisations, e-health governance is still very much just a chief information officer (CIO)/IT director issue.[22] This is a widely reported international occurrence.[23]

Governance is, in essence, the act of governing, which involves decision making, as well as management.[24] Beyond this concept, governance is also the art of assurance, which becomes relevant because of the need for greater results accountability in the best interest of all health care stakeholders.

Although there is a considerable amount of research work on implementation of e-health initiatives and e-health governance, this is still described as a 'young science',[25] demanding more understanding of implementation processes, tools and models for better results.[26] There are a number of IT governance frameworks used across sectors and industries, commonly COBIT, ITIL and a range of ISO standards (e.g., ISO9000, ISO17799 and ISO 38500)—the first two being the most commonly adopted within the health care sector.[27]

USING FRAMEWORKS FOR E-HEALTH GOVERNANCE

The research discussed here is a continuation of a previous study conducted between 2005 and 2010, which involved:

- A comprehensive literature review[28]
- A Delphi exercise[29] proposing a causal model of determining factors involved in the adaptation of NHS to the digital society with a particular focus on Scotland

This model identified a number of factors to be understood in order to help organisations and governments make better e-health investment decisions and strategies (**figure 1**). This article and the related technical report *(www.isaca.org/monitoring-progress-on-ehealth)* focus on two of the main factors identified in the causal model: e-health governance and e-health strategic alignment.

The study started in 2008 as part of an IT governance project cosponsored by the Scottish Executive to demonstrate practical results in adopting IT governance best practices and to provide recommendations for a future adoption across the NHS in Scotland.[30] Three representative NHS boards in Scotland were selected for this trial.[31]

The technical report is based on a longitudinal study (2008-2013), involving a multicase analysis of three representative health care organisations in Scotland. A combination of empiric methods has been used: semi-structured interviews with implementers, surveys using an adaptation to health care of Luftman's instrument[32] for assessing Venkatraman's SAM[33] and cross-sectoral/national benchmarking based on a literature review.

Ninety-two participants were involved across the three HCOs under the study, with representation of the main groups of e-health, clinical and nonclinical stakeholders. The benchmarking exercise incorporated 9,226 institutions providing worldwide coverage.

RESULTS AND CONCLUSIONS

The results[34] show that e-health governance is in its infancy across sectors and countries. Eighty percent of organisations worldwide are in a transition point between a "committed" and an "established" process.

The results support the proposition that the more mature e-health governance is, the better the strategic alignment between e-health and HCOs. The strategic alignment is slowly maturing across the organisation (15 percent since 2008), progressing vaguely faster than e-health governance.

The conclusions of this study suggest there is a potentially strong statistical correlation between e-health governance and strategic alignment; however, more data are required to confirm this initial finding. It is recommended that the longitudinal analysis continues over the forthcoming years to validate the actual correlation ratio. Further research is also required in order to understand the influence the rest of the SAM dimensions have and to determine how e-health governance influences strategic alignment in isolation of the rest of the SAM dimensions. For this purpose, a simplified and adapted method to monitor these trends in future HCO research has also been provided.

Figure 1—Study Proposition

Source: Beratarbide, Kelsey and Gil. Reprinted with permission.

ENDNOTES

[1] Henderson J.; N. Venkatraman; 'Strategic Alignment: Leveraging Information Technology for Transforming Organizations', *IBM Systems Journal*, vol. 32, iss. 1, 1993, p. 4-16, *http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5387398*

[2] Luftman, J.; 'Assessing Business-ITAlignment Maturity', *Communications of the Association for Information Systems*, vol. 4, 2000, article 14, *http://aisel.aisnet.org/cais/vol4/iss1/14/*

[3] World Bank, *Managing Development: The Governance Dimension*, 1991, p. 1-76, *www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/03/07/000090341_20060307104630/Rendered/PDF/34899.pdf*

[4] World Health Organization, 'ehealth', *www.who.int/topics/ehealth/en/*

[5] eEurope 2005/e-health, *http://europa.eu.int/information society/eeurope/2005/all about/ehealth/index en.htm#Setting%20the%20Targets*

[6] NHS Fife, 'What Is e-Health? Survey', Scotland, 2013

[7] eHealth Industries Innovation Centre, Swansea University, *www.ehi2.swan.ac.uk/en/what-is-ehealth.htm*

[8] Murray E.; J. Burns; C. May; T. Finch; C. O'Donnell; P. Wallace; F. Mair; 'Why Is It Difficult to Implement eHealth Initiatives? A Qualitative Study', *Implementation Science*, 2011, vol. 6, p. 1-6.

[9] Gov.uk, '£4 Million for Technological Solutions to Tackle Healthcare Problems', 28 March 2012, *https://www.gov.uk/government/news/4-million-for-technological-solutions-to-tackle-healthcare-problems*

[10] European Commission, *European eHealth Interoperability Roadmap*, December 2010, *www.ehgi.eu/Download/European%20eHealth%20Interoperability%20Roadmap%20[CALLIOPE%20-%20published%20by%20DG%20INFSO].pdf*

[11] *Op cit*, Murray, et al.

[12] eScience News, 'National Survey Finds Information Tech and Business Alignment a Struggle for American Companies', 22 September 2008, *http://esciencenews.com/articles/2008/09/22/national.survey.finds.information.tech.and.business.alignment.a.struggle.american.companies*

[13] Shaffer, V.; A. Roswell-Jones; B. Runyon; 'The State of IT Governance in Healthcare Delivery Organizations and How to Make It Better', Gartner, 25 June 2007, *https://www.gartner.com/doc/507917/state-it-governance-healthcare-delivery*

[14] Datasec, *eHealth Demonstrator Project for IT Governance*, project reports, NHS Fife, 2009, S/N(1), p. 1-69

[15] Mieritz, L.; 'Survey Shows Why Projects Fail', Gartner, 1 June 2012, *https://www.gartner.com/doc/2034616/survey-shows-projects-fail*

[16] ITGI, *IT Governance Global Status Report April 2008*, ISACA, *www.isaca.org*

[17] *Op cit*, Mieritz

[18] *Op cit*, ITGI

[19] *Op cit*, Shaffer, *et al*.

[20] *Op cit*, Datasec

[21] Foh, K.; *Integrating Healthcare: The Role and Value of Mobile Operators in eHealth*, GSMA, May 2002, *www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/05/Role-and-Value-of-MNOs-in-eHealth1.pdf*

[22] *Op cit*, ITGI

[23] Beratarbide E.; T. Kelsey; *eHealth Governance in Scotland: A Cross-sectoral and Cross-national Comparison*, Springer Berlin Heidelberg, UK, 2013, *http://link.springer.com/chapter/10.1007/978-3-642-22474-4_13*

[24] *Op cit*, World Bank

[25] Eccles M.; D. Armstrong; R. Baker; K. Cleary; H. Davis; S. Davies; et al.; 'An Implementation Research Agenda', *Implementation Science 2009*, *www.implementationscience.com/content/4/1/18*

[26] Clinical Effectiveness Research Agenda Group, *An Implementation Research Agenda*, 2009, *www.biomedcentral.com/content/supplementary/1748-5908-4-18-S1.pdf*

[27] *Op cit*, Beratarbide and Kelsey

[28] Beratarbide E; *Critical Factors in the Adaptation of NHS to the Information Society in Fife: An Initial Causal Model*, project reports, 2008, p. 1-60

[29] Beratarbide, E.; *Proceedings of the IADIS International Conference eHealth 2010*, IADIS, Freiburg, Germany, 30 June 2010

[30] *Op cit,* Datasec

[31] Beratarbide E.; T. Kelsey; *eHealth Governance, A Key Factor for Better Health Care: Implementation of IT Governance to Ensure Better Care Through Better eHealth*, IGI Global, 2011, *www.igi-global.com/chapter/ehealth-governance-key-factor-better/52361*

[32] *Op cit*, Luftman

[33] *Op cit*, Henderson and Venkatraman

[34] Full results and conclusions are described in a comprehensive e-health technical report available in the ISACA Knowledge Center, *www.isaca.org/monitoring-progress-on-ehealth*.

Cloud Insecurities

Larry G. Wlosinski, CISA, CISM, CRISC, CAP, CBCP, CDP, CISSP, ITIL V3, is an IT security consultant at ActioNet Inc., with more than 15 years of experience in IT security. Wlosinski has been a speaker on cloud security at US government and professional conferences and meetings, and has written numerous articles on the topic for professional magazines and newspapers.

Information security events that affect cloud systems are occurring with no end in sight, so it should be no surprise that the cloud should be treated as a nonsecure environment with numerous threats and concerns. The cloud has all of the same (and even more) vulnerabilities and weaknesses as other computing platforms, including configuration issues, patching and upgrade requirements (to fix weaknesses), source code issues, unauthorized privilege escalation, and unexpected downtime, to name a few. A statistical analysis of cloud security incidents over a five-year period identified 175 cloud security incidents and 12 threats to cloud security (**figure 1**).[1]

Figure 1—CSA Threat Categories and Incident Counts

Number	Threat	Incidents
1	Abuse and nefarious use of cloud computing	12
2	Insecure interfaces and application programming interfaces (APIs)	51
3	Malicious insiders	3
4	Shared technology issues	5
5	Data loss or leakage	43
6	Account or service hijacking	3
7	Unknown risk profile	11
8	Hardware failure	18
9	Natural disasters	4
10	Closure of cloud service	4
11	Cloud-related malware	6
12	Inadequate infrastructure design and planning	15
	TOTAL	**175**

The average unavailability of cloud services has been stated to be 7.5 hours per year, which amounts to an availability rate of 99.9 percent. The cost of an hour-long outage ranges between US $89,000 and US $225,000 per hour.[2] These costs underscore the importance of having a cloud security program within an organization that will satisfy customer expectations.

The following information on vulnerabilities, threats and weaknesses is intended to not only enlighten those who manage the cloud, but also bring an awareness of what to monitor and how to implement and maintain a secure cloud environment.

PROVIDER VULNERABILITIES

The threats to cloud platforms are ongoing and affect everyone who uses cloud services for business or personal reasons.[3] **Figure 2** contains a list of recent examples of cloud-related events that were the result of security weaknesses at the provider.

PREVENTING EVENTS

The solutions lie with the providers. Providers need to implement more proactive programs in the areas of configuration management, web application hardening, internal security (e.g., background checks) and continuous monitoring, which include a regular patching program, updating of antivirus systems and event log management. The cloud service providers (CSPs) should also have mirrored systems to provide for increased uptime, a means for a patching program and business continuity for their customers.

Actions that should be taken to prevent events like those listed in **figure 2** include:

- **Configure the network and devices**—Applicable actions include removing unnecessary services and setting control parameters to only what is necessary.
- **Patch and update the system components regularly**—This includes the operating system, commercial-off-the-shelf (COTS) products, system utilities and the software that is used for custom applications. Do not expect the software used to be perfect. It is subject to human error as well.
- **Run vulnerability scans and remediate weaknesses as quickly as reasonably possible**—Critical and high vulnerabilities are the most serious and should be corrected as soon as possible.

Figure 2—Vendor Vulnerability Summary			
Report Date	**Provider/Vendor**	**Problem Type**	**Event**
9 October 2012	CloudStack	Configuration issue	The system had a configuration issue that meant any use could execute arbitrary CloudStack API calls, such as deleting all virtual machines (VMs) in the system.
22 October 2012	Amazon AWS	System not available	Several web sites that use Amazon's AWS cloud computing service for hosting, including Reddit, Coursera, Flipboard, FastCompany, Foursquare, Netflix, Pinterest and Airbnb, were taken down as it experienced degraded performance for a small number of Elastic Block Store (EBS) volumes in a single availability zone in the Northern Virginia (USA) zone.
30 October 2012	Not specified	Inadequate CSP protection	Some CSPs failed to detect and block malicious traffic originating from their networks, which provided cybercriminals with an opportunity to launch attacks in a botnet-like fashion, according to a report from security consultancy firm, Stratsec.
6 November 2012	Amazon EC2	Inadequate key protection	Scientists devised a VM that can extract private cryptographic keys stored on a separate VM when it resides on the same piece of hardware.
16 November 2012	VMware	Directory traversal vulnerability	VMware patched a critical vulnerability in its VMware View desktop virtualization product that could have led to a directory traversal attack and an attacker reading or downloading files without the need for authentication.
28 November 2012	Cloud browsers	Mobile device weaknesses	Researchers found that mobile device browser services can be abused to crack passwords, wage denial-of-service (DoS) attacks or perform other unauthorized computations with the free computing power.
28 March 2013	Amazon	Data exposure	A researcher at Rapid 7 found sensitive files exposed to the Internet in Amazon's Simple Storage System (S3) cloud service due to users improperly configuring the service.
25 August 2013	Amazon	Data integrity	A packet loss issue at an Amazon cloud services data center caused outages for several high-profile web services including Instagram, Netflix and Vine. The problem was caused by a partial failure of a networking device.
15 November 2013	VMware	Account privilege escalation	VMware released updates for its VMware Workstation and VMware Player software, thereby fixing a vulnerability in how shared libraries are handled. The vulnerability could have allowed an attacker to escalate their privileges to root.
4 December 2013	VMware	Privilege escalation	VMware published updates for certain versions of its Workstation, Fusion, ESXi and ESX products, closing a vulnerability that could have allowed privilege escalation in older versions of Windows.
31 January 2014	Oracle's Java	Unauthorized access and more	Researchers at Security Explorations analyzed Oracle's Java Cloud Service and found 28 security issues—16 of which could be leveraged to bypass the Java security sandbox of a targeted WebLogic server environment. The vulnerabilities could also be leveraged to gain access to deployments of other users in the same regional data center.
23 April 2014	Amazon	Missing patches	In the course of a customer-prompted investigation, researchers at Bkav found that several servers for Amazon's cloud Infrastructure as a Service (IaaS) and HP's public cloud service contain several vulnerabilities as a result of Microsoft Windows Server installations not being updated for several months.
15 May 2014	Adobe	System availability	Adobe restored service to users of its Creative Cloud service after a 24-hour outage that left users unable to use some aspects of the service and unable to use the service if not already logged in.
25 June 2014	Oracle DB Java VM	Privilege escalation	Security Explorations' researchers reported finding 22 vulnerabilities affecting the Java VM implementation used in Oracle Database that could be leveraged by an attacker to escalate privileges and execute arbitrary Java code on vulnerable Oracle Database servers.

Figure 2—Vendor Vulnerability Summary *(cont.)*			
Report Date	**Provider/Vendor**	**Problem Type**	**Event**
26 June 2014	VMware	Product vulnerabilities	VMware released an update for its vCenter Operations Management Suite (vCOps) that closed several vulnerabilities affecting the Apache Struts Java application framework.
23 July 2014	VMWare vCenter servers	Product vulnerabilities	Data collected and analyzed by CloudPhysics found that 57 percent of deployed VMware vCenter servers and 58 percent of ESXi hypervisor hosts remained vulnerable to the Heartbleed virus in OpenSSL, affecting 40 percent of organizations in the CloudPhysics dataset.
2 October 2014	VMware	Product vulnerabilities	VMware releases a software patch to fix Shellshock bug.
Based on: US Department of Homeland Security (DHS), Daily Open Source Infrastructure Reports, USA, 2013-2014, *www.dhs.gov/dhs-daily-open-source-infrastructure-report*			

- **Design and implement good architectural best practices**—This includes having at least one firewall. If an organization is on the receiving end of a DoS attack, consider sharing (or splitting) the attack among multiple and/or layered firewalls. Having an intrusion detection system (IDS) and an intrusion prevention system (IPS) that is monitored daily is essential to protecting systems and data. If an organization lacks internal capability, investigate Security as a Service (SecaaS). Having a third party that is dedicated to protecting an organization's assets will compensate for lack of staff or the appropriate skill sets. Organizations should also consider having a network architect to design a secure environment.
- **Prepare for unexpected hardware failures**—This can be done with spare devices/components, a tested contingency plan and, possibly, a mirrored site.

CRIMINAL ACTIVITY

Since October 2012, many criminal and malicious activities have occurred in the cloud environment, for example:

- VMware source code exposure[4]
- Advanced persistent threats (APTs) utilizing cloud-based platforms[5]
- Cybercriminals using cloud services to distribute their malware[6]
- Cybercriminals using Google Cloud Messaging as a command and control for their Android malware[7]
- Spammers using SoundCloud to spread links to spam[8]
- Cloud hosting service provider DigitalOcean targeted by a distributed denial-of-service (DDoS) attack[9]
- A cloud-based Microsoft Structured Query Language (MSSQL) database used by a botnet to steal online banking credentials[10]
- A hypervisor management console used by attackers who exploited an insecure password[11]
- Cybercriminals abusing cloud services to create and host malicious web sites[12]
- The Trojan Zeus used to attack Platform as a Service (PaaS) and Software as a Service (SaaS) infrastructures[13]
- Vulnerabilities in major web browsers used to compromise cloud-based point of service (PoS) software used by grocery stores, retailers and small businesses[14]
- CodeSpaces ceased operations because an attacker accessed their Amazon Elastic Compute Cloud (EC2) and deleted the customer database and most backups[15]
- Botnets and malware hosted on cloud servers[16]
- Attackers using Amazon Cloud Services to launch DDoS attacks[17]
- Cybercriminals using Amazon cloud to host Linux DDoS Trojans[18]

To combat these types of events, the following actions could have been taken by CSPs:

- Implement a company security program that includes patching, configuration management, firewall, antivirus software, intrusion detection and prevention systems, testing backup recovery capability, performing web site scans, and using data encryption whenever possible (especially for critical systems and sensitive data).
- Conduct awareness training. Users need to be trained on spam and other criminal tricks that can circumvent technical defenses.
- Implement a secure network design that is able to withstand DDoS attacks.
- Implement password strength testing and controls that limit access attempts.

- To prevent (or limit) cloud provider misuse, implement a program of continuous monitoring of outbound traffic for contract violations (i.e., enforcement of security practices), implement SecaaS, and harden web sites/applications against SQL attacks.

OTHER WEAKNESSES

Weaknesses in the cyberworld that affect cloud system users include users not having the tools or means to prevent remote access. One example is that operating systems (OSs) do not identify what is running in the tasking/monitoring table(s). Since the utilities are cryptic, users will not even try to end a system process on their computer because they fear that deleting one could possibly harm their system(s). More actionable information needs to be available to users in the operating system utilities to protect their computing devices because purchased, existing tools (e.g., firewalls, antivirus software, intrusion detection systems) are not good enough. User action is the last resort and the OS information provided is currently insufficient to protect these devices. Malware is constantly being installed on home computers and portable devices via the Internet, and the cloud and CSPs are being used as distribution agents for criminals. Providers need to implement security measures similar to those that governments and financial institutions use to protect their systems and their data.

Vendor products, such as security suites, that continually report that a system has weaknesses and that settings have changed and malware are other areas of concern. Vendors need to come together to unite their efforts for the optimal solution. Competition between antivirus vendors can do only so much to aid the user. This is because vendors are not constantly at their best. Reasons include being distracted by company takeovers, loss of key staff and poor product comparative ratings. These product weaknesses affect everyone and need to be dealt with in a cooperative manner.

> "Think like criminals in order to better know their methods."

WHAT ELSE CAN BE DONE?

To prevent misuse of the cloud, organizations should think like criminals in order to better know their methods, asking themselves, for example: How does the organization combat an attack system that searches all computers connected to the Internet for weaknesses? The answer may lie in understanding a cybercriminal's approach to conducting an attack. The following steps taken by an attacker leading up to an attack can be analyzed and countermeasures implemented:

1. Gather data of device weaknesses.
2. Create or obtain a program or series of programs to exploit those weaknesses.
3. Plant malware to allow access and retrieve data of value from those devices.
4. Categorize the devices by expected value (e.g., bank, accounting system, private personnel information, normal users).
5. Assign specialists to search and retrieve data of value (e.g., account numbers, customer names, passwords, privacy information).
6. Store and compile the data for misuse (e.g., funds transfer, blackmail, identity theft, resale).

Another question to ask is: If one knows what countries are not cooperating with capturing and preventing malicious cyberactivity, what can be done to prevent those countries from receiving data? Furthermore, should there be a strengthening of international laws (especially by country) to restrict the data they receive? Do new monitoring devices and/or software that enforce the law(s) need to be created and implemented? Where could these protective tools be placed, and could they be used to track the source(s)?

With all of the vulnerabilities, threats and malicious activity that are going on, it is important to be as vigilant with a private cloud (i.e., your in-house computing environment) as with public clouds.

CONCLUSION

In addition to what businesses can do to protect themselves, authorities need to work with businesses to implement protections and enforcement on a global scale. Many clouds are not only global in nature, but because of the surge in mobile devices and applications, they affect many people wherever they go.

ENDNOTES

[1] CSA Cloud Vulnerabilities Working Group, "Cloud Computing Vulnerability Incidents: A Statistical Overview," Cloud Security Alliance, 13 March 2013, *https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/*

[2] Essers, L.; "Cloud Failures Cost More Than $70 Million Since 2007, Researchers Estimate," *PCWorld*, 19 June 2012, *www.pcworld.com/article/257860/cloud_failures_cost_more_than_70_million_since_2007_researchers_estimate.html*

[3] US Department of Homeland Security (DHS), Daily Open Source Infrastructure Reports, USA, 2013-2014, *www.dhs.gov/dhs-daily-open-source-infrastructure-report*

[4] Leyden, John; "More VMware Secret Source Splattered Across Internet," *The Register*, 5 November 2012, *www.theregister.co.uk/2012/11/05/vmware_source_code_leak/*

[5] Kovacs, Eduard; "Experts Reveal How Chinese APT Hackers Abuse Dropbox and WordPress," *Softpedia*, 12 July 2013, *http://news.softpedia.com/news/Experts-Reveal-How-Chinese-APT-Hackers-Abuse-Dropbox-and-WordPress-367652.shtml*

[6] Vijayan, Jaikumar; "Attackers Turning to Legit Cloud Services Firms to Plant Malware," *Computerworld*, 2 August 2013, *https://www.computerworld.com/s/article/9241324/Attackers_turning_to_legit_cloud_services_firms_to_plant_malware*

[7] Kovacs, Eduard; "Hackers Abuse Google Cloud Messaging Service in Android Malware Attacks," *Softpedia*, 14 August 2013, *http://news.softpedia.com/news/Hackers-Abuse-Google-Cloud-Messaging-Service-to-Distribute-Android-Malware-375327.shtml*

[8] Kovacs, Eduard; " SoundCloud Users Warned of Spam Shady Software, Scams," *Softpedia*, 22 August 2013, *http://news.softpedia.com/news/SoundCloud-Users-Warned-of-Spam-Shady-Software-Scams-377395.shtml*

[9] Kovacs, Eduard; "Cloud Hosting Company DigitalOcean Hit by DDoS Attack," *Softpedia*, 28 August 2013, *http://news.softpedia.com/news/Cloud-Hosting-Company-DigitalOcean-Hit-by-DDOS-Attack-378713.shtml*

[10] Jackson Higgins, Kelly; "Cybercriminals Now Enlisting Database Cloud Services," *InformationWeek* DARKReading, 11 December 2013, *www.darkreading.com/attacks-breaches/cybercriminals-now-elisting-database-clo/240164662*

[11] Kovacs, Eduard; "Softpedia, OpenSSL Website Hacked Through Insecure Password at Hosting Provider," *Softpedia*, 3 January 2014, *http://news.softpedia.com/news/OpenSSL-Website-Hacked-Through-Insecure-Password-at-Hosting-Provider-413377.shtml*

[12] Kovacs, Eduard; "Man Admits Hacking Former Employer's Systems to Damage Servers and Reputation," *Softpedia*, 9 January 2014, *http://news.softpedia.com/news/Man-Admits-Hacking-Former-Employer-s-Systems-to-Damage-Servers-and-Reputation-415363.shtml*

[13] Peters, Sara; "Zeus Being Used in DDoS, Attacks on Cloud Providers," *InformationWeek* DARKReading, 10 June 2014, *www.darkreading.com/zeus-being-used-in-ddos-attacks-on-cloud-providers/d/d-id/1269554*

[14] Rashid, Fahmida Y.; "Cybercriminals Targeting Cloud-based PoS Systems Via Browser Attacks," *Security Week*, 12 June 2014, *www.securityweek.com/attackers-targeting-cloud-based-pos-systems-browser-attacks*

[15] Greenberg, Adam; "Code Space Shuts Down Following DDoS Extortion, Deletion of Sensitive Data," *SC Magazine*, 19 June 2014, *www.scmagazine.com/code-spaces-shuts-down-following-ddos-extortion-deletion-of-sensitive-data/article/356774/*

[16] Butler, Brandon; "Hackers Found Controlling Malware and Botnets From the Cloud," *NetworkWorld*, 26 June 2014, *www.networkworld.com/article/2369887/cloud-security/hackers-found-controlling-malware-and-botnets-from-the-cloud.html*

[17] Constantin, Lucian; "Attackers Install DDoS Bots on Amazon Cloud, Exploit Elasticsearch Weakness," *Computerworld*, 28 July 2014, *www.computerworld.com/s/article/9249991/Attackers_install_DDoS_bots_on_Amazon_cloud_exploit_Elasticsearch_weakness?taxonomyId=17*

[18] Kovacs, Eduard; "Cybercriminals Abuse Amazon Cloud to Host Linux DDoS Trojans," *Security Week*, 28 July 2014, *www.securityweek.com/cybercriminals-abuse-amazon-cloud-host-linux-ddos-trojans*

Selected COBIT 5 Processes for Essential Enterprise Security

Fredric Greene, CISSP, is an experienced IT auditor specializing in technology infrastructure in the financial services industry. Vice president of IT audit at MUFG Union Bank, he has presented at international conferences and provided in-house corporate training and seminars on information security, risk-based auditing, IT risk and control assessment, ITIL framework practices, and database auditing. Greene previously worked for the legacy organization Bank of Tokyo (prior to its merger to form MUFG Union Bank), Depository Trust & Clearing Corporation (DTCC) and KPMG.

Selected processes from the COBIT® 5[1] framework can improve the effectiveness of enterprise security in an organization. The objective here is to develop a security strategy with technical processes, controls and tools for security across an enterprise. This is a risk-based strategy to defend critical enterprise resources against a wide range of threats and vulnerabilities.[2]

The risk component of this strategy includes a coherent, well-thought-out approach to identify, inventory, analyze, manage and respond to key risk factors. Using this risk approach, security efforts can be focused to defend networks, end points and data against malware and other threats.

The assumption here is that much of the IT governance, organization structure, policies and skilled talent are in place.

The threat landscape appears very intimidating at the moment. High-profile organizations including banks, government agencies and retailers are recent victims of exploits and attacks. What is even more intimidating is that these organizations have the resources to defend themselves, yet even they have fallen victim. The security posture of small and mid-sized businesses (SMBs) and other sectors of the global economy appears to be vulnerable.

Threats may include cybercrime (e.g., fraud, theft, destruction of IT resources, blackmail, extortion), social or political hacktivism, or advanced persistent threats (APTs) with national or commercial objectives. Threats may come from foreign governments, organized crime syndicates, hacktivists with an agenda, and employees or consultants from within the organization.

STRATEGY TO IMPROVE SECURITY

What is a smart strategy and what specific steps can be taken to quickly improve enterprise security?

COBIT 5 provides guidance on best practices for enterprise security. Other sources of best practices to consider include: ISO 27001 (information security),[3] ISO 27032 (guidelines for cybersecurity),[4] the US National Institute of Standards and Technology (NIST) SP 800-53 (recommended security controls),[5] NIST Framework for Improving Critical Infrastructure Cybersecurity[6] and SANS Critical Security Controls[7] (top 20).

Turkçesi de bulunmaktadır
www.isaca.org/currentissue

COBIT 5 includes a set of seven enablers for the governance and management of enterprise IT (GEIT), one of which is processes. Of the 37 COBIT 5 processes, this article focuses on three core security processes:

- APO12 *Manage risk*
- APO13 *Manage Security*
- DSS05 *Manage security services*

APO12 MANAGE RISK

This Align, Plan and Organize (APO) process is a prerequisite for any set of security controls and is referenced by virtually every framework or standard on information security. A risk assessment process is essential to identify an organization's "crown jewels" and to focus resources on the most critical, sensitive, threatened and vulnerable areas.

Specific practices that make up the *Manage risk* process follow. Data should be collected from all relevant sources (e.g., systems, applications, networks, databases) in multiple categories (e.g., access, configurations) to support the understanding of risk (APO12.01); these data should be considered in the risk analysis, especially for business impact analysis (what is important to the enterprise), estimating the probability of different threats and identifying the mitigating controls in place (APO12.02).

Risk profiles should be maintained on an inventory of business processes and the supporting IT systems, applications, infrastructure, data, facilities and capabilities (APO12.03). This inventory should be used to identify the IT elements/assets that are most critical (highest risk)

and that require the strongest controls. Risk indicators or factors (internal/external) used to maintain this inventory should be reviewed and validated periodically.

Key stakeholders should be kept informed through the articulation of risk status, including worst-case and most-probable scenarios (APO12.04). A risk management action portfolio should be defined and maintained for the control activities to manage, avoid, prevent or transfer (insurance) risk (APO12.05).

Response to risk events should be timely and effective based on formal test plans (APO12.06). Such plans should be prepared, maintained and tested periodically for responding to IT-related incidents that may impact business operations.

APO13 MANAGE SECURITY

This APO process consists of defining, operating and monitoring an information security management system (ISMS). This is an essential link to translate the risk process into effective security services. To build this ISMS, risk and security professionals should consider and document risk appetite, security requirements and security solutions.

Specific practices that make up the *Manage security* process follow. An ISMS (APO13.01) should be established as a standard, formal and continuous approach to IT security. This approach should be aligned with business requirements and business processes.

To formalize this approach, an information security risk treatment plan should be defined based on realistic business cases and implemented as part of strategic objectives and enterprise architecture (APO13.02). The overall ISMS should be monitored and reviewed regularly (APO13.03) through management reviews and security audits. An underlying theme here is a culture of security and continual improvement.

DSS05 MANAGE SECURITY SERVICES

This Deliver, Service and Support (DSS) process covers technical security controls to defend the most critical, vulnerable and sensitive resources including information (data), network and communications infrastructure, network end points (e.g., users, PCs), and systems access.

Specific practices that make up the *Manage security services* process follow. Protection against malware (viruses, worms, spyware, scanning tools, remote access tools) should be implemented through threat (malware) detection systems (e.g. Next Generation firewalls), intrusion detection/prevention systems (IDS/IPS), searchable event (log) repositories (e.g. security information and event management [SIEM] systems), forensic capabilities (tools) and the maintenance of security patches. Malware should be prevented, detected and removed at all layers of the IT environment including applications, operating systems, networks, shared resources (e.g., directories) and hardware (e.g., USB ports) (DSS05.01).

Network security should be actively managed with an integrated strategy and set of tools across network layers and topology (e.g., switch/router access control lists [ACL], firewalls, IDS/IPS). Controls should be deployed at all points of entry including email, web applications, file transfer protocols, social networking, messaging, cloud applications/storage and hardware (USB) ports (DSS05.02).

End-point security (antivirus/antimalware software, web/email security, firewalls) should be deployed and managed to ensure that laptops, desktops, servers and mobile devices are adequately secured (as measured against value of information). High-value targets (e.g., crown jewels) should be protected with stronger security and controls (DSS05.03).

User identity and logical access should be managed on business need-to-know and least-privilege bases. A good practice is to strengthen controls around authentication (i.e., user ID, password) and authorization to sensitive resources. One must ensure that privileged or administrator access (e.g., "keys to the kingdom") is especially well-controlled and monitored (DSS05.04).

Physical access to IT assets should be managed with procedures to grant, limit and revoke physical access to

organization sites based on business need. Access should be justified, authorized, logged and monitored (DSS05.05).

Sensitive documents (e.g. special forms, negotiable instruments) should be safeguarded with appropriate controls. Output devices (e.g. security tokens) should also be controlled with an accurate accounting (DSS05.06).

Security monitoring of IT infrastructure is a key component of the control environment. A set of robust controls and tools such as a searchable repository (e.g., SIEM system), centralized and secure log aggregator systems, forensic tools and processes, and malware detection software (event correlation, rule based, pattern recognition) should be considered. Integration with incident management and escalation processes (DSS05.07) should be ensured.

CONCLUSION

The three essential COBIT 5 processes for information security—*Manage risk* (APO12), *Manage security* (APO13) and *Manage security services* (DSS05)—offer a risk-based approach to defend enterprise resources against a wide range of threats and vulnerabilities. The risk process is the prerequisite to any security process—first to understand and assess risk before managing and controlling risk. The logical next step is to manage a coherent security program with appropriate controls focused on the highest risk assets and resources.

As the threat landscape gets more complex, these processes represent the critical path toward effective security.

COBIT® 5 for Information Security, an extension of the core framework with a focus on information security, includes practical guidance on information security processes in an enterprise environment along with a wealth of supporting detail including service capabilities, policies, principles, security-specific organizational structures, security skills and competencies.

ENDNOTES

[1] ISACA, COBIT 5, 2012, *www.isaca.org/cobit*

[2] ISACA, *Transforming Cybersecurity: Using COBIT® 5*, 2013, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx*

[3] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements,* 2005, *www.iso.org/iso/catalogue_detail?csnumber=42103*

[4] ISO, ISO/IEC 27032:2012, *Information technology—Security techniques—Guidelines for cybersecurity,* 2012, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375*

[5] National Institute of Standards and Technologies, SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," USA, 2010, *http://csrc.nist.gov/publications/PubsSPs.html*

[6] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2014, USA, *www.nist.gov/cyberframework/*

[7] SANS Institute, *Critical Security Controls*, *www.sans.org/critical-security-controls/*

Evaluating Information Security Solutions

Swapping the Cost of Failure for Success

Kerry A. Anderson, CISA, CISM, CGEIT, CRISC, CCSK, CFE, CISSP, CSSLP, ISSAP, ISSMP, is an information security professional with more than 17 years of experience in information security and compliance. She is an adjunct professor in cybersecurity at Clark University (Worcester, Massachusetts, USA). Anderson is the author of numerous articles in professional journals and the book, *The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture*, and has been a speaker, panelist, moderator and chairperson at many professional conferences. She can be reached at *kerry.ann.anderson@verizon.net.*

One of biggest budget busters for an information security program is technology solutions that are not a good match for the organization. Often, the technology is more than adequate in terms of functionality; however, other attributes of the solution may clash with the organization's needs and culture. Some acquisitions fail because there is a poor match between the solution's functionality and the capabilities required to meet the real needs to ensure the organization's security posture. Thus, it is critical to identify and evaluate security technology solutions to maximize the potential for a successful implementation.

The number of information security solutions available has grown exponentially as the marketplace for these products has matured. Much of the demand for these products has resulted from one or more of the following factors:

- Regulatory compliance requirements and legislation
- Increasing incidence of data breaches
- Increase in hacktivism
- Increasing cyberthreat landscape
- Trend toward IT consumerism, such as bring your own device (BYOD)

While the increase in solution alternatives makes it easier for an organization to find a security product that offers the perfect fit for its specific requirements, the myriad of options can be confusing for the information security manager. In addition, there is a key trend among solution vendors to merge new functionality into their core products, which previously existed as stand-alone applications, such as malware-detection capabilities in a vulnerability management suite. It can be more difficult to evaluate these hybrid solutions when seeking to fill gaps in the information security organization's tool set. Besides enhanced functionality, vendors may offer their products under a variety of service models, such as private or public clouds or on-premise options.

SYMPTOMS AND COSTS OF A POOR FIT BETWEEN ORGANIZATION NEEDS AND SOLUTION

The consequences of a poor fit between the actual needs of the organization and a security solution may surface as the following symptoms:

1. Consuming too many resources and too much time
2. Requiring extensive technical and product expertise
3. Necessitating extensive customization
4. Purchasing supplementary solutions to augment missing functionality
5. Extensive manual workarounds

In addition to creating frustration for staff and customers, a bad match between the solution and the organization can waste budget resources. For example, an organization purchased a data loss/leak prevention (DLP) solution for US $250,000, only to replace it with another equally costly solution within a few years. The advantages of wrapping a more extensive solution evaluation process around the product acquisition would have increased costs on the front end, but the benefits would exceed the expenditure and include:

- Diminishing the need for do-overs or premature replacement of a solution
- Decreasing costs associated with excessive consulting, customization or training due to incompatibilities with the infrastructure or organizational culture

COMMON MISTAKES IN EVALUATING SECURITY SOLUTIONS

One mistake that information security managers seeking security solutions to fill a gap in their tools portfolio or replace an existing product make is to develop a set of selection criteria that mirrors a solution with which they are familiar. The disadvantages to using this approach for the creation of solution criteria include:

- May lead to single-sourcing because no other vendor offering meets overly specific criteria

- Limits exploration of other options or solutions
- Discourages performing an assessment to determine specific needs to be filled by a solution

The information security manager or individual responsible for performing a needs analysis may omit this step and jump to vendor selection. Often, the outcome can be summed up as "if it does not fit, I will make it fit" because the information security team attempts to make a solution work. The result is a subpar solution that may require premature replacement. Insufficient product evaluation prior to purchase could potentially result in a solution with capabilities that are inconsistent with the sales pitch or the organization's security needs.

OPTIMIZING ACQUISITION USING A STANDARD EVALUATION PROCESS

A standard evaluation process allows potential solutions to be assessed based on an agreed-upon set of criteria designed to meet the identified needs of the organization. At its essence, it allows an apples-to-apples comparison of essential features. Additionally, it avoids the potential for undue vendor or other internal influences on the purchasing decision by vetting all possible solutions against a common set of criteria. The objective of this process is to narrow the possible set of alternatives down to a few—perhaps two or three—potential solutions for further assessment:

1. **Document key requirements and restrictions.** Start by determining the specific needs and requirements the organization must fill to increase its security posture. This is a list of must-haves that are generally nonnegotiable. While this might seem obvious, the information may not be documented and functionality that is cool or nice-to-have may overshadow the original purpose for seeking a security solution. Before proceeding with seeking potential vendors, the following needs to be recorded and agreed upon by stakeholders:
   - What need(s) will the solution fill? The needs should be concise and ideally written in vendor-neutral language.
   - Are there any specific restrictions or requirements, such as operating systems, compatibility with other solutions or other architectural issues, that must be taken into consideration?
   - Does a budget exist for this purchase? If so, what is the upper limit in terms of initial purchase price?
   - In addition to the solution, what other costs need to be taken into consideration related to the acquisition, such as training and consulting?

2. **Use the Goldilocks Principle.** The Goldilocks Principle states that a solution to something must fall within certain parameters rather than going to extremes in terms of offering too little or too much functionality. The most successful solutions provide a "just right" balance in terms of benefits received, security needs met and resources required for support.

> "The most successful solutions provide a 'just right' balance in terms of benefits received, security needs met and resources required for support."

   Additional features outside the scope of an organization's needs, rather than providing potential extra value, can add costs because unwanted functionality cannot be disabled easily, becomes reactivated in successive releases or requires additional workarounds. This may be true when a feature such as monitoring functionality runs contrary to the organizational culture. To simplify, an organization would be paying for something it cannot use, and that is a waste of money.
3. **Avoid "analysis paralysis."** Without specific criteria to provide guidance to identify appropriate solutions, an information security team may cast too wide of a net in its search. The result could lead to analysis paralysis with the consequences of additional purchasing costs and longer acquisition times.
4. **Consider total cost of ownership.** When evaluating a security solution, it is important to consider the total cost throughout its life cycle. Rather than focusing on the immediate acquisition costs, estimate the total expenditures required to implement and support the solution throughout its expected life cycle. Implementation of innovative technology or

unfamiliar solutions can require extensive consulting beyond basic setup fees included in the purchase price. According to Fred Brooks, author of *The Mythical Man-Month*, the costs of support and maintenance may be up to 90 percent of an initial technology investment.[1] It can be tempting to believe some of these costs, such as consulting and training, are optional and do not need consideration in preparation of an initial cost estimate. However, for many solutions involving complex technologies, these expenditures are necessary for a successful implementation and adoption of the product. Some components of the total cost of the solution may include:

- Training
- Testing
- Consulting
- Legal
- Required infrastructure upgrades
- Hiring additional staff

5. **Develop use cases.** Use-case diagrams[2] are a simple way to document requirements. They are graphic representations using stick figures (actors) and ovals (use cases) with lines documenting their interactions. Use cases provide a way to document the required processes from the point of view of the users. A complete use case consists of diagrams and textual descriptions. Use cases offer some clear benefits to evaluating candidate solutions, including:
   - Providing a mechanism to allow stakeholders to walk through a process with the inclusion of different solution alternatives. This answers the question: How would this work with solution X?
   - Identifying any potential issues.

   Use cases do have a limitation in regard to documenting requirements. Use cases are an effective technique for capturing and documenting functional requirements. However, functional requirements are only one type of requirement. Other types of requirements include legal and compliance requirements, architectural strategy, usability, reliability, and performance requirement. Therefore, it is important to identify the relationship between the functional requirements captured in the use cases and other types of requirements.

USING SWOT AS AN EVALUATION TOOL FOR SECURITY SOLUTIONS

After the possible field of contenders has been reduced to a maximum of two or three, the evaluation process may require a deeper dive to assess each alternative. One method is to perform a strengths, weaknesses/limitations, opportunities and threats (SWOT)[3] analysis of each solution option. SWOT analysis is designed as strategic planning to provide information for matching the organization's resources and competencies to the environment in which it runs. However, it is readily adaptable to evaluation and selection of other alternatives, such as a strategic technology investment. As such, it is instrumental in strategy formulation and selection. As a strategic evaluation tool, SWOT considers the strengths, weaknesses, opportunities and threats involved with the different options. It involves identifying the internal and external factors that are favorable and unfavorable to achieve the objectives of a project (**figure 1**):

- **Strengths**—The solution's strengths are its capabilities that increase its ability to meet or exceed the objective of the acquisition. Examples of such strengths include:
  - Innovative technology
  - Start-up vendor, hungry for opportunities
- **Weaknesses**—In some cases, a weakness may be the other side of strength. A weakness is any attribute that might prevent the achievement of the acquisition's objectives. For example, each of the following may be considered weaknesses:
  - Unproven technology/limited performance history
  - Start-up with limited financial history

Figure 1—SWOT Analysis for Antimalware Solution (Not Actual Product Analysis)

Internal Factors	External Factors
Strengths	**Opportunities**
Multilayered browsing protection against web-based attacks	Provide security-in-breadth by providing heterogeneous antimalware product environment
Smart updates provide frequent automatic updates	Provides protection against malware for remote and network devices
Uses a combination of reactive blacklists and proactive content analysis	
Weaknesses	**Threats**
No central console manager	Potential that users might experience some minimal performance drop
No automatic distribution mechanism	Attack software that could potentially disable application

Source: Kerry A. Anderson. Reprinted with permission.

- **Opportunities**—An external factor that is capable of increasing or optimizing the value of an acquisition. Some examples include:
  - Single, secure authentication mechanism across all platforms and devices
  - Use of two-factor authentication decreasing potential for security breaches
- **Threats**—An external factor that is capable of decreasing the value of an acquisition or diminishing the chance of achieving the acquisition's objectives. Some examples of such threats include:
  - Meeting compliance requirements
  - Untested technology

BENEFITS OF USING SWOT ANALYSIS TECHNIQUE IN SOLUTION EVALUATIONS

Using the SWOT technique can offer insights into the strengths and weaknesses of a solution candidate, its ability to achieve business and technical objectives, and the ability to exploit the solution to support the business strategy. The primary advantages of conducting a SWOT analysis are that it costs very little and can be performed quickly. Additional benefits include:

- Concentrates on the most important factors affecting how a solution might affect a business
- Showcases the solution's weaknesses and strengths
- Offers the potential to identify external opportunities available as well as possible external threats to the organization
- Compares the specific environmental factors of the organization against the candidate solution to determine a potential fit between the two

LIMITATIONS OF USING SWOT ANALYSIS TECHNIQUE IN SOLUTION EVALUATIONS

The results of a SWOT analysis could be misleading if inadequate or incorrect data are used in the analysis. In addition, the resulting analysis could be biased if internal teams wish to sway the purchasing decision toward a particular solution. Additionally, the following are some limitations of the SWOT technique:

- Covers only issues that can positively be considered as a strength, weakness, opportunity or threat
- Does not factor in other issues and nuances with the potential to affect the success of a particular solution within a specific organization
- Does not prioritize issues

A SWOT analysis should not be the sole tool used in the decision-making process. For complex or strategic acquisitions, it may be necessary to conduct additional in-depth analysis.

CRITICAL SUCCESS FACTORS

Critical success factors (CSFs)[4] are influential factors in the success of a project or function. They are required for ensuring the success of an organization. In the evaluation of multiple options available to carry out an initiative, CSFs may appear equally capable of achieving the objectives of the project. However, on closer inspection, specific attributes of one potential solution may present a better fit for the organization.

That solution may offer tangible or intangible benefits more aligned with an organization's culture, mission or direction. Therefore, these factors need to be weighted more heavily in recommending the best alternative to pursue for a specific organization and project. CSFs are elements that are essential for the success of any project or strategy. They propel it forward and can make or break its outcome. Project failures often have their root causation in neglecting to consider CSFs, including:

- Organizational culture
- Ease of use
- User profiles (technical proficiency, backgrounds, job tasks performed)
- Degree of customization possible
- Long-term support requirements

KEY PERFORMANCE INDICATORS

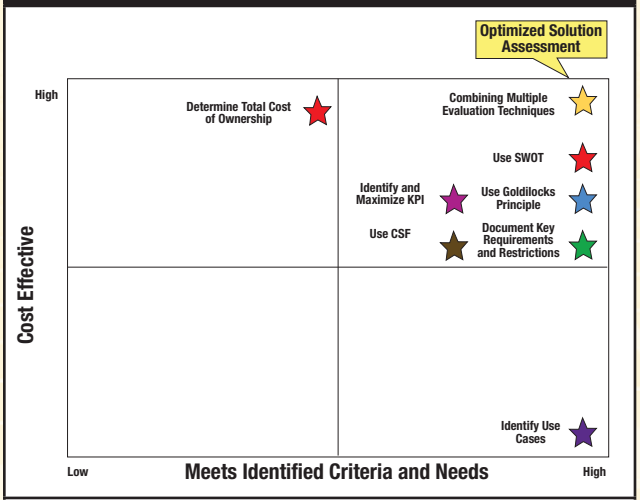
Key performance indicators (KPIs)[5] define and chart progress toward a business or project objectives. KPIs are objective measurements that should reflect the CSFs. Candidate solutions should be evaluated against their ability to meet CSFs and perform against the agreed upon KPIs. Common KPIs include:

- Performance
- Security
- End-user support
- Solution support and maintenance
- Ongoing infrastructure support
- Appropriate functionality
- Ease of modification

SWAPPING THE COST OF FAILURE FOR SUCCESS

The tactical approaches discussed in this article have the objective of optimizing the outcome of the solution assessment by identifying the most cost-effective or fulfilling organizational needs. Each tactic mentioned serves one or both of these purposes when mapped against a matrix of these two benefits. However, it is the combining of these tactics into a comprehensive framework that allows for the achievement of the maximized benefit and for the solution selection process to be optimized (**figure 2**).

Figure 2—Matrix of Benefits for Assessment Tactics



Source: Kerry A. Anderson. Reprinted with permission.

Fully evaluating a list of possible solutions against an agreed-upon set of technical and business criteria increases the opportunity for successful implementation. While common sense says that one should identify what is needed before seeking a solution, in many instances, the order of activities is reversed. Solution selection may be overly influenced by a vendor's persuasiveness or a stakeholder's bias toward a specific product. This consequence may be a poor fit between the product and the organization. Often, the fault for less than successful technology investment is attributed to one or more of the following causes:

- The vendor, sales representative or product itself
- Prior management that made the acquisition
- Lack of senior management support
- Project team

While some of the reasons cited in this article may also be partially true, often the root cause is a poor fit between the solution and the organization. Identifying the best fit between a security solution and a specific organization is analogous to finding the correct piece in a complex jigsaw puzzle. To find the right piece, it is necessary to look at all aspects of the piece itself, as well as the surrounding pieces. If there is a failure to make an appropriate survey of both the piece (solution) and the puzzle (organization), a mismatch may result. Each organization is unique because of a fusion of its culture, mission, vision and individuals. An organization's security solution portfolio must be designed with a custom-made approach to optimize its value.

> "Identifying the best fit between a security solution and a specific organization is analogous to finding the correct piece in a complex jigsaw puzzle."

ENDNOTES

[1] Brooks, Fred; *The Mythical Man-Month, 2nd Edition*, Addison-Wesley Professional, 1995

[2] Visual Paradigm Essential Online Training, "Writing Effective Use Case Tutorial," *www.visual-paradigm.com/tutorials/writingeffectiveusecase.jsp*

[3] Management Study Guide, "SWOT Analysis—Definition, Advantages and Limitations," *www.managementstudyguide.com/swot-analysis.htm*

[4] University of Washington, "Critical Success Factors: Identifying the Things That Really Matter for Success," *https://depts.washington.edu/oei/resources/toolsTemplates/crit_success_factors.pdf*

[5] Reh, John; "Key Performance Indicators (KPI): How an Organization Defines and Measures Progress Toward Its Goals," About.com, *http://management.about.com/cs/generalmanagement/a/keyperfindic.htm*

A Practical Approach to Continuous Controls Monitoring

David Vohradsky, CGEIT, CRISC, is an independent consultant with more than 30 years of experience in the areas of applications development, program management and information risk management. He has previously held senior-level management and consulting positions with Protiviti Inc., Commonwealth Bank of Australia, NSW State Government, Macquarie Bank, and Tata Consultancy Services. Vohradsky is a member of ISACA's CRISC Certification Committee. He can be contacted at *davidvoh9@gmail.com*

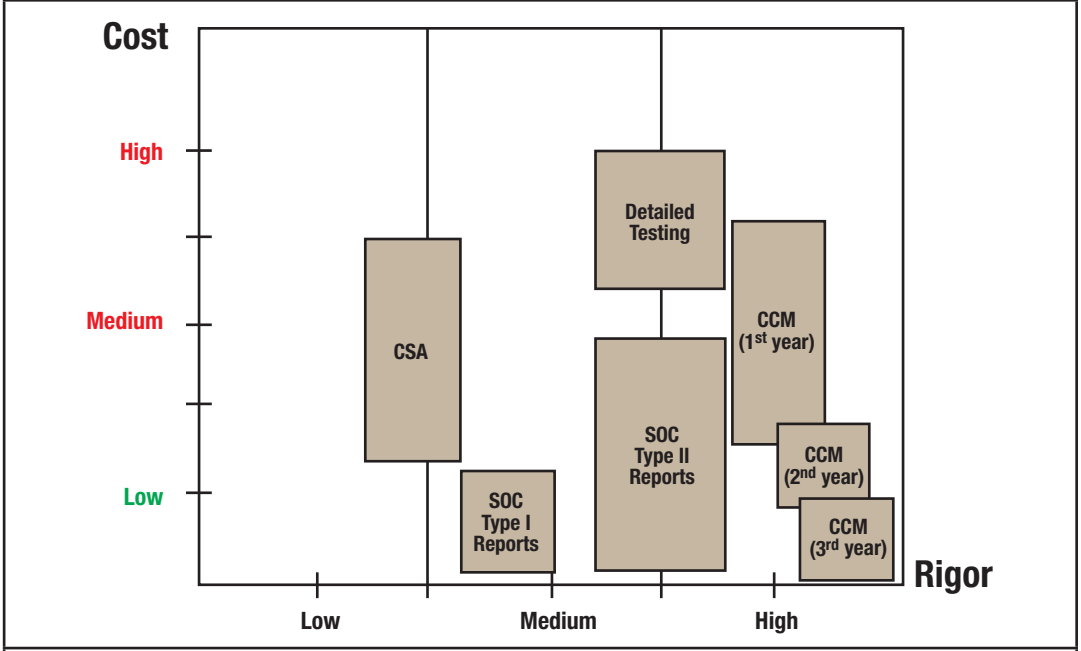
One of the responsibilities of line management in many organisations (particularly in financial services) is to provide assurance to the chief executive officer (CEO) and executives that high-rated risk factors are managed and that appropriate controls are in place and operating effectively.[1] With increases in the regulatory regime, increasing technology complexity and pressures on cost, organisations are seeking productivity improvements in the evaluation of the performance of internal controls. One method of productivity improvement is applying technology to allow near continuous (or at least high-frequency) monitoring of control operating effectiveness, known as continuous controls monitoring (CCM).[2] CCM is a subset of continuous assurance, alongside continuous data assurance (verifying the integrity of data flowing through systems) and continuous risk monitoring and assessment (dynamically measuring risk).

Improved management and monitoring of controls through CCM (and associated risk management activities) may reduce the extent to which audit and assurance staff need to undertake annual detailed testing of controls.[3] In addition to cost reductions through improved efficiency and effectiveness (**figure 1**), other benefits include increased test coverage (through greater sampling and the ability to do more with the same or less labour), improved timeliness of testing, reduced risk velocity and potentially reduced remediation cost, greater visibility (when included in a governance, risk and compliance [GRC] solution), improved consistency, and the ability to identify trends.[4, 5] CCM also allows the replacement of manual, error-prone preventive controls with automated detective controls in which this would reduce the risk profile.[6]

The steps for implementing CCM include:[7, 8, 9]

1. Identify potential processes or controls according to industry frameworks such as COSO, COBIT® 5 and ITIL; define the scope of control assurance based on business and IT risk assessments; and establish priority controls for continuous monitoring.

Figure 1–Indicative Cost-benefit of CCM



Source: David Vohradsky. Reprinted with permission.

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:

2. Identify the control objectives (or goals) and key assurance assertions for each control objective. (Guidelines for the formalisation of assertions may need to be developed as the concept of formal assertions is not well developed within IT risk).
3. Define a series of automated tests (or metrics) that will highlight (or suggest) success or failure of each assertion using a "reasonable person holistic review."[10]
4. Determine the process frequencies in order to conduct the tests at a point in time close to when the transactions or processes occur.
5. Create processes for managing the generated alarms, including communicating and investigating any failed assertions and ultimately correcting the control weakness.

DEFINING CONTROLS TO MONITOR

The scope of overall IT control assurance is usually determined from critical business and IT processes, which are prioritised based on risk and prior experience in reviewing the controls through audits, self-assessments and control breakdowns. For the purposes of example, one can assume the organisation has determined a scope of annual control assurance based on the controls in **figure 2**.

Of these controls, the priorities for implementation of CCM[11, 12, 13] should be based on risk ratings/return on investment (ROI) (such as value to the organisation) and ease of implementation (such as having readily available data from systems and controls that already have an aspect of monitoring and reporting).

Figure 2—Priority of Controls for Continuous Monitoring

In Scope Controls	System	Monitored	Metrics	Risk*	Audit ROI+
Vendor service level agreement (SLA) management	Partial	No	No?		Medium
Software development life cycle (SDLC)	No	No	Yes		Low
Human resources (HR) management	Partial	Operational	No		Medium
User access reviews	Partial	No	Partial	High	High
Segregation of duties	No	No	No		High
Change management	Yes	Operational	Yes	High	High
Incident management	Yes	Operational	Yes		Low
Backup and recovery	Yes	Operational	Yes		Low
Capacity, availability and performance	Partial	Operational	Yes		Medium
IT service continuity	Partial	No	Yes		Medium
IT perimeter security	Yes	Alerts?	No?	High	High
AV management	Yes	Alerts	Yes	Medium	High
Data loss prevention	Yes	Alerts	Yes	High	High
End point encryption	Yes	Alerts	Yes		Medium
Security monitoring	Yes	Operational	Yes	Medium	High

* Self-assessed
\+ Focus areas

Source: David Vohradsky. Reprinted with permission.

In the **figure 2** example, the high-profile controls highlighted by the internal audit function have been assessed against data availability and existing monitoring or metrics. Controls highlighted in green are candidates for continuous control monitoring (red indicates a roadblock that may preclude a control from being considered). The priority or suitability of controls for continuous monitoring also needs to consider the relationships among controls. For example, configuration and vulnerability management rely on asset management, which may be deficient and not suitable for inclusion in the scope of assurance. In such a case, the controls that depend on it may not be suitable for continuous monitoring.

IDENTIFYING ASSERTIONS

Processes for management assurance of controls are usually more informal than an audit because they are often based on professional judgment, rather than detailed testing. An audit is a systematic process in which a qualified team or person objectively obtains and evaluates evidence regarding assertions about a process and forms an opinion on the degree to which the assertion is implemented.[14] To automate an assurance process, control descriptions need to be reviewed to separate those components of the control that can be formally tested and those components that will rely on professional judgement.[15]

Internal control objectives in a business context are categorised against five assertions used in the COSO model[16]—existence/occurrence/validity, completeness, rights and obligations, valuation, and presentation and disclosure. These assertions have been expanded in the SAS 106, "Audit Evidence,"[17] and, for the purposes of a technology context, can be restated in generic terms, as shown in **figure 3**.

COSO objectives are known as enterprise goals, IT-related goals and enabler goals in COBIT 5,[18] and the financial statement assertions are loosely translated in the technology context to "completeness, accuracy, validity and restricted access."[19] Much (if not all) of the literature on CCM relates to business processes, and, as such, there is no documented alignment or mapping among IT control objectives (or goals) and the formal assertions necessary for formalised objective testing.

In an attempt to bridge this gap, **figure 4** compares example control descriptions against related guidance from an IT security context and the related COBIT 5 goals, and proposes a formal assertion that could be used in a CCM context.

DEFINING AUTOMATED TESTS

To continuously assess controls, rules need to be developed to test in real-time (or near-real-time) compliance with the

Figure 3—SAS 106 Financial Statement Assertions

Classification	Assertion
Assertions about classes of transactions and events	Occurrence: Transactions and events that have been recorded have occurred.
	Completeness: All transactions and events that should have been recorded have been recorded.
	Accuracy: Data related to the transactions and events have been recorded appropriately.
	Cut-off: Transactions and events have been recorded in the correct period.
	Classification: Transactions and events have been recorded in proper accounts.
Assertions about account balances (assets)	Existence: The assets exist.
	Rights and obligations: The entity holds or controls the rights to assets.
	Completeness: All assets that should have been recorded have been recorded.
	Valuation and allocation: Assets are included in financial statements.
Assertions about presentation and disclosure	Occurrence, rights and obligations: Disclosed transactions and events have occurred.
	Completeness: All disclosures that should have been included have been included.
	Classification and understanding: Information is appropriately presented and described, and disclosures are clearly expressed.
	Accuracy and valuation: Financial and other information are disclosed fairly and at appropriate amounts.

Source: David Vohradsky. Reprinted with permission.

Figure 4—Proposed Formal Assertions for Selected Controls			
Example Control Description	**ISO 27002 Guidance**	**COBIT 5 Process Goals**	**Proposed Formal Assertions**
All changes to the IT systems (including hardware, networks and software) are managed to minimise the likelihood of disruption, unauthorised alterations and errors.	12.5.1 (e) Obtaining formal approval for detailed proposals before work commences 12.5.1 (f) Ensuring authorized users accept changes prior to implementation 12.5.1 (i) Maintaining an audit trail of all change requests	BAI06: (a) Authorised changes are made in a timely manner and with minimal errors. (b) Impact assessments reveal the effect of the change on all affected components. (c) All emergency changes are reviewed and authorised after the change. (d) Key stakeholders are kept informed of all aspects of the change.	CM1 An authorisation has occurred prior to every change. CM2 Testing has been completed for all changes prior to implementation. CM3 An approval has occurred, indicating completeness of testing conducted. CM4 An authorisation has occurred for every emergency change.
Security measures are in place to prevent, detect and remove malicious software.	10.4.1 Installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control or on a routine basis	DSS05.01 Protect against malware. Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	AV1 AV protection exists on all required assets. AV2 All AV signature updates that should have been made in the period have been made.
Security measures are in place to detect potential data breaches/ data exfiltration transmissions and prevent them by monitoring, detecting and blocking sensitive data.	10.8.1 (a) Procedures designed to protect exchanged information from interception, copying, modification, misrouting and destruction 10.8.1 (g) Use of cryptographic techniques	DSS05: (2) Information processed on, stored on and transmitted by end point devices is protected. (5) Electronic information is properly secured when stored, transmitted or destroyed.	DLP1 Data loss prevention (DLP) protection exists on all required assets. DLP2 End point encryption exists on all required assets. DLP3 DLP protection exists on all network paths. DLP4 DLP alerts have been accurately recorded. DLP5 All DLP alerts that should have been disclosed (and actioned) have been disclosed and actioned.
Source: David Vohradsky. Reprinted with permission.			

previously mentioned formal assertions that are required to be made about the selected controls.[20] The required tests can be classified[21, 22] into seven broad categories based on traditional audit processes or evidence types:

1. **Asset management queries** (where accurate), in place of physical examination of assets
2. **Electronic transaction confirmations**, in place of authenticated transaction documents, including verifying atomic elements of transactions
3. **Electronic statement queries**, in place of internal or external documentation
4. **Re-performance of selected controls**, using some form of automation
5. **Observation** (still a manual periodic test)
6. **Analytical procedures**, such as statistical analysis, comparisons with other internal or external data sets, and pattern-matching within transaction data
7. **Automating collation of responses** to inquiries such as control self-assessment surveys

The types of tests that could be employed in the case study example appear in **figure 5**.

Generally, tests need to answer the question: What would the data look like if the control objective was met or was not met?[23]

Asset management queries and transaction confirmation (type 1 and 2) tests can use existing or improved key risk indicators (KRIs) to provide what is described[24] as a risk indicator continuous assurance (RICA) framework. Past audit report evidence can also be used to identify sources of data and applicable analytics.[25] In this testing approach, a designated threshold being met in two or more consecutive months (or the majority of the time) may indicate a strong control, whereas the threshold not being met in two or more consecutive months may indicate a weak control.[26]

Statement (or tabular data) tests (type 3) can use a belief function approach,[27] in which evidence for and against an assertion is mathematically combined (or aggregated) to determine a result. In this approach, assurance levels are divided into five categories (very low, low, medium, high and very high) based on value ranges. For example, the strength of evidence supporting completeness of testing could be determined by ranges of test coverage or ranges of outstanding defect percentages.

Large data sets or complex behavioural controls may require analytical testing (type 6) to validate an assertion. This analysis may employ a risk score methodology[28] or probability models[29] to create an equal distribution of values 0 to 1 across all samples, with bands reflecting confidence in the assertion. The analysis may be based on:

- Higher or lower than expected values
- Expected or opposite to expected movement
- Small or large changes from one period to the next
- Process metrics
- Erratic behaviour or volatility (variance) in the process

Figure 5—Assertion Test Plan

Proposed Assertion (Refer to figure 4)	**Test Type** (Refer to seven test types noted previously)	**Proposed Pass Condition for Test to Indicate a Strong Control**
CM1. An authorisation has occurred for every change.	(2) Transaction confirmation	Percentage of changes with prior authorisation meeting the threshold for last two consecutive months
CM2. Testing has been completed for all changes prior to implementation.	(3) Statement (test results) query (6) Analytical procedure	High or very high confidence in testing for last two consecutive months, based on number of open defects
CM3. An approval has occurred for completeness of testing conducted.	(2) Transaction confirmation	Percentage of changes with testing approvals meeting threshold for last two consecutive months
CM4. An authorisation has occurred for every emergency change.	(2) Transaction confirmation	Percentage of emergency changes with authorisation meeting threshold for last two consecutive months
AV1. AV protection exists on all required assets.	(1) Asset management query	Percentage of required assets with AV protection meeting threshold for last two consecutive months
AV2. All AV signature updates that should have been made in the period have been made.	(2) Transaction confirmation	Percentage of assets with the latest AV signature meeting threshold for last two consecutive months
DLP1. DLP protection exists on all required assets.	(1) Asset management query	Percentage of required assets with DLP protection meeting threshold for last two consecutive months
DLP2. End point encryption exists on all required assets.	(1) Asset management query	Percentage of required assets with end point encryption meeting threshold for last two consecutive months
DLP3. DLP protection exists on all network paths.	(4) Re-performance (with test data) (7) Vendor control self-assessment	Result of weekly automated control tests to trigger DLP events, passing on two consecutive months (36 per annum)
DLP4. DLP alerts have been accurately recorded.	(4) Re-performance (with test data) (6) Analytical procedure	Result of weekly automated control tests to trigger DLP events, passing on two consecutive months (36 per annum)
DLP5. All DLP alerts that should have been disclosed (and actioned) have been disclosed and actioned.	(6) Analytical procedure	Statistical analysis of DLP alerts and corresponding incident actions to determine volatility of process

Source: David Vohradsky. Reprinted with permission.

Assertions that need to be tested by subjective judgement (type 7, such as those obtained through control self-assessments by service managers or vendors) can be validated[30] through the Delphi Method. In this approach, a more accurate consensus of control effectiveness is obtained through one or more rounds of anonymous self-assessments, which may be reviewed, and feedback provided by experts between rounds.

Planning for the implementation of any of the previously described automated tests needs to take into account likely difficulties such as obtaining data management approvals; data sourcing and aggregation lead times; the need for control domain expertise; technology acquisition and integration costs; and the need for information sharing and coordination among audit, risk and compliance functions.[31]

REPORTING

Figure 6 shows the governance and management processes associated with control assurance. Management monitors processes through mechanisms including KRIs, which are used to alert the business to potential control issues and are part of a continuous improvement cycle.

CCM takes selected KRIs and the results of other tests and analytics on processes and forms part of an overall control assurance program (CAP) in which the concerns over the monitored controls are validated before being prioritised and acted upon alongside issues identified by other periodic manual testing.[32] Additional risk and key control deficiencies may also be identified through management risk and control self-assessments (RCSA) that form part of the program based on management knowledge gained through operating the plan-build-run-monitor cycle. Integrated issue management using a GRC platform facilitates[33] digitisation, automation of alerts and management of remediation activities, once agreed upon by management.

Mature KRIs linked to formal assertions are continuously monitored and reported, automatically form part of the risk and control profile, and are integrated into daily management processes.[34]

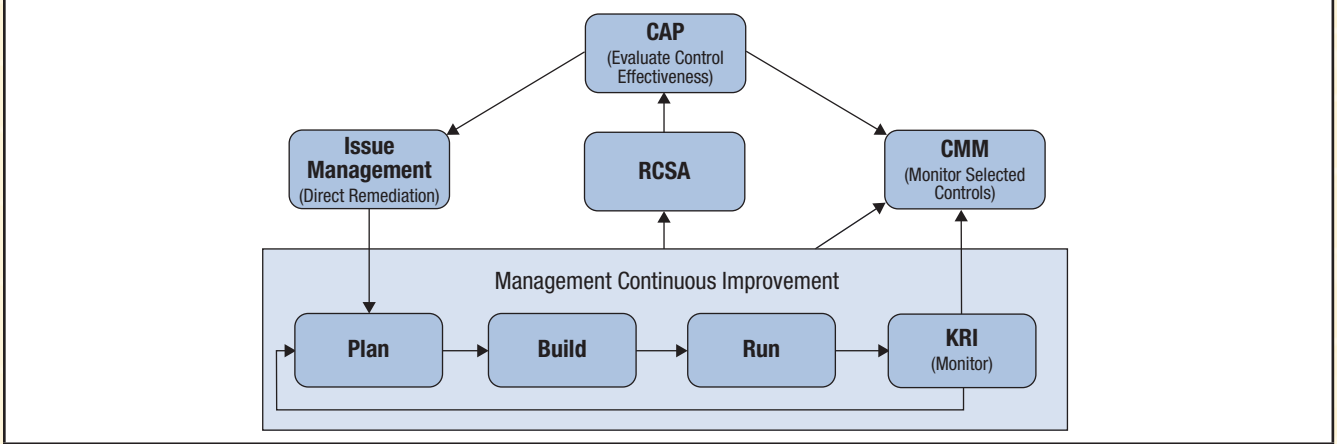
Other KRIs that may be subject to false positives are used in day-to-day management of the process in question and adjusted to a point where they can be relied upon for management self-assessment and continuous improvement of the process.[35] As they mature, they can be incorporated in an expanded CCM regime.

CONCLUSION

This article provides guidance on the identification and prioritisation of controls for CCM implementation and introduces the need to transform COBIT® (and other) management practices into formal assertions (in line with SAS 106) in order to facilitate objective automated testing. It defines the categories of testing available, maps a sample set of assertions to testing types and provides high-level guidance on applicable test rules.

Further work is needed to define formal assertions for the complete set of COBIT 5 management practices as a necessary

Figure 6—Control Assurance Processes



Source: David Vohradsky. Reprinted with permission.

precursor to the wider use of CCM within an IT risk context. This work ideally should occur with further development of *COBIT® 5 for Risk* and other COBIT guidance from ISACA®.

ENDNOTES

[1] Coderre, D., *Global Technology Audit Guide—Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, Institute of Internal Auditors, 2005
[2] Vasarhelyi, M. A.; M. Alles; K. T. Williams; 'Continuous Assurance for the Now Economy', Institute of Chartered Accountants in Australia, 2010
[3] MarFan, K.; IT Audit and Assurance Guideline G42, Continuous Assurance, ISACA, 2010, *www.isaca.org/standards*
[4] Deloitte, *Continuous Monitoring and Continuous Auditing: From Idea to Implementation*, 2010
[5] Gohil, J.; 'Reduce Audit Time Using Automation, by Example', presentation to ISACA Atlanta Chapter, Protiviti, 2013
[6] *Op cit*, Deloitte
[7] *Op cit*, Coderre
[8] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC27002:2006, *Information Technology—Security techniques—Code of practice for information security management*, 2006
[9] *Op cit*, Vasarhelyi 2010
[10] *Op cit*, Standards Australia
[11] *Op cit*, Deloitte
[12] *Op cit*, MarFan
[13] *Op cit*, Vasarhelyi 2010
[14] ISACA, *2009 CISA Review Manual*, USA, 2008
[15] *Op cit*, Vasarhelyi 2010
[16] ISACA, *Relating the COSO Internal Control—Integrated Framework and COBIT*, USA, 2014
[17] American Institute of Certified Public Accountants (AICPA), SAS 106, 'Audit Evidence', February 2006
[18] *Op cit*, ISACA 2014
[19] ISACA, *IT Assurance Guide: Using COBIT*, USA, 2007
[20] *Op cit*, Coderre
[21] Majdalawieh, M.; S. Sahraoui; R. Barkhi; 'Intra/Inter Process Continuous Auditing (IIPCA), Integrating CA Within an Enterprise System Environment', *Business Process Management Journal*, 18 (2), 2012, p. 304-327
[22] Vasarhelyi, M. A.; M. G. Alles; A. Kogan; 'Principles of Analytic Monitoring for Continuous Assurance', *Journal of Emerging Technologies in Accounting*, vol. 1, p. 1-21, 2004
[23] *Op cit*, Coderre
[24] Nigrini, M. J.; A. J. Johnson; 'Using Key Performance Indicators and Risk Measures in Continuous Monitoring', *Journal of Emerging Technologies in Accounting*, vol. 5, 2008, p. 65-80
[25] *Op cit*, Vasarhelyi 2010
[26] *Op cit*, Dale
[27] Mock, T.J.; A. Wright; R. P. Srivastava; 'Audit Program Planning Using a Belief Function Framework', Proceedings of the 1998 Deloitte & Touch University of Kansas Symposium on Auditing Problems, USA, 1998, p. 115-142
[28] *Op cit*, Nigrini
[29] Alles, M. G.; A. Kogan; M. A. Vasarhelyi; 'Putting Continuous Auditing Theory Into Practice: Lessons From Two Pilot Implementations', *Journal of Information Systems*, 22 (2), 2008, p. 195-214
[30] *Op cit*, Vasarhelyi 2010
[31] Vasarhelyi, M. A.; S. Romero; S. Kuenkaikaew; 'Adopting Continuous Auditing/Continuous Monitoring in Internal Audit', *ISACA Journal*, vol. 3 , 2012, p. 1-5
[32] *Op cit*, Coderre
[33] Schermann, M.; M. Wiesche; H. Krcmar; 'The Role of Information Systems in Supporting Exploitative and Exploratory Management Control Activities', *Journal of Management Accounting Research*, vol. 24, 2012, p. 31-59
[34] Dale, J.; E. Chung Yee Wong; 'Achieving Continuous IT Auditing: RICA', *ISACA Journal*, vol. 6, 2009, p. 1-5
[35] *Op cit*, Coderre

Checking the Maturity of Security Policies for Information and Communication

Mauricio Rocha Lyra, Ph.D., COBIT Foundation, CTFL, ISO 20000, ITIL, MCSO, OCUP, PMP, RUP, is a leading professor at Centro Universitário de Brasília and has more than 25 years of experience in the computer science field. He is the author of *Segurança e Auditoria em Sistemas de Informação (Informational Systems Security and Auditing).*

Jose Carlos Ferrer Simoes has more than 10 years of experience working in the Bank of Brasil in the field of information security.

The transformations experienced by organizations due to technological advances has made information, arguably, an enterprise's most valuable asset. As a result, this highly sensitive and vulnerable asset must be protected from potential threats. Organizations are increasingly experiencing risk susceptibility and financial losses due to their information systems and computer networks.

As an example of how to check the level of maturity of security policies for information and communication, this article analyzes the case of a Brazilian government agency. While a Latin American example, this analysis can be applied to any government agency or private entity at the national or international level.

With the importance of information processed in federal public administration departments and entities in mind, the president of Brazil issued Decree, no. 3505, on 13 June 2000,[1] establishing Brazil's National Information Security Policy. The decree mandates that all departments and entities of the federal government have a security policy for information and communication (SPIC). This decree presented the need for protecting information considered sensitive and for general guidelines that should be adopted to prevent and treat vulnerabilities, threats and risk factors that deserve special treatment by all departments and agencies of Brazil's Federal Public Administration.

For this decree to be effective, the federal government has focused its efforts on implementing information security measures in the Federal Public Administration. The implementation consists of applying best practices such as ISO/IEC 27002: 2013,[2] federal legislation such as Decree no. 3505 and the Federal Public Administration's Information Security Policy and Regulatory Instruction no. 01,[3] established by the presidency's Institutional Security Office.

Decree no. 3505's publication established and ruled that all areas of the federal government should establish an SPIC. This Decree is aimed at ensuring the SPIC maturity level in all Federal Public Administration entities.

To achieve this goal, the best practices for creating an SPIC were mapped for organizations using the ISO/IEC 27000 family of international standards. Next, 10 federal government departments in various areas were identified in order to complete a comparative analysis of these best practices. Finally, a critical and comparative analysis, introducing an SPIC maturity-level matrix within those chosen organizations was performed, as well as an analysis of SPIC regarding each area of expertise.

ANALYSIS OF SPIC

The objective of the SPIC comparative analysis was to compare 12 standard requirements for their usefulness for an SPIC. The analyses were to be performed according to ISO 27002:2013, among the 40 federal government entities (the presidency and 39 ministries) of Brazil. **Figure 1** presents the requirements met by each department studied.

ATTRIBUTES REQUIREMENT ANALYSIS

To better understand the aspects dealt with in an SPIC, the 12 essential requirements were classified, according to the best practices in three major groups by their similar attributes, which were designated as regulation, prevention/control and responsibility/penalty. Among the 12 requirements, four requirements were identified with attributes of regulation, five attributes with requirements of prevention/control and three requirements with attributes of responsibility/penalty, as shown in **figure 2**.

In **figure 2**, the percentage of the requirements are also presented and mapped to the creation

Figure 1—Consolidated SPIC Requirements Analyzed

	Requirements for SPIC According to ISO 27002:2013	SPIC—Ministry of Defense	SPIC—Ministry of Justice	SPIC—Ministry of Health	SPIC—Ministry of Science, Technology and Innovation	SPIC—Ministry of Planning, Budget and Management	SPIC—Ministry of Culture	SPIC—Ministry of Tourism	SPIC—Ministry of Labor and Employment	SPIC—Ministry of Education	SPIC—Ministry of Agriculture, Livestock and Supply
1.	Does it contain regulations, laws and contracts that must be SPIC-supported?	Yes	No	No	Yes	Yes	No	Yes	No	Yes	No
2.	Does it contain a framework for setting control objectives and controls, structure analysis, evaluation and control management, and assessment and risk management?	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No
3.	Do scope, concepts, definitions and a description of information security importance exist?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.	Are principles of information security and communications policy declared?	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No
5.	Are there objectives and principles to guide all activities related to information security?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.	Is there attribution of responsibilities, general and specific to information security management, for defined roles?	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes
7.	Is there a provision for the management process of business continuity (business continuity management)?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8.	In case of violation of the SPIC, are the consequences (penalties) stated in this document?	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
9.	Are there specific policies that require the implementation of security controls and that are structured to consider the needs of certain interest groups within the organization or to cover specific topics (e.g., access control, classification, processing of information)?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10.	Are the policies of information and communication security communicated to employees and relevant external parties so that they are understood, relevant and accessible to users (i.e., in the context of a program of awareness, education and training in information security)?	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes
11.	Are the security policies of information and communication critically analyzed at planned intervals?	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No
12.	Is there a statement of commitment directly supporting the goals and principles of the organization?	No	No	No	No	No	No	Yes	No	No	No

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

of an SPIC per ISO 27002:2013, as observed by the Federal Public Administration, among the departments that were analyzed. Further, the average percentage of the requirements was verified for each attribute properly classified, and for this percentage, the arithmetic mean was used for the requirements classified into each of the attributes.

Figure 2 makes it clear that there were attributes with greater or lesser levels of maturity. However, although none of

Figure 2—Attributes Requirements Analysis

Attributes of the Requirements	Requirements Checked by Attribute	Percent of Requirements Attended by the Department Analyzed	Average Percent of the Requirements Checked by Attribute
Regulation	1. Does it contain regulations, laws and contracts that must be SPIC-supported?	50%	77.5%
	3. Do scope, concepts, definitions and a description of information security importance exist?	100%	
	4. Are principles of information security and communications policy declared?	60%	
	5. Are there objectives and principles to guide all activities related to information security?	100%	
Prevention and/or Control	2. Does it contain a framework for setting control objectives and controls, structure analysis, evaluation and control management, and assessment and risk management?	60%	82.0%
	7. Is there a provision for the management process of business continuity in an SPIC (business continuity management)?	100%	
	9. Are there specific policies that require the implementation of security controls and that are structured to consider the needs of certain interest groups within the organization or to cover specific topics (i.e., access control, classification, processing of information?)	100%	
	10. Are the policies of information and communication security communicated to employees and relevant external parties so that they are understood, relevant and accessible to users (i.e., in the context of a program of awareness, education and training in information security)?	70%	
	11. Are the security policies of information and communication critically analyzed at planned intervals?	80%	
Responsibility and Penalty	6. Is there attribution of responsibilities, general and specific to information security management, for defined roles?	70%	56.7%
	8. In case of violation of the SPIC, are the consequences (penalties) stated in this document?	90%	
	12. Is there a statement of commitment directly supporting the goals and principles of the organization?	10%	

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

the three attributes had full classified prediction, it should be emphasized that the prevention and/or control attribute has a greater predictability in an SPIC, and of the five requirements that comprised this attribute, two requirements (numbers 7 and 9) were provided in all SPICs analyzed. Requirement number 11, despite being absent in two SPICs, was performed in all 10 departments that had recently updated their policies. In practice, the requirement has been observed; however, there is no formal prediction to support best practices. Thus, it is necessary that requirements 2 and 10 should be revalued so that those attributes are handled as soon as best practices are established.

The control attribute, which had the second best predictor in the SPICs, is composed of four requirements, and two of these requirements (3 and 5) are fully provided in all SPICs analyzed in this work. Requirements 4 and 5 are provided in only five and six departments, respectively, which shows the need for the Federal Public Administration to act in partnership so that there is greater interaction when drafting or reviewing a department's SPIC. These two requirements are simple requirements and are generally already included in an SPIC because the entities already directly or indirectly respect the precepts of information security and legislation in which these requirements are supported.

The responsibility/penalty attribute was identified with less predictability in the SPICs—possibly because it is an area that involves issues related to IT and is often an area of little knowledge by managers. This is verified by the point that only one of the 10 departments analyzed shows the requirement of "12" that had the lowest prediction in SPIC analyzed. For greater support of activities and responsibilities related to information security, and to improve the IT governance of public entities, the use of organizational structures is suggested (i.e., the creation of a committee connected directly to top management [strategic IT committee] to support the IT strategy development, in addition to monitoring the achievement of strategic IT goals, using, among other instruments, periodic reports on actions related to IT, generated to give greater technical protection to the top management who will be able to act with higher effectiveness). Thus, top management is engaged in guided predictability of the 12 SPIC requirements while also managing the periodic update of this policy.

SPIC MATURITY-LEVEL MATRIX

In **figure 3**, the amount and the percentage of checked requirements in an SPIC, per ISO 27002:2013, are presented for each department analyzed in this work.

Figure 3—Amount of Requirements Met in the Analyzed Departments

Ministry	Number of Checked Requirements	Percent of Conditions Verified in Departments
Tourism	12	100%
Science, Technology and Innovation	11	91.67%
Planning, Budget and Management	11	91.67%
Defense	11	91.67%
Justice	9	75%
Culture	8	66.67%
Labor and Employment	7	58.33%
Education	7	58.33%
Agriculture, Livestock and Supply	7	58.33%
Health	6	50%

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

Figure 3 verifies the amount of attributes checked in the ministries. Then, by performing calculations, the arithmetic mean (8.90) of SPIC conditions is verified and the standard deviation (2.07) of these requirements can be observed. Hence, a maturity matrix of the analyzed departments was applied, as shown in **figure 4**, where the ranges of the quantity of verified SPIC conditions are presented and their respective maturity is analyzed.

Figure 4—SPIC Maturity Matrix

Average Number of Requirements Verified in SPIC	Degree of Maturity	Number of Analyzed Departments Attending This Range of Requirements
Above 10.97	High	4
Between 8.9 and 10.97	Good	2
Between 6.83 and 8.90	Reasonable	3
Less than 6.83	Undesirable	1

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

STRATEGIC, FUNDAMENTAL AND SPECIAL AREA

For better analysis, the 10 departments observed in this study were classified into three groups (strategic, fundamental and special) and by area of expertise (**figure 5**).

Figure 5—Amount of Requirements Attended Per Area of Operation

Area	Ministry	Number of Checked Requirements in Each Department
Strategic	Planning, Budget and Management	11
	Science, Technology and Innovation	11
	Defense	11
	Justice	9
Fundamental	Health	6
	Education	7
	Labor and Employment	7
	Agriculture, Livestock and Supply	7
Special	Tourism	12
	Culture	8

Source: Jose Carlos Ferrer Simoes and Mauricio Rocha Lyra. Reprinted with permission.

The areas that determine the guidelines and planning of the state were classified as strategic. Departments engaged in services essential to survival and social well-being were classified as fundamental. The areas not related to strategic and key themes were classified as special.

The four ministries classified in this work as strategic showed an SPIC with a level of maturity above average in comparison with other analyzed departments. This study indicates that the departments classified as strategic use a standard based on best practices for building and updating their SPICs. Finally, it can be said that strategic areas' SPICs have a good homogeneity and are consistent with their degree of expertise, presenting documents with nearly all essential requirements for compliance with the policy.

The four departments classified as fundamental areas showed a degree of maturity, as shown in **figure 5**, ranging from reasonable to undesirable. This homogeneity and lower SPIC maturity level are probably due to a lack of benchmarking. Apparently, these departments developed their SPIC without much critical analysis of their current affairs, but instead by simply using a previous SPIC model, generating policies with the absence of several essential requirements of information security. As for the departments that had their SPIC classified as special, a heterogeneity was observed in their SPIC, ranging from reasonable to high maturity.

FINAL REPORT ANALYSIS

In the study, it is inferred through the analysis of several decrees and laws that the federal government is directing its efforts to implement information security standards to be followed by departments in order to consistently conduct business with best practices and in compliance with specific legislation. However, based on data collected from the government areas studied, one can verify that an SPIC is applied in direct Federal Public Administration departments at a very diverse level of maturity.

> "A well-implemented SPIC can mitigate or even determine responsibility for undesired actions in an organization."

Regarding the compliance with essential requirements in an SPIC, it was found that only one of the departments studied met all 12 requirements, which shows a deficiency and a risk to public administration in general, especially because a well-implemented SPIC can mitigate or even determine responsibility for undesired actions in an organization.

Another aspect addressed in this study was the analysis of the essential requirements in an SPIC based on attributes in which it was identified that the departments analyzed had greater predictability when the attribute related to prevention and/or control. This fact is due to the culture of the Federal Public Administration, which is directly supervised by control entities of the federal government.

When the analysis from the perspective of the Federal Public Administration expertise area was conducted, it was found that the departments classified as strategic, as well as the ones classified as critical, showed a similarity to the requirements in their SPIC for area performance, which can be interpreted as these entities making an effort to meet best practices with respect to information security, although there is no study or a more critical analysis of this tendency addressed in their policies' requirements.

For an SPIC in the Federal Public Administration to reach a high level of maturity, it is necessary to create a temporary, multidisciplinary safety committee, which should have a central management with the responsibility of analyzing, evaluating, criticizing and reviewing SPICs before these policies are published. It is worth noting that the decision to accept this committee's recommendations would be the responsibility of each department's management. However, surely the department, while receiving feedback from a specialist in the subject area, would be inclined to at least predict, even in a partial way, those recommendations in its SPIC.

Finally, although this work has been conducted in 10 departments, it is not possible to assess or infer the maturity level of the 30 departments that were not analyzed. Another fact that needs to be emphasized is that this study considered only the quantitative value of the requirements, which do not evaluate the merits of qualitative requirements. Based on these facts, it is understood that for an accurate assessment of how the SPIC is applied in public administration, a larger study addressing not only every department, but a detailed analysis of the qualitative value of these essential requirements is necessary.

This study aimed to verify the applicability of the SPIC in organizations and to analyze the maturity of this document on the best information security practices. To facilitate the analysis,

the study was made based on the SPIC of Brazilian public organizations. However, this methodology can be used in any company in the public or private sectors. This study can be extended beyond merely analyzing the predictability in SPIC—to also evaluating the merits of these attributes.

ENDNOTES

[1] Decree, no. 3505, 13 June 2000 established the Information Security Policy in the organizations and entities of the Brazilian Federal Public Administration.

[2] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27002:2013, *Information technology—Security techniques—Code of practice for information security management*, 2013

[3] Federal Public Administration's Information Security Policy and Regulatory Instruction no. 01. This document presents directives for the preparation of an SPIC in organizations and entities of the Brazilian Federal Public Administration.

HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com or
publication@isaca.org

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Ganapathi Subramaniam heads the information security function at Flipkart *(www.flipkart.com)*, India's leading e-commerce marketplace. An accomplished professional with 24 years of industry experience, Subramaniam's passion and profession has always been information security. Until recently, he was employed at Microsoft Corporation India as its chief security officer, performing the role of a security evangelist within its sales and marketing support group. He's previously worked at Accenture and big 4 firms such as Ernst & Young and PricewaterhouseCoopers. As a conference speaker and columnist, he has addressed numerous gatherings of chief information officers and chief information security officers risk worldwide.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

Q My company has outsourced call center operations. Both inbound and outbound call services are provided by the outsourced vendor. My team is planning to conduct an audit of the security controls with respect to the outsourced call center operations.

What are the key controls that we must consider for assessing the third-party vendor?

A Using a framework such as COBIT® or a standard such as ISO 27001:2013 is a good option. Using one or a combination of these, you may choose the relevant controls. Because business continuity is a key component of any outsourced arrangement, it can be audited using international standards that are available.

Given that the call center staff may have access to a lot of sensitive data or personally identifiable information (PII), one of the big risk factors is potential data spillage.

The following is an indicative list of controls that require assessment (This list assumes that the contract with the vendor provides for an independent audit as a matter of right and not as an optional obligation. If the contract does not provide for an independent audit, recommend an amendment to the contract for inclusion of a right-to-audit clause.):

- The contract must provide for a liability clause in which the vendor agrees to compansate the company for any losses generated due to any data breach.
- Depending in which country/continent the company operates, there may be local legal and regulatory requirements that forbid transfer of data outside of the country. In some countries, such transfer may be permitted if certain conditions are met. Obtain a clear understanding of the local laws/regulations and assess whether the outsourced arrangements meet such tenets. Additional controls may require assessments if such data are to reside in a public cloud.
- Access to data, in particular to sensitive data, must be restricted and must be provided on a need-to-know basis as dictated by the business need. A data classification policy will help determine how to bucket the data into groups so that a granular level of access can be provided. An access control policy must exist to govern data access.
- The outsourced vendor must complete background checks of all new employees and contractors prior to gaining access to live data. This is one of the weakest links and must be made strong. If the agents were to deal with any credit-card-related information, they must not locally store such information for potential abuse later.
- USB ports must be disabled for use with removable storage media. For example, in some of the major business process outsourcers [BPOs] in India, no one, including visitors, employees and contractors, is permitted to bring any memory sticks onsite. An Internet access policy must be reasonably restrictive. There is no point in governing Internet access internally while allowing unrestricted access at the third-party vendor end.
- Desktops/laptops must follow certain baseline security standards. Such baseline standards must include a number of controls such as local administrator disablement. Granting of local administrator rights to all users will enable anyone to install any software, which, in some cases, may be inappropriate. Thus, such unwarranted rights must be curtailed.
- The network and applications must be regularly tested for vulnerabilities; there must be a patch management regime to ensure that the right patches are applied at the right time to plug the holes. Any third-party, vendor-supplied applications must also be patched appropriately.
- All connectivity must be clearly documented. Such documentation must be current.
- Disaster recovery arrangements and properly tested, well-documented continuity plans are

also a must. The absence of such tested plans implies a lack of adequate recovery arrangements in the event of a disaster. The crisis management group must be comprised of individuals representing both organizations—the outsourcer and the outsourced—with roles and responsibilities clearly defined.

- In the event of any security breach, a well-defined incident management framework must help handle it. A clear communication process must exist with proper escalation mechanisms. A root-cause analysis (RCA) is a must for all incidents in order to prevent recurrence.
- There must be regular, periodic internal assessment of controls. While an auditor cannot place complete reliance on such work, internal assessment will definitely contribute to identification of key issues.

Additionally, please refer to the *ISACA Journal* volume 1, 2015, HelpSource Q&A on privacy audit. Most of the privacy control requirements included there will also apply.

Enjoying this article?

- Read *Outsourced IT Environments Audit/Assurance Program*.

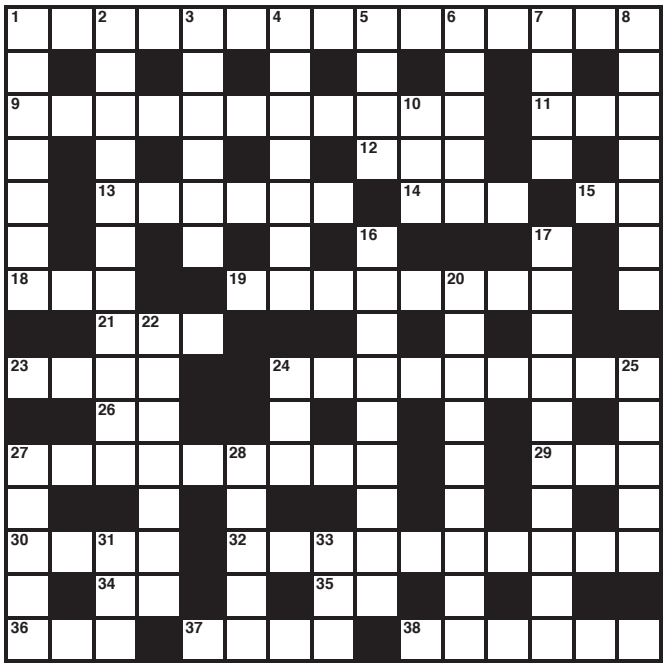
  www.isaca.org/outsourced-IT-AP

- Discuss and collaborate on governance of enterprise IT in the Knowledge Center.

  www.isaca.org/topic-governance-of-enterprise-it

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1 Actions taken to protect against threats
9 This type of information, when stolen, has the most damaging economic effects
11 Anomalous
12 Finish, with "up"
13 Cyberrobberies, e.g.
14 Speculate
15 MAC rival
18 E-mail address ending
19 *The New York Times* writer who coined the phrase 'makers' and 'breakers' of the Internet"
21 Supersonic plane, for short
23 COBIT 5 is frequently the framework of choice for this type of governance technology, abbr.
24 Using human characteristics (in identity verification)
26 Deja ___
27 General who is the commander of the US Cyber Command
29 Quid __ quo
30 ___ stamp
32 Withheld from general circulation
34 Overtime, briefly
35 What a CIO runs
36 Call upon, for a job or project
37 Go off protocol, in terms of the rules
38 Forerunner of the web

DOWN

1 Input of data, not as a direct result of data entry
2 Not easily seen
3 Recent corporate victim of credit card thefts
4 Get back into the web site
5 Inspection
6 Internet phone company owned by Microsoft
7 ____kit
8 Lured away from moral principles
10 Steal
16 Architecture approach first recommended by Forrester Research (2 words)
17 One of the best methods to counter credit card hacks
20 Memory developing technique
22 2010 computer worm
24 Compete for a project
25 Server-based data storage
27 Inspect, verify and make recommendations
28 Special place in the market
31 Exceed
33 Assist

(Answers on page 58)

CPE Quiz

Prepared by Smita Totade, Ph.D., CISA, CISM, CGEIT, CRISC

Take the quiz online:

QUIZ #159

Based on Volume 6, 2014—Cybersecurity

Value—1 hour of CISA/CISM/CGEIT/CRISC continuing professional education (CPE) credit

TRUE OR FALSE

BECK ARTICLE

1. Effective contingency planning for cyberattacks replace Cyber DRaaS infrastructure investment by delivering computer event response team (CERT)-compliant organizational readiness.

2. The NGF offers stronger access-control capabilities than the current generation of port-based firewalls because authorization occurs at the application and user levels while simultaneously blocking all port-level access.

3. Cyber DRaaS reflects a future theoretical architecture for cyberrecovery and not one that can be implemented today with existing technology and proper planning.

4. Zero trust places a high-performance NGF cluster at the boundary of the network to act as a data traffic distribution hub, segmenting the network into isolated work groups.

MATTSSON ARTICLE

5. Format-preserving encryption preserves the ability of users and applications to read the protected data and is one of the fastest performing encryption processes.

6. SDM is utilized in test/development environments in which data that look and act like real data are needed for testing, but sensitive data are not exposed to developers or systems administrators.

7. DDM provides security to data at rest or in transit and from privileged users.

8. Tokenization allows for no flexibility in the levels of data security privileges, as authority cannot be granted on a field-by-field or partial-field basis.

9. While vaultless tokenization offers unparalleled access and security for structured data, encryption may be employed for unstructured, nonanalytical data.

GELBSTEIN AND POLIC ARTICLE

10. The data custodian is accountable for ensuring data disposal is carried out according to good practices.

11. For critical applications and data, it may be appropriate to consider having the right to audit the CSP and/or engage ethical hackers to conduct an assessment of their security arrangements.

12. When using cryptography, the security of the system should be ensured by the secrecy of the algorithm and not by the secret key.

ANDERSON ARTICLE

13. One defining symptom of the first stage of an information security program's maturity is the silver bullet syndrome, in which the answer to all problems is the acquisition of technology.

14. The Maturity Path approach offers a way to gauge maturity progress and takes into consideration people, process and technology, while also providing precision and exact stages in assessing the maturity of the information security program.

15. Nolan's Model provides a quantitative measure of maturity.

16. Every information security team needs to achieve the highest maturation stage irrespective of the level of maturity to support the needs of the organization it serves.

17. A compliance culture is the reward at the end of the integration phase of the information security program.

18. The appropriate destination stage for an information security program's maturity is dependent on the organization, its threat landscape, risk tolerance and business segment.

ISACA Journal
CPE Quiz
Based on Volume 6, 2014—Cybersecurity

Quiz #159 Answer Form

(Please print or type)

Name _____

_____

Address_____

_____

_____

CISA, CISM, CGEIT or CRISC #_____

Quiz #159

True or False

BECK ARTICLE

1._____

2._____

3._____

4._____

MATTSSON ARTICLE

5._____

6._____

7._____

8._____

9._____

GELBSTEIN AND POLIC ARTICLE

10._____

11._____

12._____

ANDERSON ARTICLE

13._____

14._____

15._____

16._____

17._____

18._____

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.

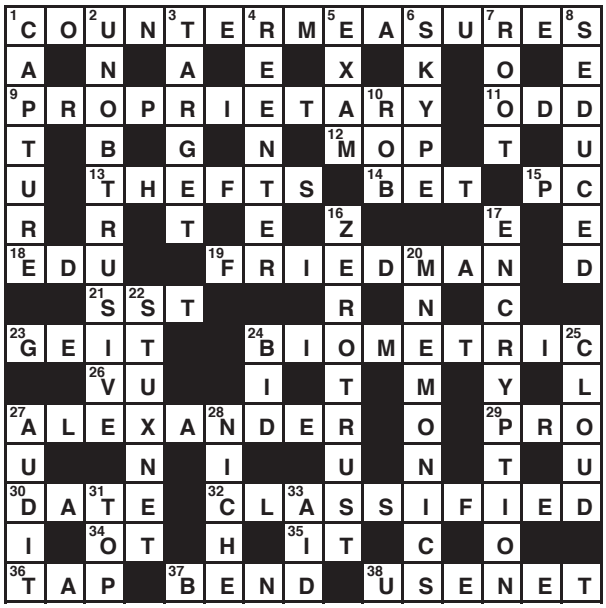
Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

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 56 for the puzzle.



ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

The specialised nature of information systems (IS) audit and assurance and the skills necessary to perform such engagements require standards that apply specifically to IS audit and assurance. The development and dissemination of the IS audit and assurance standards are a cornerstone of the ISACA® professional contribution to the audit community.

IS audit and assurance standards define mandatory requirements for IS auditing. They report and inform:

- IS 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 committee and, ultimately, in disciplinary action.

ITAF™, 3rd Edition (www.isaca.org/itaf) provides a framework for multiple levels of guidance:

- **IS Audit and Assurance Standards**
  - The standards are divided into three categories:
  - General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
  - Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care
  - Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated
- **IS Audit and Assurance**
  The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorisation as the standards (also divided into three categories):
  - General guidelines (2000 series)
  - Performance guidelines (2200 series)
  - Reporting guidelines (2400 series)
- **IS Audit and Assurance Tools and Techniques**
  - These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programmes, reference books, and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf*

An online glossary of terms used in ITAF is provided at *www.isaca.org/glossary*.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IS environment.

IS Audit and Assurance Standards

The titles of issued standards documents are listed as follows:

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

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

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

Please note that the new guidelines are effective 1 September 2014.

General
2001 Audit Charter
2002 Organisational Independence
2003 Professional Independence
2004 Reasonable Expectation
2005 Due Professional Care
2006 Proficiency
2007 Assertions
2008 Criteria

Performance
2201 Engagement Planning
2202 Risk Assessment in Planning
2203 Performance and Supervision
2204 Materiality
2205 Evidence
2206 Using the Work of other Experts
2207 Irregularity and Illegal Acts
2208 Sampling

Reporting
2401 Reporting
2402 Follow-up Activities

The ISACA Professional Standards and Career Management Committee (PSCMC) is dedicated to ensuring wide consultation in the preparation of ITAF standards and guidelines. Prior to issuing any document, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director of Professional Standards Development via email (*standards@isaca.org*); fax (+1.847. 253.1443) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at *www.isaca.org/standards.*

Advertisers/Web Sites

Leaders and Supporters

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

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

ISSN 1944-1967

ISACA®
Trust in, and value from, information systems

BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

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

NEW PRODUCTS

IT Control Objectives for Sarbanes-Oxley: Using COBIT® 5 in the Design and Implementation of Internal Controls Over Financial Reporting, 3rd Edition*

Available in print – **PSOX3** and eBook – **WPSOX3**
Member: $35.00 Nonmember: $60.00

Risk Scenarios: Using COBIT 5 for Risk*

Available in print – **CB5RS** and eBook – **WCB5RS**
Member: $35.00 Nonmember: $60.00

CISM Review Questions, Answers & Explanations Database – 12 month Subscription*

Available on the web – **XMXCM15-12M**
Member: $185.00 Nonmember: $225.00

Blindsided: A Manager's Guide to Crisis Leadership

Available in print – **9RO**
Member: $30.00 Nonmember: $40.00

CISA Review Manual 2015*

Available in print – **CRM15**
Member: $105.00 Nonmember: $135.00

FEATURED PRODUCTS

Insights and Resources for the Cybersecurity Professional from the ISACA Bookstore. Find the latest research and expert thinking on standards, best practices, emerging trends and beyond at ***www.isaca.org/bookstore***

CSX Cybersecurity Fundamentals Study Guide*

Available in print – **CSXG1**
Member: $25.00 Nonmember: $35.00
eBook – **WCXG1**
Member: $35.00 Nonmember: $45.00

Implementing the NIST Cybersecurity Framework*

Available in print – **CSNIST** and eBook – **WCSNIST**
Member: $35.00 Nonmember: $60.00

Advanced Persistent Threats: How to Manage the Risk to your Business*

Available in print – **APT** and eBook – **WAPT**
Member: $35.00 Nonmember: $60.00

Transforming Cybersecurity*

Available in print – **CB5TC** and eBook – **WCB5TC**
Member: $35.00 Nonmember: $60.00

Responding to Targeted Cyberattacks*

Available in print – **RTC** and eBook – **WRTC**
Member: $35.00 Nonmember: $59.00

Securing Mobile Devices*

Available in print – **CB5SMD** and eBook – **WCB5SMD**
Member: $35.00 Nonmember: $75.00

* Published by ISACA

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

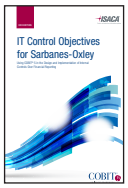
All prices are listed in US Dollars and are subject to change

We are constantly expanding. Check out our new books and eBooks!

New/Featured Products

NEW PRODUCTS

IT Control Objectives for Sarbanes-Oxley: Using COBIT 5 in the Design and Implementation of Internal Controls Over Financial Reporting, 3rd Edition*



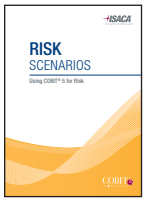
by ISACA

This publication provides CIOs, IT managers, and control and assurance professionals with scoping and assessment ideas, approaches and guidance in support of the IT-related Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control objectives for financial reporting. Enhancements include:

- The requirements of the PCAOB's Auditing Standard No. 5 (AS 5)
- Mappings of the role of the COSO framework and its relationship to COBIT 5
- Detailed examples of application controls
- Issues in using SSAE 16 SOC 1 Examination reports
- IT Sarbanes-Oxley compliance road map

Available in print – **PSOX3**
Member: $35.00 Nonmember: $60.00
eBook – **WPSOX3**
Member: Free Nonmember: $60.00

Risk Scenarios: Using COBIT 5 for Risk*

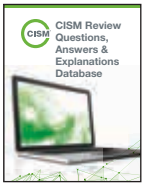


by ISACA

Risk Scenarios: Using COBIT 5 for Risk provides practical guidance on how to use *COBIT 5 for Risk* to solve for current business issues. The publication provides a high level overview of risk concepts, along with over 50 complete risk scenarios covering all 20 categories described in *COBIT 5 for Risk*. An accompanying toolkit contains interactive risk scenario templates for each of the 20 categories.

Available in print – **CB5RS**
Member: $35.00 Nonmember: $60.00
eBook – **WCB5RS**
Member: Free Nonmember: $60.00

CISM Review Questions, Answers & Explanations Database – 12 month Subscription*

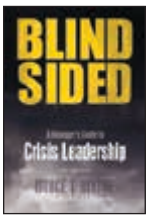


by ISACA

A comprehensive 1015-question pool of items that combine the questions from the *CISM Review Questions, Answers & Explanations Manual 2014* with those from the *2014* and *2015* editions of the *CISM Review Questions, Answers & Explanations Manual Supplement*. The database is available via the web, allowing our CISM Candidates to log in at home, at work or anywhere they have Internet connectivity.

Available on the web – **XMXCM15-12M**
Member: $185.00 Nonmember: $225.00

Blindsided: A Manager's Guide to Crisis Leadership



by Bruce T. Blythe

Blythe's book is different… a step-by-step guide to process excellence… a veritable encyclopedia of crisis leadership, rich in strategic insights, invaluable for any leader."—*Dr. Daniel Diermeier, Kellogg School of Management, Northwestern University*

Blythe lands you in the middle of a fast-breaking crisis and uses case studies and examples to demonstrate what a top-notch leader would say and do at every turn. He then uses his 30 years of global experience to show you how to develop and write a highly practical crisis management plan. His is uniquely two books in one—Crisis Response and Crisis Preparedness interwoven with lessons in Crisis Leadership.

Available in print – **9RO**
Member: $30.00 Nonmember: $40.00

New/Featured Products

CISA Review Manual 2015*

by ISACA

CISA Review Manual 2015 is a comprehensive reference guide designed to help individuals prepare for the CISA exam and understand the roles and responsibilities of an information systems (IS) auditor. The manual has been enhanced over the past editions and represents the most current, comprehensive, peer-reviewed IS audit, assurance, security and control resource available worldwide. The 2015 manual is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Support
- Protection of Information Assets

Available in print – **CRM15**
Member: $105.00 Nonmember: $135.00

FEATURED PRODUCTS

CSX Cybersecurity Fundamentals Study Guide*

by ISACA

The *Cybersecurity Fundamentals Study Guide* is a comprehensive study aid that will help to prepare learners for the Cybersecurity Fundamentals Certificate exam. By passing the exam and agreeing to adhere to ISACA's Code of Ethics, candidates will earn the Cybersecurity Fundamentals Certificate, a knowledge-based certificate that was developed to address the growing demand for skilled cybersecurity professionals. The *Cybersecurity Fundamentals Study Guide* covers key areas that will be tested on the exam, including: cybersecurity concepts, security architecture principles, incident response, security of networks, systems, applications, and data, and security implications of evolving technology.

Available in print – **CSXG1**
Member: $45.00 Nonmember: $55.00
eBook – **WCXG1**
Member: $45.00 Nonmember: $55.00

Implementing the NIST Cybersecurity Framework*

by ISACA

In 2013, US President Obama issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, which called for the development of a voluntary risk-based cybersecurity framework (CSF) that is "prioritized, flexible, repeatable, performance-based, and cost-effective." The CSF was developed through an international partnership of small and large organizations, including owners and operators of the nation's critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST). ISACA participated in the CSF's development and helped embed key principles from the COBIT framework into the industry-led effort. As part of the knowledge, tools and guidance provided by CSX, ISACA has developed this guide for implementing the NIST *Framework for Improving Critical Infrastructure Cybersecurity.*

Available in print – **CSNIST**
Member: $35.00 Nonmember: $60.00
eBook – **WCSNIST**
Member: Free Nonmember: $60.00

Advanced Persistent Threats: How to Manage the Risk to Your Business*

by ISACA

This book explains the nature of the security phenomenon known as the advanced persistent threat (APT). It also provides helpful advice on how to assess the risk of an APT to the organization and recommends practical measures that can be taken to prevent, detect and respond to such an attack. In addition, it highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk.

Available in print – **APT**
Member: $35.00 Nonmember: $60.00
eBook – **WAPT**
Member: Free Nonmember: $60.00

New/Featured Products

FEATURED PRODUCTS *(cont.)*

Transforming Cybersecurity*

by ISACA

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace?

The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability.

This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity.

Available in print – **CB5TC1**
Member: $35.00 Nonmember: $60.00
eBook – **WCB5TC1**
Member: Free Nonmember: $60.00

Responding to Targeted Cyberattacks*

by ISACA

A Breach WILL Eventually Occur! Is your enterprise prepared?

The threat environment had radically changed over the last decade. Most enterprises have not kept pace and lack the necessary fundamentals required to prepare and plan against cyberattacks. To successfully expel attackers, the enterprise must be able to:

- Conduct an investigation
- Feed threat intelligence into a detailed remediation/eradication plan
- Execute the remediation/eradication plan

Available in print – **RTC**
Member: $35.00 Nonmember: $59.00
eBook – **WRTC**
Member: $Free Nonmember: $59.00

Securing Mobile Devices*

by ISACA

Securing Mobile Devices should be read in the context of the existing publications *COBIT 5 Information Security, Business Model for Information Security* (BMIS) and COBIT 5 itself.

This publication is intended for several audiences who use mobile devises directly or indirectly. These include end users, IT administrators, information security managers, service providers for mobile devices and IT auditors.

The main purpose of applying COBIT 5 to mobile device security is to establish a uniform management framework and to give guidance on planning, implementing and maintaining comprehensive security for mobile devices in the context of enterprises. The secondary purpose is to provide guidance on how to embed security for mobile devices in a corporate governance, risk management and compliance (GRC) strategy using COBIT 5 as the overarching framework for GRC. 2012, 100 pages

Available in print – **CB5SMD1**
Member: $35.00 Nonmember: $75.00
eBook – **WCB5SMD1**
Member: Free Nonmember: $75.00

* Published by ISACA
ISACA member complimentary download *www.isaca.org/downloads* All prices are listed in US Dollars and are subject to change

LEVERAGE MORE RELEVANT, TIMELY INFORMATION.

Stay on the Cutting-Edge of What's New in Today's Modern Business World.

Online-exclusive *ISACA® Journal* Articles Now Featured Biweekly

Between the online-exclusive articles and the author blog, the *ISACA® Journal* will now be providing new online content weekly!

NEW! *Journal* podcasts are now available!

ISACA®
Trust in, and value from, information systems

www.isaca.org/Journal-Jv2

Same great content, fresh new looks!

Take a glimpse online at ISACA's revamped digital periodicals *@ISACA* and *COBIT® Focus*, and watch for the newly updated ISACA Journal Author Blog—coming soon!

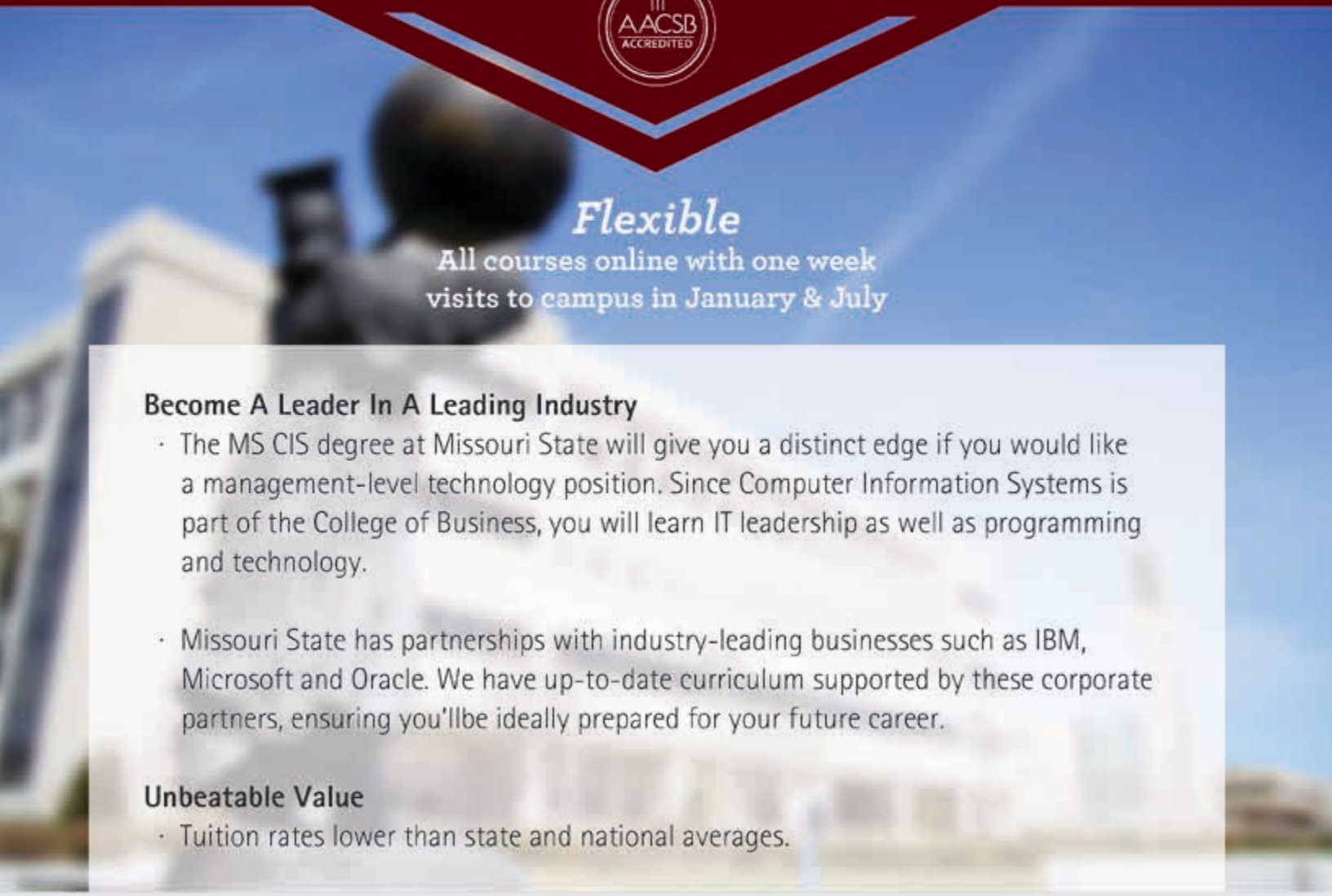
FOLLOW YOUR PASSION. FIND YOUR PLACE.

WITH A MS CIS DEGREE FROM MISSOURI STATE

68%

of MSU MS CIS students earned a promotion after graduation

AACSB ACCREDITED



Flexible

All courses online with one week visits to campus in January & July

Become A Leader In A Leading Industry

- The MS CIS degree at Missouri State will give you a distinct edge if you would like a management-level technology position. Since Computer Information Systems is part of the College of Business, you will learn IT leadership as well as programming and technology.

- Missouri State has partnerships with industry-leading businesses such as IBM, Microsoft and Oracle. We have up-to-date curriculum supported by these corporate partners, ensuring you'llbe ideally prepared for your future career.

Unbeatable Value

- Tuition rates lower than state and national averages.

Missouri State.

MASTER OF SCIENCE
COMPUTER INFORMATION SYSTEMS

mscis.missouristate.edu

@MSCISatMSU

EO/AA/M/F/VETERANS/DISABILITY