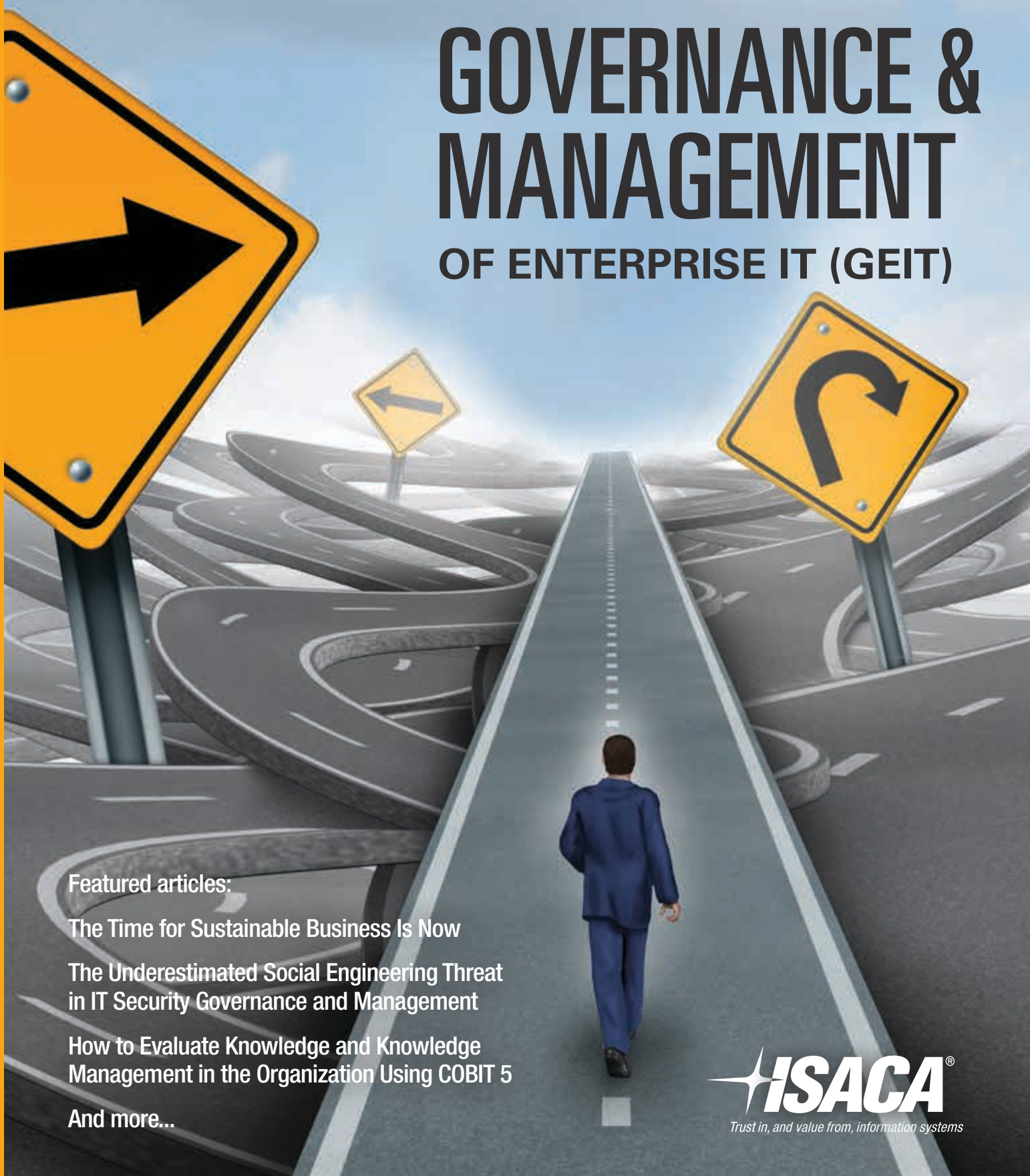
Volume 3, 2015

ISACA® Journal

GOVERNANCE & MANAGEMENT OF ENTERPRISE IT (GEIT)



Featured articles:

The Time for Sustainable Business Is Now

The Underestimated Social Engineering Threat in IT Security Governance and Management

How to Evaluate Knowledge and Knowledge Management in the Organization Using COBIT 5

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

ISACA BYLAWS **ARE BEING REFRESHED.**

ISACA MEMBERS **ARE ASKED TO VOTE.**

The ISACA® Governance Advisory Council, at the request of the Board of Directors and with the assistance of ISACA staff and legal counsel, conducted a comprehensive review of the Bylaws. This review provided the basis for a full refresh of the Bylaws to align to best practices and embed applicable law.

AFFECT MORE

ISACA members will be asked to vote on the Bylaws when voting is open:

27 April – 6 June 2015

Visit ***www.isaca.org/vote2015***

REGISTER FOR A 2015 SEPTEMBER CISA OR CISM ISACA CERTIFICATION EXAM TODAY!

"IN MY WORK, I INTERACT WITH **VARIOUS PROFESSIONALS**. MY ISACA CERTIFICATIONS HELP **BUILD IMMEDIATE TRUST**."

— NICKSON CHOO, CISA, CRISC
DIRECTOR, RISK ADVISORY
CROWE HORWATH GOVERNANCE SDN BHDKUALA LUMPUR, MALAYSIA
ISACA MEMBER SINCE 2000

Becoming ISACA-certified showcases your knowledge and expertise. Elevate your career and gain the recognition you deserve with ISACA certifications—register for an exam today!

Register at *www.isaca.org/SeptExams15*

ACCOMPLISH MORE

UPCOMING CERTIFICATION EXAMS*:
12 September 2015
*CISA and CISM only. Held in select locations.

Early Registration Deadline: 17 June 2015
Final Registration Deadline: 24 July 2015
Register early and save US $50!

CISA®
Certified Information Systems Auditor®

CISM®
Certified Information Security Manager®

ISACA®
Trust in, and value from, information systems

www.isaca.org/SeptExams15

*CISA®, CISM®, CGEIT® and CRISC™ exams are also available in December—registration opens soon!

VOLUME 3, 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 these articles at *www.isaca.org/journal.*

Online Features
The following is a sample of the upcoming features planned for May and June.

Security Mysteries in the Cloud
Sivarama Subramanian, CISM, and Devaraj Munuswamy, CEH

Simultaneous Implementation of an Integrated ISMS and a BCMS
Nurudeen Odeshina, CISA, CISM, CRISC, ISO 27001 LI, ITSM

IS Audit Basics: The Soft Skills Challenge, Part 2
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;* Hashtag: #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

THERE'S NO SHORTAGE OF **CYBER SECURITY THREATS**

BUT THERE IS A **SHORTAGE OF IT SECURITY PROFESSIONALS**

DO YOU HAVE WHAT IT TAKES TO BE PART OF THE **SOLUTION**?

Cyber attacks are on the rise. Information security professionals are in high demand. Get up-to-date security skills with Capella University's master's or graduate certificate in Digital Forensics or Network Defense, aligned to the latest NSA focus areas.

The new graduate certificates can be completed in as little as 9 months, then applied toward your Master's in Information Assurance and Security (MS-IAS) to make an even bigger impact.

Plus, the knowledge you gained for your CISSP®, CEH®, or CNDA® certifications can help you earn credit toward your MS-IAS, saving you time and money.

ANSWER THE CALL. START TODAY TO LEARN MORE AND EARN MORE.

CAPELLA.EDU/ISACA OR **1.866.933.5836**

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

CAPELLA UNIVERSITY

Frameworkers of the World, Unite 2

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.*

Every now and again, I like to take a poke at standards, just to see what makes them work.[1] Under consideration here is the cybersecurity framework published by the US National Institute of Standards and Technology[2] early in 2014. This document is no longer breaking news; I am more interested in how organizations might comply with it now that it is well known.

I can understand compliance with laws, regulations and even standards. But a framework? It would be easy to say that compliance with a framework is a *non sequitur,* but that would not account for the perception of the document since its publication.[3] In the absence of a true standard, it is being treated as one by many of the organizations with which I am familiar.

Of course, evaluation of a framework as though it were a standard can lead to some very unfair criticism. But then, explicit standards come in for their share of contumely as well. I want to make clear that I think the NIST framework is an excellent beginning of what must be a long process of applying standards to the defense against cyberattacks. I should add that as a publication of the US government, it formally applies only to US government agencies. However, as was made clear in NIST's recent *Update on the Cybersecurity Framework*,[4] it is being applied by a wide swath of the private sector, and international alignment is a major objective of these organizations.[5]

STRUCTURE OF THE FRAMEWORK

The framework is organized in a way that only a bureaucrat could love. There is the framework core, which is composed of functions, which begat categories and subcategories and then information references. Following the framework core, there are framework implementation tiers and a description of framework profiles. Of all these, only the subcategories provide any direction whatsoever toward cybersecurity.

The implementation tiers describe different levels of what can only be termed compliance with the framework, ranging from partial to adaptive. Even NIST admits that the tiers are "the least-used part of the Framework," ascribing this to "their enterprise-level scope."[6] I say it is because there is no purpose to being just a little compliant with a standard (oops, a framework) that is supposed to lead to security, so organizations are only paying attention to the adaptive tier.

The profiles are a way of describing the as-is and will-be states of compliance with the framework. The terms used are "current profile" and "target profile." I find this terminology confusing, and NIST accepts that it is "clear that there remains some confusion over terminology that should be addressed in future efforts."[7]

REFERENCES TO OTHER STANDARDS

For each of the subcategories, there are references given to other standards and frameworks on which the framework is built. These include other NIST standards, ISO 27001 and ISACA's COBIT®.[8] The cross-references are both strengths and weaknesses of the framework.

They are a strength in that they place the framework specifically, and cybersecurity more generally, within the context of information security as it has been known and practiced for many years. With all of these other standards and frameworks, it would seem that there is no need for the Cybersecurity Framework at all...that all an organization needs to do is comply with all the referenced standards and—voila!—cybersecurity will take care of itself. Of course, if a corporation or government agency adhered to every listed standard in detail, plus others not mentioned,[9] they would be so busy complying that they would not have time for information technology and, therefore, would not be at risk. Okay, a bit of an exaggeration, but even if they did comply with all those standards, would they have achieved *cyber*security?

That question, to my mind, points to a weakness of the framework. There is no doubt in my mind that effective cybersecurity rests on a foundation of information security, just as effective information security is built upon a system of internal control. But the need for cybersecurity derives from a substantively different threat—that of organized attackers targeting the systems and information of specific organizations. For that reason, cybersecurity is above and beyond information security (**figure 1**).[10]

Figure 1—Cybersecurity Above and Beyond

Source: Risk Masters Inc. Reprinted with permission.

Compliance with the NIST Cybersecurity Framework requires an organization to put in place a series of measures specifically designed to address *cyber*threats. I take issue with the framework in that in many of its functions, it conflates information security and cybersecurity.

Information security is business-driven. The differential requirement for security in any organization is based on risk management, an industry-by-industry, business-by-business appreciation of the potential for abuse of information resources. Information security results in prudent investment in safeguards and countermeasures. Cybersecurity is threat-driven, the menace being well-financed, expert, patient criminals, terrorists and governments. All of an organization's information assets are at risk, because their interconnectedness exposes all of them to a failure of their most vulnerable elements. As a result of not differentiating the two, the majority of subcategories in the framework are not directly focused on the issue of cybersecurity. Of the 98 subcategories in the framework, only 32 of them directly address cybersecurity (by my count).

> "Effective cybersecurity rests on a foundation of information security, just as effective information security is built upon a system of internal control."

THE 20-YEAR RULE

I come to that conclusion by applying what I call the 20-year Rule. If there was a security measure I was using 20 years ago, it was not a cybersecurity safeguard, because I was not worried about cyberattacks that long ago. So, for example, in the Identify function, Asset Management category of the Cybersecurity Framework, there are six subcategories:

1. Physical devices and systems within the organization are inventoried.
2. Software platforms and applications within the organization are inventoried.
3. Organizational communication and data flows are mapped.
4. External information systems are cataloged.
5. Resources (e.g., hardware, devices, data, software) are prioritized based on their classification, criticality and business value.
6. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

All but the last subcategory fall under the 20-year Rule. That is, only the sixth one addresses a cybersecurity-specific control. Again, it is not that the first five are unimportant; it is just that they are not specific to the threats of cyberattacks, cybercrimes, cybertheft, etc.

But lookie here what I found lurking in the middle of a perfectly nice framework: The 32 subcategories that are cybersecurity-specific constitute a *standard*. Or perhaps it would be better to say they constitute the beginnings of a

standard, since they do not have much depth. For instance, a statement that "incident alert thresholds are established" cries out for answers to what are appropriate thresholds and what should happen if they are surpassed.

NIST states that "the framework developers' intention [was] to encourage alignment among standards already in use." It is to be hoped that new standards will arise that address the open questions raised in this important step supporting broad appreciation of cybersecurity.

ENDNOTES

[1] An article of this same name, minus the 2, appeared in this space in volume 6, 2004. And once again, thanks go to the late William Safire of *The New York Times* for this play on words.

[2] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, USA, 2013. I will refer to it simply as "the framework" here, although I have seen it referred to as NCsF. A search on "ncsf" has convinced me to stay away from that acronym.

[3] See, for example, PivotPoint Security, "Does ISO 27001 Certification Make You NIST Cybersecurity Framework Compliant?" Information Security Blog, *www.pivotpointsecurity.com/risky-business/iso-27001-nist-cybersecurity-framework-compliance*, which directly addresses the issue of compliance.

[4] National Institute of Standards and Technology, *Update on the Cybersecurity Framework*, USA, 5 December 2014

[5] *Ibid.*, p. 5

[6] *Ibid.*, p. 2

[7] *Ibid.*, p. 3

[8] *Op cit*, NIST 2013, p. 35

[9] Such as Payment Card Industry Data Security Standard (PCI DSS), ISO 22301 or NFPA 1600

[10] The little representation of "above and beyond" in **figure 1** is a trademark of my consulting firm. I hereby grant irrevocable license to all readers of the *ISACA Journal* to reuse and reproduce it.

The Soft Skills Challenge

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 1990s, 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.

In my previous column "Auditor: About Yourself (and How Others See You)," published on 1 April 2015 at *www.isaca.org/journal*, I touched on how being more aware of oneself helps to understand our interactions with others. Here, we explore those soft skills that do not appear in the Certified Information Systems Auditor® (CISA®) examination, but are important components of an auditor's life and work.

Figure 1 lists the differences between those things that are part of our nature and so deeply ingrained that they are hard (even impossible) to change and those that can be learned through the combination of the 3 Ds—desire, dedication and discipline. However, these learnable skills are necessary but are not sufficient on their own.

Figure 1—Changeable Vs. Unchangeable Traits

Hard to Change	Learnable
• Temperament • Personality • Cultural values • Work ethic • Risk appetite	• Communications • Interviews • Time management • Negotiation • Collaboration • Problem solving

Source: Ed Gelbstein. Reprinted with permission.

It is important to remember the motto of the University of Salamanca in Spain, which, in 2018, will be celebrating 800 years of existence: *"Quod natura non dat, Salamantica non praestat."*[1]

This Latin expression can be loosely translated as, "If you did not get it from nature, Salamanca cannot give it to you," i.e., without talent, learning is that much harder. This is why not everyone can become a concert violinist or world-record-holding athlete. While there is truth in this, it should never be used as an excuse for not making the best of the knowledge, skills and abilities we do have. And the answer to this involves *learning*.

Learning takes time and it helps to have learned how to learn—a process that depends so much on one's nature that there is no single way that works for everyone. A search engine query on "learning to learn" will lead to many web sites[2] to explore and exploit. Curiosity (not listed in **figure 1**) should be treated as a good thing to have and to exploit.

Be prepared to accept that learning may require you to first unlearn what you already know. Many of the topics covered in my studies 50 years ago now belong in a museum, and the things we deal with today were totally unthought of until recently and had to be learned from scratch. A challenge, but the results are well worth it.

For those seriously interested in soft skills, consider exploring the following:

- An article on soft skills published in the *ISACA Journal* in volume 1, 2011,[3] that takes a different perspective than this column
- A document titled "Soft Skills Resources"[4] on the ISACA® web site
- A 19-minute video[5] produced by the University of Aarhus in Denmark. This is available both as a DVD and online (YouTube).

THE PRIMARY LEARNABLE SKILLS

The exploration of soft skills can make a difference to personal development. In this column, we will focus on communications and interviewing. A subsequent column will explore time management, collaboration, organizational politics and problem solving, and a third column will focus on negotiation and conflict resolution.

Communications

Communications can be broken down into three categories: the verbal, the written and the presentation (the hybrid). All need to be learned and continuously improved. Fortunately, there are many helpful sources of advice. Some starting points are included in the endnotes, but there is a great deal more material from which you can choose.

The prerequisites for successful communications include mastery of language, scope of vocabulary and understanding the culture of those involved. These make a difference in all three areas of communication.

Lack of such competencies, on the other hand, may lead to misunderstandings, mistrust and loss of credibility.

Listening and Nonverbal Cues

Becoming a good listener[6] is probably the hardest skill to acquire, and, interestingly, the Latin root of the word "auditor" precisely defines this skill. But learning to be a good listener requires more than reading a few words; it takes a lot of concentration, willpower and practice.

A really good listener must also learn how to take into account nonverbal communications, also known as body language.[7] This includes body movements, gestures, eye contact, facial expression, physiological changes and more.

Warning: Body language is, like national languages, not universal and is strongly embedded in the culture. For example, some cultures allow body language to be explicit and show emotions openly through gestures, physical proximity and strong—even challenging—eye contact; whereas, other cultures are more focused on controlling emotions and body language and reveal little, unless you are truly familiar with the particular culture.

Control and understanding of body language can be learned and mastered, as evidenced by the best poker players and diplomats. Like good listening, this demands a conscious effort and time to develop and perfect.

Writing

Written communications inevitably involve the drafts and final reports of an audit.[8, 9] The two guides in the endnotes offer particularly good guidance for the preparation of such reports.

However, there are many less-formal communications, such as electronic mail,[10] short text messages or Tweets. These should be used with care to reflect the culture and protocols of the organization. Bypassing lines of authority, using casual language and informality may be inappropriate. Professions like diplomacy, where these tools are valued yet the problems that may arise if they are misused are recognized, have published guidelines11 that may be equally appropriate for auditors.

Presentations and Public Speaking

Presentations and public speaking (e.g., presenting to an audit committee) can cause anxiety. Not doing it successfully can be detrimental to your image and reputation. Fortunately, there are many helpful sources of guidance.[12, 13] There is no secret as to what makes such events successful: knowledge of the subject matter, careful preparation and a clear focus on the audience's needs.

An auditor's challenge is to deliver in such a way that the presentation makes good use of the listeners' time, conveys insights and does so using the language of business, not technical jargon.

Too much detail and lengthy presentations are not only boring, they risk overwhelming the listener. It is interesting to note that scientific studies show the average attention span of an adult is in the range of 10 to 20 minutes, possibly less.[14] As with most things, practice makes perfect.

Interviewing

This is a subset of communications requiring the auditor to:

- Listen carefully, in particular for those things that are not said
- Prepare the interview so that the questions are pertinent and formulated in a manner to encourage the interviewee to open up and provide information other than simple yes and no responses
- Take accurate notes and produce a summary that can be provided to the interviewee for validation or modification

In a multicultural environment, the parties need to be aware of the interaction of a high-context culture[15] (one in which many things are left unsaid and are still clearly understood by members of the same culture) and a low-context culture (in which specificity and directness are more common). When both types of culture are involved in an interview and participants are unaware of such differences, misunderstandings are almost inevitable.

The interviewee, however, needs to make sure that any question is understood correctly and that the reply covers what is needed to answer the question.

DIFFERENT ACTORS HAVE DIFFERENT NEEDS

The audience for auditor communications includes parties with significantly different needs: the auditees with whom contact and exchanges will be the most intense from the start to the end of the audit and beyond; the auditees' management; the chief audit executive; the audit committee; and, from time to time, the external auditors and board.

> "Communicating… must be given attention at the planning stage."

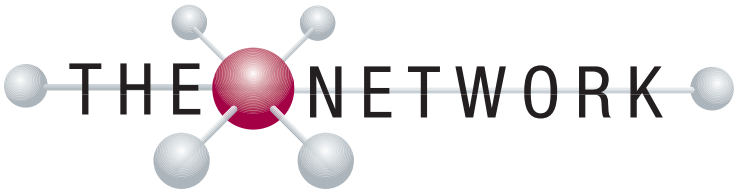
Time is a scarce resource, and communicating with each of these parties must be given attention at the planning stage so that participants do not perceive their time as having been wasted.

CONCLUSION

There is much more to communications skills than the short overview presented here. In the ideal situation, your curiosity and wish for self-improvement will encourage you to explore these topics further.

ENDNOTES

1 Clerus, *www.clerus.org/bibliaclerusonline/es/h2n.htm*
2 Study Guides and Strategies, *www.studygs.net/metacognition.htm*
3 Kandra, Mark; Tim Sewell; Jotham Nyamari; "A Young Professional's Guide to Career Success Using Soft Skills," *ISACA Journal*, vol. 1, 2011, *www.isaca.org/archives*
4 ISACA Knowledge Center, "Soft Skills Resources," *www.isaca.org/Groups/Professional-English/young-professionals/GroupDocuments/Soft Skills Resources.doc*
5 Brabrand, Claus; "Teaching Teaching & Understanding Understanding," *www.daimi.au.dk/~brabrand/short-film/*
6 Skillsyouneed.com, "Listening Skills," *www.skillsyouneed.com/ips/listening-skills.html*
7 Mind Tools Ltd., "Body Language," *www.mindtools.com/pages/article/Body_Language.htm*
8 Gallegos, Fredrick; "The Audit Report and Follow-up: Methods and Techniques for Communicating Audit Findings and Recommendations," *Information Systems Control Journal*, ISACA, vol. 4, 2000, *www.isaca.org/archives*
9 Kaplan, Jim; "The Auditnet Guide to Audit Report Writing," 2009, *www.auditnet.org*
10 Rosenberg McKay, Dawn; "Email Etiquette: Rules for Business Correspondence," About.com, *http://careerplanning.about.com/od/communication/a/email_etiquette.htm*
11 Sandre, Andreas; *Twitter for Diplomats*, DiploFoundation and Istituto Diplomatico, 2013, *http://isdi.esteri.it:4300/ISDI%20ALLEGATI/Twitter%20for%20diplomats.pdf*
12 State of the Art Presentations (SOAP), *http://soappresentations.com/*
13 Presentation Zen, "10 Tips for Improving Your Presentations & Speeches," 6 November 2014, *www.presentationzen.com/*
14 Tomorrow's Professor Mailing List, "Shifting Attention Spans," Msg. #953, Stanford Center for Teaching and Learning, *http://cgi.stanford.edu/~dept-ctl/tomprof/posting.php?ID=953*
15 Education Portal, "Low-Context Culture: Definition, Lesson & Quiz," *http://education-portal.com/academy/lesson/low-context-culture-definition-lesson-quiz.html#lesson*



Opeyemi Onifade

Opeyemi Onifade, CISA, CISM, CGEIT, COBIT 5 Certified Assessor, COBIT 5 Certified Implementer, CISSP, CompTIA Cloud Essentials, ISO 20000 Prac, ISO 27001 LA, ITIL-F, SCJP, ITBMC, PRINCE2 PMP, provides business leadership and execution at Afenoid Enterprise Limited. Afenoid Enterprise offers solutions in business technology optimisation, management systems consulting (ISO 27001, 20000 and 22301) and competence development programmes in IT governance and management. Prior to becoming the founding director and practice leader at Afenoid Enterprise, he held leadership positions as chief information security officer at Galaxy Backbone Limited, senior consultant and regional manager at Digital Jewels Limited, and pioneer country/regional information security officer with the Group Security Office of Ecobank Transnational Incorporated. Onifade's passion is to help top management and boards define and implement technology directions and processes, and manage the risk of technology adoption in order to foster the productive capacities of their businesses.

Q: *As a governance of enterprise (GEIT) professional, how do you believe your background in information security and audit has supported and guided your career to date?*

A: I became interested in information security as a result of an undergraduate project related to smart cards. The project work led to my research in java card, which led to my first professional certification, Sun Certified Java Programmer. I soon realized that I did not want to pursue a career as a programmer but was still interested in information security. I was able to secure employment with a consultancy firm in Lagos, Nigeria, as a senior analyst in its information systems and e-business practice. My manager at the time was a Certified Information Systems Auditor® (CISA®) and Certified Information Systems Security Professional (CISSP), and I set a goal to pass the two exams within a year of my employment. I accomplished my goal and gained the necessary experience to be certified. I left the consultancy to join an international bank, where I became the pioneer information security officer. My experience in that bank spurred my interest in corporate governance, risk management and business management. I became very interested in the ISACA® body of knowledge and, in the process, took and passed the Certified Information Security Manager® (CISM®) exam to strengthen my role at the bank. Then, I began to miss consulting and left to join a start-up consultancy that was passionate about raising awareness in information security and IT governance. It was the only firm in the country offering COBIT® 4.1 training. The extensive exposure to COBIT 4.1 helped me to consolidate my competencies for GEIT. I sat for Certified in the Governance of Enterprise IT® (CGEIT®) in 2010, and I was an early adopter of COBIT® 5. I also became the first COBIT 5 Certified Assessor on my continent.

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

A: I like to describe waste as anything that adds cost without adding value. I think the biggest risk factors being addressed by GEIT professionals, especially in my country, include the likelihood of IT not delivering what is promised and rogue and hidden IT expenses. Another risk factor is the increasing exposure to cyberthreats as a result of technology adoption without sufficient risk analysis and adequate risk controls.

Q: *How do you see the role of GEIT changing in the long term?*

A: I believe that with the deepening of the pervasiveness of IT, IT will no longer be seen as a function, a unit or a department but as a preeminent organizational capability. In the long term, I believe what will count is not what IT delivers but what the business is able to deliver as a result of what IT delivers. I perceive a conceptual evolution whereby IT projects will not just become IT-related projects but business projects. When that time comes, IT governance will not need to be integrated into corporate governance; a distinction will not be reasonable.

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

A: My certifications have not only given me a voice, they have earned me the right to be heard. I believe that certifications are important, because they show one's interest in self-improvement. Our work requires proven knowledge and experience in the COBIT 5 process domains including strategy, risk, security and service management. I am always eager to consider a CGEIT holder.

Q: *What has been, or do you anticipate being, the biggest compliance challenge in 2015? How will you face it?*

A: I think the biggest compliance challenge, especially for the developing economies, will be cybersecurity-related. In my country, for instance, there is a cybersecurity bill that is about to be signed into law. Our government also recently published a cybersecurity strategy. We are responding by developing capabilities and resources to help the market comply.

WHAT ARE YOUR THREE GOALS FOR 2015?

1. Work from home on Mondays.
2. Stay more in touch with friends and family and spend more time assisting my two sons with their assignments.
3. Learn more about investing.

WHAT IS YOUR FAVORITE BLOG?

Personalmba.com

WHAT IS ON YOUR DESK RIGHT NOW?

- Macbook Air
- Desktop computer
- RFPs

HOW HAS SOCIAL MEDIA IMPACTED YOU PROFESSIONALLY?

LinkedIn has been very useful in broadening my contacts and marketing our services.

WHAT IS YOUR NUMBER ONE PIECE OF ADVICE FOR OTHER GEIT PROFESSIONALS?

Seek to earn at least one credential relevant to each of the COBIT® 5 domains.

WHAT ARE YOUR FAVORITE BENEFITS OF YOUR ISACA MEMBERSHIP?

The rich exposure to emerging technologies, vast body of knowledge and kind-hearted professionals

Steve Woo is cofounder and vice president of products at VeloCloud Inc.

Software-defined WAN Changes Retail Security Paradigm

The adoption of cloud-based retail applications, as well as increasing demands for agility, for example, with pop-up retail, is changing the requirements for network access. These trends impact users working from remote retail branches who are accessing applications over the wide area network (WAN). Along with the challenges of providing network access to cloud-based applications from the WAN are demands of a new cybersecurity paradigm. The new security framework compliance mandates requires the delivery of security services over the cloud without complicating branch infrastructure and increasing cost, especially for retailers who need strict adherence to Payment Card Industry Data Security Standard (PCI DSS) 3.0.

Increasingly agile and distributed businesses, continued migration of applications to the cloud, and the parallel advances in networking have enabled technology companies to deliver innovative new approaches to these security requirements.

Utah-based retailer Redmond Inc., which began in 1958 after a prolonged drought forced two brothers to abandon farming and begin mining a prehistoric salt deposit on their property, operates four Real Foods retail markets in Utah and owns 16 manufacturing plants, warehouse facilities and branches located in Utah and Colorado.

> "Diversity creates challenges for the IT team."

Although the facilities operate separately, a centralized IT organization supports all of them. As a diverse, entrepreneurial company, each brand's business model places different demands on the IT infrastructure. For example, the retail stores require compliance with PCI DSS, integration with the existing IT security infrastructure that includes firewalls, intrusion detection and prevention services; and VPN services. Wholesale manufacturing and warehouses require support for mobility, and branch office workers need secure access to their company desktop while teleworking. This diversity creates challenges for the IT team, which needs to support all of the business's operations from a common infrastructure in their headquarters.

Redmond's far-flung operations are connected by a WAN comprised of public Internet links. Advanced security for the applications and devices accessing the cloud applications over the Internet is critically important. Users sometimes had difficulty accessing their virtual desktops, encountered downtime or experienced poor voice quality. Redmond's IT team wanted a WAN solution that would allow them to migrate their unified communications and virtual desktop systems to significantly improve performance and employees' experiences everywhere across the organization.

Compounding the problem were branch office network devices that were reaching end-of-life status. It made sense to decide on a new WAN solution before upgrading branch locations. PCI DSS compliance was another concern. The company's retail locations accept credit card payment and, therefore, must comply with PCI DSS. Retail point-of-sale (POS) systems were compliant with advanced firewall, intrusion detection and software features. However, Redmond wanted to enhance the security of its WAN to further secure retail operations. At the same time, a new WAN could not require a network redesign or additional management resources. The IT team operates as lean as possible, and this would not change.

Redmond's IT team evaluated multiple WAN solutions. They chose a complete cloud-delivered, software-defined WAN (SD-WAN) solution that delivers virtualized services to branch locations with enterprise-class performance, visibility and control. The VeloCloud SD-WAN solution is flexible and can be delivered over the top of public Internet and private networks. The team conducted a proof of concept to ensure that they could connect all branches and achieve improved performance.

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:

SD-WAN delivers enterprise-grade performance across a hybrid WAN combination of private networks and broadband Internet, along with flexible security services such as application-aware firewalls and cloud-enabled virtual private networks (VPNs).

The deployment flexibility of the approach greatly simplified WAN implementation. A business policy approach simplified configurations, including ensuring the correct quality of service (QoS) for business-critical applications. No matter how many Internet links a Redmond site uses or the type of physical connectivity required, it can be handled with automatic discovery instead of manual configuration. Today, Redmond has Long Term Evolution (4G LTE), fiber, digital subscriber line (DSL), cable and mixed 4G/3G wireless links in use across its WAN—all connecting easily with the cloud-delivered SD-WAN.

The solution is now an integral part of the company's infrastructure and available almost everywhere in Redmond's WAN, except for a few large manufacturing sites. Aaron Gabrielson, Redmond's senior manager of IT, says that it takes one IT team member about 30 minutes to install the edge device at each location with only minor changes to the firewall and a few routers. And then they leave—the WAN takes care of itself without requiring IT staff to be present at the remote location.

Key to the deployment is the ease of management based on cloud delivery and adherence to the PCI 3.0 security mandates. With this SD-WAN solution, Redmond IT fulfilled the requirement to segregate the POS network using the virtual local area network (VLAN) trunking feature and restricted user access to the network with a role-based access control. The solution provided an end-to-end encrypted session for the POS traffic with the strong AES-256 scheme and ensured that the payment card traffic was never open in the Internet. Centralized cloud management ensured that policies were consistently deployed across multiple sites and simplified audits to ensure that configurations remained compliant over time.

With the cloud-delivered SD-WAN solution, retailers such as Redmond now have a choice to leverage the benefits of cloud networking and deliver security services in an all-new way.

The Limits of Rules

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 interests include information security and corporate governance. Opinions expressed in this column are his own and not those of Creighton University. He can be reached at *vraval@creighton.edu.*

T. H. Green, a renowned ethicist, once said: "…Whatever moral capacity must be presupposed, it is only actualized through the habits, institutions, and laws, in virtue of which the individuals form a nation."[1] Habits are shaped by one's personal character, family, formal and informal groups, and the community to which one belongs. Families have formal or informal rules by which they attempt to stabilize expectations of behavior among the family members. Institutions and organizations also have to have rules. Interpreted in a larger context, these would include codes of conduct, policies, protocols and other dictates. From neighborhood associations to the county, city, state and nation to which the community belongs, there are all sorts of requirements imposed upon the citizen. Some may be called codes or covenants, others regulations and still others the law. While they are not all laws as such, most of these are often accompanied by some degree of consequences for violation. These are all instruments, artifacts and understandings that cause social, institutional and moral pressure for everyone to behave in the interests of the larger community and, in turn, their own interests.[2]

Any organized form of a community needs rules. Even when we trust each other to do the right thing, rules may help induce and guide proper behavior. In this sense, rules have existed for as long as humans have lived on this earth, for they allow us to set expectations of behavior in families, in organizations and in communities. Rules make life easier because one knows how others will behave, or at least are likely to behave. For example, if the rule is that everyone will drive on the right side of the road, one would expect that the oncoming traffic will show up on the left side of the road. Consistency in following the rules, once set, will provide stability in the group, whether it is a family, institution, business or government. The common interests of a group are maintained by having rules and enforcing them to generate stability.

Codes of conduct, policies, guidelines and protocols—these are all rules in various forms, albeit some at higher levels and, therefore, may not all be considered as such. Rules are somewhat like goals and objectives. When one sets goals, one essentially commits to not indulge in alternatives. For example, if one decides to study for the next few hours, one would refuse an offer to play golf during that time. Goals and objectives provide direction, harnessing energy to achieve something. In contrast, rules do not provide a particular destination or measurement metric one would set out to achieve. They do, however, harness people into behaviors that others expect in the larger interest of the group. The problem is: No one likes being harnessed!

In an interesting reflection on rules, C. S. Lewis notes,[3] rules are made to "restrain…the lusts of our neighbours and to give a pompous coloring to our own." Thus, rules are frequently denials of desires, including those involving morality, such as not to cheat or lie or commit any moral compromise. They also serve the function of self-approval through obedience. For example, corporate executives may brag about their company's regulatory compliance record or how they never had to restate their financial statements.

While all kinds of rules are evident in society, we focus here on the most critical rules: rules that help us act as moral agents.

RULE MAKERS

C. S. Lewis uses an analogy of maps and roads to raise some interesting issues. Think of the early period of time when human existence came into being. Someone had to draw the lines, like in a map, and then implement these in the form of pathways and directions. Like maps and roads that follow the initial mapping, rules exist forever, and one may not recall who set the rules. Lewis uses "landlord" and "steward" in his articulation of how rules came into existence. He argues that it is fruitless to identify the landlord; perhaps it is impossible to search for the landlord. Often, our introduction to the rules is associated with the steward. For example, compliance with corporate disclosures is monitored in the US by the US Securities and Exchange Commission (SEC), an

external steward,[4] and the code of conduct is introduced to new hires by the employer's human resources (HR) director, an internal steward.

If one did not set the rules, one would want to know who set them up and why their observance is necessary. Those who are subject to a rule may ascribe some faith in it if they are aware of the source of and the rationale behind the rule. Rules are often questioned, and, if not addressed properly, the questionability of the rules may turn into violation of the dictate. The perceived sanctity of rules is tied to the authority vested in the one (e.g., the landlord) who set the rules. Unless one has some sort of incentive to obey or fear of backlash from defecting rules, one is less likely to follow the rules.

It is often difficult, and sometimes impossible, to trace the rules to their author. And yet, it seems critical that we understand why a certain steward set a particular rule. Institutions and the government normally follow due process to make the rules. Recently, the US Federal Aviation Authority (FAA) announced a set of proposed rules to govern the deployment of drones.[5] The regulation will limit drone flights to daytime, below 500 feet, at a speed of less than 100 miles per hour, and within sight of the operator, while keeping the ban on commercial drones intact for now. The proposed rules will benefit certain industries (e.g., farming, film making, energy, construction) while capping the potential of commercial use (e.g., package delivery). After all, despite good intentions, the greater good is always a balancing act.

THE ORIGIN OF RULES

The FAA—the steward of the drone-use rules in this case—justified the proposed rules as an attempt to balance the need for flexibility for the emerging drone industry with the agency's heightened moral sensitivity for public safety. We should note, however, that not all rules inherit moral sensitivity; they vary in their association with morality. For example, driving on the designated side of the road has little to do with morality.[6] Here, we will focus on morally sensitive rules.

The origin of a rule rests with its maker. It is important to know the rule maker; if you can't know the landlord, at least you would want to know the steward of the rules. This is because rules of morality carry a value connotation assigned by the rule maker, with which we may or may not agree. If we agree, we would tend to accept the rule from our heart, and this makes the rule worthless in generating proper behavior, because we would have committed to follow our heart regardless of the presence or absence of the rule. On the other hand, if we do not agree with the rules, whose values would we want to follow? Do we follow our conscience or the steward's conscience?[7] If roads are mapped into the world by the "landlord" or his "steward," must we use the roads, or could we create our own trails? Under what conditions would people defy the rules? This is an important question for a simple reason: We rely on a great deal of rules everywhere.

PLAYING BY THE RULES

People obey the rules for various reasons. They may dread the consequences (punishment) of noncompliance, or they may be rewarded for compliance. In Bruce Schneier's terminology, the more doves (people loyal to the rules) we have, the greater the trustworthiness in society.[8] The fight is to limit the rise of the hawks, the defectors, for they thwart the existing balance.

The most recognized defector in recent years is Edward Snowden. His actions had a global impact. At home, depending on who you talk to, he was a hero or a traitor; abroad, he was seeking the sympathy of supporters. The US National Security Agency (NSA), the compromised agency, evaluated its policies and practices and likely plugged holes in their systems. They also had to address the public outcry on the nature and amount of data collected by the NSA and how these were used. On a larger scale, the issue of privacy became the most talked about platform.

> "The fight is to limit the rise of the hawks, the defectors, for they thwart the existing balance."

While most defectors leave considerable damage in the hands of the victimized organization, some may simply prove to be a catalyst for change. On the socio-political front, history echoes the story of Rosa Parks, who, in a bus ride, by not giving up her seat to an Anglo-American passenger, shone a light on the injustices of racial segregation. Indeed, there is a difference among defectors along the lines of intentions and courage to do the right thing for the greater good.

In a remarkable contrast to the defectors, among the loyal followers of rules, there are those who strive to rise above the rules. According to Green, they ask themselves: "Shall I be acting according to my ideal of virtue…as a good man should?"[9] Rising above the rules, he "will always be on the look-out for duties which no one would think worse of for not

recognizing.… He is like a judge who is perpetually making new law in ostensibly interpreting the old."[10] Interestingly, this view of Green is in complete agreement with that of C. S. Lewis, who asserts that you need no rules to obey if they originate from, or agree with, your own conscience. Wordsworth (*Rob Roy's Grave*) beautifully echoes the same sentiment:

We have a passion—make a law, too false
to guide us or control!

And for the law itself we fight in bitterness of soul.

And puzzled, blinded thus, we lose distinctions
that are plain and few;

These find I graven on my heart; that tells me what to do.

LIMITS OF RULES

Where rules do not exist, chaos prevails. The electronic currency, including its most visible variant bitCoin, suffers from the lack of rules for its governance and, therefore, is often suspected of potential criminal activities due to unregulated anonymity. Undoubtedly, the value of rules has been established; without rules, the world would not be the same. Unfortunately, we find ourselves in the midst of more and more rules. For example, rules addressing the issue of net neutrality are in the works and may be announced sometime soon. Rules provide for stability in expectations, protection, security and even human dignity. So, they have a definite place and will likely exist forever. However, rules are a double-edged sword: necessary but costly and invasive, often resulting in apparently nonvalue-added work. Enforcement of rules can detect violations, but cannot always prevent compromises. Rules engender rooted bureaucracies, and they may be overdone in response to a catastrophe or slow to change even in a dynamic environment and, thus, may become overhead at least until they are recast to fit the change.

> "Where rules do not exist, chaos prevails."

What is especially concerning is the fact that despite rules, compromises occur. People, including institutions and the government, know right from wrong but would indulge anyway. Recent hacks on Sony Corp. provide a graphic example of gross indulgence that blurred the line between a corporate hack and cyberterrorism. It seems that rules are incapable of passing on to the people any moral wisdom implicit in them. Thus, rules are mere crutches to support society in the face of anticipated defectors, necessary, but not sufficient and perhaps even effective.

The quandary is this: There appear to be no better solutions. Relying on character traits of individuals is a possibility, but even good people sometimes break their resolve. This may have been induced by the interaction with the nurture side of the nature-nurture relationship. Moral action is the expression of a man's character, as it reacts upon and responds to given circumstances.[11] People have multiple social identities, and moral behavior can change according to which identity is most on their minds. For example, leaving dropped popcorn on the floor of a movie theater may be acceptable, but doing the same on the floor of a church may not be acceptable.[12]

The context can be only an inducer of the compromise. What really matters is the character of the person involved in the act. But then, there are no strong rules for building the character of a nation. We hide behind a pile of rules to protect ourselves from the human frailty and still do not always succeed.

ENDNOTES

1 Green, T. H.; *Prolegomena to Ethics*, BiblioLife, USA, 2010, p. 211
2 Schneier, Bruce; *Liars & Outliers,* John Wiley & Sons, USA, 2012
3 The Pilgrim's Regress, *The Timeless Writings of C. S. Lewis*, Inspirational Press, USA, p. 96-97
4 One might argue that the landlord in this case is the US Congress, which passed the law, e.g., the Sarbanes-Oxley Act.
5 Nicas, Jack; Andy Pasztor; "Landmark Rules for Commercial Drones," *The Wall Street Journal*, 17 February 2015, p. B1-B2
6 This may become a moral issue if driving on one side of the road causes more fatal accidents than driving on the other side.
7 *Op cit*, The Pilgrim's Regress
8 *Op cit*, Schneier
9 *Op cit*, Green, p. 372
10 *Op cit*, Green, p. 360
11 *Op cit*, Green, p. 120
12 Sapolsky, Robert M.; "When Our Ethics Change According to Where We Are, Mind & Matter," *The Wall Street Journal,* 14 February 2015, p. C2

By Daniel Mellado, Luis Enrique Sanchez, Eduardo Fernandez-Medina and Mario Piattini

Reviewed by A. Krista Kivisild, CISA, CA, CPA, who has experience in IT audit, governance, compliance/regulatory auditing, value-for-money auditing and operational auditing in government, private companies and public organizations. She has served as a volunteer instructor, worked with the Alberta (Canada) Government Board Development Program, and served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter.

IT Security Governance Innovations—Theory and Research

With new technology supporting all areas of life, management increasingly needs to evaluate the areas of risk and concern that they need to be aware of and address within the business. Recent studies on IT risk areas indicate the following areas of concern: the rising strategic importance of corporate information and data,[1] data governance and data quality in support of broader business audit review, recent systems failures that impacted retail banking customers,[2] concerns over increased regulation, and insufficient preparation for cyberthreats.[3] These same studies support the proposal that one of the best ways to address these issues is a greater focus on IT governance.

IT Security Governance Innovations discusses a variety of academic studies in the areas of IT security governance and security standards, and it has information on guidelines in IT security governance and IT security governance innovations. This research forms the foundational groundwork to understand IT security governance, and it demonstrates how these concepts have been applied in different industries around the world.

This reference book appeals to researchers and more experienced professionals, as the subjects and techniques in the book form a solid basis to help readers make good decisions and apply effective security governance practices. A compilation of 11 different studies from researchers associated with universities around the world, the first part of the book looks at security governance frameworks, the next examines enterprise-level security governance practices, and, finally, there is an exploration of the most recent issues in information and security governance.

The book's strengths lie in its deep exploration of a wide range of IT security governance topics that will be of interest to a variety of professionals across industry verticals. Topics include a comparison of information security frameworks, IT security governance in e-banking, IT security governance legal issues, IT service management, assessing the maturity of the COBIT® framework, adoption of ISO 27001 and more.

These detailed studies may be relevant to a wide range of IS audit, security, risk and governance professionals; however, those who are less seasoned in the field may find the book to be an interesting read but too technical in nature. Professionals who have worked across different industries and implemented different frameworks but never had the time to do an in-depth comparison will find that this book answers many of their questions and provides insights and guidance on contemporary well-studied approaches for a variety of modern IT security and governance areas.

Progressively increasing technology in the world requires the need for governance and security systems to also become progressively more sophisticated, to have well-supported solutions and to rely upon industry standard frameworks that have been pragmatically applied to the individual organization. *IT Security Governance Innovations* will help readers better support their organizations in achieving these goals.

EDITOR'S NOTE

IT Security Governance Innovations: Theory and Research is available from the ISACA® Bookstore. For information, see the ISACA Bookstore Supplement in this issue of the *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

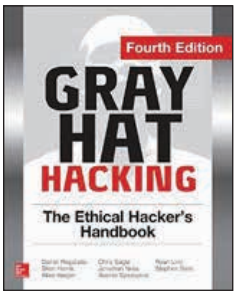
ENDNOTES

[1] Kann, Ronnie; *et al.*; "2015 IT Audit Plan Hot Spots," CEB Audit Leadership Council, 1 November 2014, *https://www.executiveboard.com/*

[2] Sobers, Mike; *et al.*; "Under Control 2015 Hot Topics for IT Internal Audit in Financial Services," Deloitte UK LLP, 1 January 2014, *www2.deloitte.com*

[3] Protiviti, "Cybersecurity Concerns Rise as a Risk Factor for Board Members and Senior Executives in 2015," *www.prnewswire.com/news-releases/cybersecurity-concerns-rise-as-a-risk-factor-for-board-members-and-senior-executives-in-2015-300032571.html*

Gray Hat Hacking: The Ethical Hacker's Handbook



By Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams

Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA, a corporate governance, internal controls, fraud and enterprise risk assurance professional. Etea also serves as a member on the advisory council of the Association of Certified Fraud Examiners (ACFE).

The rise of hacking exploits and their potential to cause havoc to enterprises, nations, industries and individuals has led to a need for more information on hacking. *Gray Hat Hacking: The Ethical Hacker's Handbook* is written by a team of experts with advanced knowledge in gray hat hacking and penetration testing, and the book includes proven strategies and techniques meant to fortify user networks and help prevent current and emerging digital catastrophes.

The book offers a variety of hacking tools and weapons, case studies, mitigating remedies against attacks, and ready-to-deploy models. It gives an overview of modern hacking tools and techniques such as Android-based exploits and reverse-engineering techniques. It also outlines the ethical considerations of hacking, including existing cyberlaws. The book was compiled by a team of experts with years of experience in the field, demonstrated by the depth and accuracy of this book. *Gray Hat Hacking* highlights important points in its note bookmarks and lists useful links and references in each chapter. Additionally, practical codes and command structures bring theory to real-life scenarios, which are included in the book as engaging illustrations, graphics and tables.

The book succeeds in giving a holistic guide to the subject of gray hat hacking by addressing the different facets of the subject, from definitions to legal developments in the area. It also provides up-to-date granular threat profiles, processes, techniques, commands and tools that are utilized in modern-day hacking. All of this is achieved while keeping to the key theme of the gray hat—responsible and truly ethical in its intentions and the materials prescribed. A key aspect of the book's coverage is a focus on programming, which is needed in order to be able to create exploits or review source code. Fuzzing techniques and shellcode creation are also reviewed, as are advanced penetration methods and exploits.

The benefits derived from the book are numerous and readers will be able to:

- Build and launch spoofing exploits with Ettercap and Evilgrade
- Hack Cisco routers, switches and network hardware
- Bypass Windows Access Control and memory-protection schemes
- Use advanced reverse-engineering to exploit Windows and Linux software and learn the use-after-free technique in recent zero-day exploits
- Neutralize ransomware before it takes control of their desktop
- Find one-day vulnerabilities with binary diffing and other similar techniques

The book itself is broken into three parts and has 23 chapters. The first part prepares the readers with essential tools and techniques, such as programming and reverse engineering. It describes the distinctions between black, gray and white hat hackers and their respective characteristics. The second part delves deep into advanced penetration techniques and exploits, with hands-on testing labs, covered beyond what is available in print and other materials on the subject. The final part covers Android malware, ransomware, 64-bit malware and next-generation reverse engineering.

The book delivers a comprehensive and up-to-date compilation of the gray hat hacker's tools and materials, with downloadable hands-on labs that can be replicated by readers. Since the last edition, 12 new chapters have been added and many of the gaps from the previous edition have been addressed.

EDITOR'S NOTE

Gray Hat Hacking: The Ethical Hacker's Handbook is available from the ISACA® Bookstore. For information, see the ISACA Bookstore Supplement in this issue of the *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

How to Evaluate Knowledge and Knowledge Management in the Organization Using COBIT 5

Bostjan Delak, Ph.D., CISA, CIS, is an assistant professor on several faculties in Slovenia and senior consultant for IS advisory and IS audit at ITAD, Technology Park Ljubljana, Slovenia. His research interests include IS analysis, IS due diligences and knowledge management. His main occupation is IS auditing.

Knowledge is recognized as the most important strategic asset of any and every organization. It is very important to identify, capture/acquire, share, reuse and unlearn knowledge. These activities are managed through knowledge management. It is a rather challenging task to evaluate the level of knowledge and knowledge management in an organization. This article seeks to evaluate how the use of COBIT® 5 can enhance the due diligence for knowledge management and knowledge evaluation within the enterprise. Due diligence was conducted on two Slovenian companies using the COBIT 5 framework for knowledge and knowledge management evaluation. The results of the study, presented here, clearly indicate that COBIT 5 can be effectively used as an approach to assess an organization's knowledge management within due diligence.

The next step beyond data and information is knowledge.[1] Knowledge is considered to be an important resource to maintain the competitiveness of an organization. "In an economy where the only certainty is uncertainty, the one sure source of lasting competitive advantage is knowledge."[2] For every organization, it is important to know how to identify knowledge and how to share it. One challenge is determining how to identify the level of knowledge and evaluate the level of knowledge management. COBIT 5 has stepped forward to help solve this issue, with its inclusion of process BAI08 *Manage knowledge*. Together with process APO07 *Manage human resources*, these processes provide a sufficient basis for knowledge and knowledge management evaluation.

Is it feasible to measure knowledge, knowledge sharing and knowledge management within the organization using the COBIT 5 framework?

WHAT IS KNOWLEDGE?

"Knowledge is the currency of the current economy, a vital organizational asset and a key to creating a sustainable competitive advantage,"[3] according to Mohamed Ragab and Amr Arisha. Knowledge is epistemologically classified in two dimensions—tacit and explicit—and from an organization's perspective, has two distinct goals: generate knowledge and apply knowledge. Author Michael Polanyi defines tacit knowledge as personal, context-specific and, thus, not easily visible and expressible, nor easy to formalize and communicate to others.[4] Professor Levy vividly described tacit knowledge, as "What someone has between the ears."[5] On the other hand, Polanyi refers to explicit knowledge as being transmittable in some systematic language such as words, numbers, diagrams or models.

Sharing knowledge can help an organization achieve better organizational performance through the implementation of new ideas, processes, products and/or services. The need to measure knowledge resources within the organization has, therefore, emerged as a key area of interest for researchers and practitioners within the knowledge management domain.

MANAGING KNOWLEDGE

One of the simplest definitions of knowledge management is the "conscious strategy of getting the right knowledge to the right people at the right time and helping people share and put information into action in ways that strive to improve organizational performance."[6] Today, information and communications technology (ICT) plays an important role in major competitive organizations, and several papers refer to the role of ICT in knowledge management. Some argue that the measurement of knowledge is one of the most difficult knowledge management activities.[7] There are different frameworks and methodologies to measure knowledge and knowledge management.

COBIT 5 AND KNOWLEDGE MANAGEMENT

When it was issued in 2012, one of many improvements in COBIT 5 was BAI08. The process's description is "Maintain the availability

of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge."[8] The pre-existing process APO07 also deals with knowledge and knowledge sharing and says, "Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported by competent and motivated people."[9]

CASE STUDIES

The two COBIT 5 processes mentioned, APO07 and BAI08, serve as a basis for this study's qualitative analysis. The purpose of the case studies was to validate the approach by conducting closed interviews (a questionnaire with predefined possible answers) with top management in the case study companies. The questionnaire was built using the COBIT 5 description of these two processes and their practices from the COBIT 5 product family documentation: *COBIT® 5: Enabling Processes*, *COBIT® 5: for Assurance* and *COBIT® Process Assessment Model (PAM): Using COBIT® 5*. The COBIT 5 knowledge management questionnaire contained 97 questions and was divided into three parts: enabling processes (with 36 questions in 11 question subgroups), assessment (with 15 questions in eight question subgroups) and process assessment (with 28 questions).[10]

For these case studies, two companies from Slovenia were selected. The first (company A) is a software/solution development company with an international focus. The second (company B) is a consultancy and service company that works mainly with the Slovene market. The study was conducted in the first quarter of 2014. The evaluation method was based on the mathematical analysis of responses from interviewees. For each answer, the transition to numeric values was made for the first and second part of the questionnaire based on: "yes" equals 2, "partially" equals 1 and "no" equals 0. Each management practice question consisted of several subquestions (marks for subquestions were added and divided by the number of subquestions).

Figure 1—Results for Part 1 of the Questionnaire: Enabling Processes

	Knowledge Management Questionnaire Part 1	Company A	Company B
ID	Management practices/ total score	**1.34**	**0.71**
APO07 Manage Human Resources		**1.55**	**0.84**
APO07.01	Maintain adequate and appropriate staffing.	2.00	1.20
APO07.02	Identify key IT personnel.	1.25	1.00
APO07.03	Maintain the skills and competencies of personnel.	1.29	0.71
APO07.04	Evaluate employee job performance.	1.50	0.63
APO07.05	Plan and track the usage of IT and business human resources.	1.75	0.75
APO07.06	Manage contract staff.	1.50	0.75
BAI08 Manage Knowledge		**1.10**	**0.55**
BAI08.01	Nurture and facilitate a knowledge-sharing culture.	2.00	0.60
BAI08.02	Identify and classify sources of information.	0.75	0.75
BAI08.03	Organize and contextualize information into knowledge.	1.25	0.75
BAI08.04	Use and share knowledge.	1.00	0.67
BAI08.05	Evaluate and retire information.	0.50	0.00

Figure 1 presents the calculated results for enabling processes for both companies (part 1 of the questionnaire). The research shows that company A has partially implemented both processes (total score is 1.34), where the calculated result of the survey performers based on their assessment of the survey value scale for process APO07 is 1.55 and the score for process BAI08 is 1.10. For company B, the research also indicates some implementation of the knowledge management process (total score is 0.71), which, correlated with the organization's calculated result from the survey, was almost half that of company A.

Figure 2—Results for Part 2 of the Questionnaire: Assurance			
	Knowledge Management Questionnaire Part 2	**Company A**	**Company B**
ID	Management practices/ total result	**0.97**	**0.47**
APO07 Manage Human Resources		**0.69**	**0.44**
APO07.01	Maintain adequate and appropriate staffing.	1.00	1.00
APO07.03	Maintain the skills and competencies of personnel.	1.75	0.75
APO07.04	Evaluate employee job performance.	0.00	0.00
APO07.05	Plan and track the usage of IT and business human resources.	0.00	0.00
BAI08 Manage Knowledge		**1.25**	**0.50**
BAI08.01	Nurture and facilitate a knowledge-sharing culture.	1.50	1.00
BAI08.02	Identify and classify sources of information.	1.50	0.00
BAI08.04	Use and share knowledge.	1.00	1.00
BAI08.05	Evaluate and retire information.	1.00	0.00
Note: There were no questions included in the questionnaire for subprocesses APO07.02 *Identify key IT personnel*, APO07.06 *Manage contract staff* and BAI08.03 *Organize and contextualize information into knowledge.*			

Figure 2 presents the calculated results for part 2 of the questionnaire, assurance for both companies. The set of assurance questions is different from the questions used in the first part, enabling processes, but the survey audience is the same. The research shown that company A has partially implemented both processes (total score is 0.97), which correlated with the average of the calculated result from the survey for process APO07 (0.69) and for process BAI08 (1.25). For company B, the research shown a lower score (0.47), which was in-line with the organization's calculated result from the survey for process BAI08 (0.50) and process APO07 (0.44).

The third part of the questionnaire covered the process assessment model (PAM) questions, which have a wider range of values, as the questionnaire allows for four possible answers. In this case, the numeric transformation was based on: fully achieved equals 3, largely achieved equals 2, partially achieved equals 1 and not achieved equals 0.

The work products in **figure 3** present summary headings, and for each heading, there were several statements/questions in the actual questionnaire. **Figure 3** presents the numeric results for both companies. The differences between company A and company B are even bigger than within the data presented in **figures 1** and **2**.

To validate the approach, management of both companies also completed a self-assessment questionnaire provided by ISACA®. Results from company A show that the company is at the third process capability level—managed—out of six possible capability levels for both reviewed processes, which correlated with the result from COBIT 5 PA 2.1 *Performance management*.[11] Results from company B show that the company is at the second process capability level—performed—which is in-line with their result from COBIT 5 PA 1.1 *Process performance*.

DISCUSSION

A study of research papers on knowledge management outlined several issues that had not been fully answered and left open the question as to how knowledge management could be easily measured during process analysis. While the case studies were realized within only one country (Slovenia) and with a limited number of organizations, the research completed indicates that the COBIT 5 framework is suitable for use in rapid assessment of knowledge management within companies that are ICT-oriented and have major processes supported by ICT. COBIT 5 does not integrate widely used human capital methods such as human capital readiness, human capital index and human capital monitor, which were presented in the critical review of knowledge and knowledge management.[12] Some authors suggest a chief knowledge officer (CKO) be appointed to lead an organization's knowledge effort; however, COBIT 5 does not address this item. Currently, the chief information officer (CIO) is accountable for all management practices within APO7. BAI08 is more complicated, and the accountability for

Figure 3—Results for Part 3 of the Questionnaire: Process Assessment			
		Company A	Company B
Organization Level of Knowledge Management for Both Processes		**1.76**	**0.43**
APO07 Manage Human Resources		**1.71**	**0.41**
Outcomes			
APO07.O1	The IT organizational structure and relationships are flexible and responsive.	3	1
APO07.O2	Human resources are effectively and efficiently managed.	3	2
Work Products			
APO07.WP1	Staffing requirement evaluations	1	0
APO07.WP2	Competency and career development plans	1	1
APO07.WP3	Personnel sourcing plans	1	0
APO07.WP4	Skills and competencies matrix	1	0
APO07.WP5	Skills development plans	0	0
APO07.WP6	Review reports	0	0
APO07.WP7	Personnel goals	3	1
APO07.WP8	Performance evaluations	3	1
APO07.WP9	Improvement plans	2	0
APO07.WP10	Inventory of business and IT human resources	0	0
APO07.WP11	Resourcing shortfall analyses	0	0
APO07.WP12	Resource utilization records	2	0
APO07.WP13	Contract staff policies	3	0
APO07.WP14	Contract agreements	3	1
APO07.WP15	Contract agreement reviews	3	0
BAI08 Manage Knowledge		**1.82**	**0.45**
Outcomes			
BAI08.01	Sources of information are identified and classified.	1	1
BAI08.02	Knowledge is used and shared.	3	1
BAI08.03	Knowledge sharing is embedded in the culture of the enterprise.	3	1
BAI08.04	Knowledge is updated and improved to support requirements.	3	0
Work Products			
BAI08.WP1	Classification of information sources	2	1
BAI08.WP2	Published knowledge repositories	3	1
BAI08.WP3	Knowledge user database	2	0
BAI08.WP4	Knowledge awareness and training schemes	2	0
BAI08.WP5	Knowledge use evaluation results	1	0
BAI08.WP6	Rules for knowledge retirement	0	0
BAI08.WP7	Communications on value of knowledge	0	0

this management practice is divided into different positions, including business executives, CIOs and business process owners.

Some researchers[13, 14] state the importance of documenting measurable results/scores, and with the COBIT assessment program, ISACA provides a way to measure COBIT 5 processes' capabilities in a robust, reliable and repeatable way.

CONCLUSION

"The most important contribution management needs to make in the 21st century is to increase the productivity of knowledge work and knowledge workers."[15] COBIT 5 supports this statement and once again confirms one of its IT-related goals: knowledge, expertise and initiatives for business innovation.[16]

The answer to the question of whether it is feasible to measure knowledge, knowledge sharing and knowledge management within the organization using COBIT 5 is that the framework is an effective tool for assessing levels of knowledge sharing and knowledge management, as presented in **figures 1, 2** and **3**. While COBIT 5 has some limitations when evaluating the level of knowledge and the value of intellectual capital within the organization, this research clearly shows that an experienced COBIT 5 specialist can very quickly evaluate the level of knowledge management in an organization during due diligence, IS analysis or even IS audit.

ENDNOTES

1 Gray, P.; "Knowledge Management," Proceedings of the Americas Conference on Information Systems, paper 292, 1999

2 Nonaka, Ikujiro; "The Knowledge-Creating Company," *Harvard Business Review*, July 2007, *https://hbr.org/2007/07/the-knowledge-creating-company/ar/1*

3 Ragab, M. A. F.; A. Arisha; "Knowledge Management and Measurement: A Critical Review," *Journal of Knowledge Management*, vol. 17, no. 6, 2013, p. 873-901

4 Polanyi, M.; *The Tacit Dimension*, Routledge and Kegan Paul, England, 1966

5 Levy, L.; "Data Analytics for Knowledge Discovery, Improving, and Sustaining Quality," keynote presentation, KM Conference 2013, Novi Sad, Serbia, 2013

6 O'Dell, C.; C. J. Grayson; *If Only We Knew What We Know: The Transfer of Internal Knowledge and Best Practice*, Free Press, USA, 1998

7 Chen, A. N. K.; T. M. Edington; "Assessing Value in Organizational Knowledge Creation: Considerations for Knowledge Workers," *MIS Quarterly*, vol. 29, no. 2, June 2005, p. 279-309

8 ISACA, *COBIT® 5: Enabling Processes*, 2012, *www.isaca.org/cobit*

9 *Ibid*.

10 The full questionnaire can be obtained by a direct request to the author at *bostjan.delak@itad.si.*

11 ISACA, *COBIT® Process Assessment Model (PAM): Using COBIT® 5*, 2013, *www.isaca.org/cobit*

12 *Op cit*, Ragab and Arisha

13 Arisha, A.; M. Ragab; "The MinK Framework: Developing Metrics for the Measurement of Individual Knowledge," Proceedings of KIM2013 Knowledge & Information Management Conference, UK, 2013

14 Skyrme, D.; *Measuring Knowledge and Intellectual Capital*, Business Intelligence, 2003

15 Drucker, P.; "Knowledge-Worker Productivity: The Biggest Challenge," *California Management Review*, vol. 41, no. 2, 1999, p. 79-94

16 *Op cit*, ISACA 2012, p. 15

The Underestimated Social Engineering Threat in IT Security Governance and Management

Roberto Puricelli, CISM, is a senior information and communications technology (ICT) security consultant at CEFRIEL, an innovation company of Politecnico di Milano. He has experience in various domains of information security, including vulnerability assessment, penetration testing, web application and mobile security, and risk analysis. He is involved in research on new generation threats, with a particular focus on social engineering attacks. As such, he contributed in developing a specific methodology aimed at measuring the related risk.

The cybercrime ecosystem is radically changing. The evolution of some key technologies and the increased availability of powerful malware enable a business-oriented mind-set among cybercriminals. In recent years, numerous cases of advanced persistent threats (APTs) and data breaches have been seen, with those involving the largest, most high-profile enterprises garnering the most media attention. These scenarios represent only the known cybercrime issues, while, most likely, many attacks have not yet been detected or disclosed to the public. From this point of view, 2014 was a critical year: Large enterprises such as Sony, JP Morgan Chase, Target and many others suffered cyberattacks with serious consequences for the companies and their customers.

From the analysis of new attack strategies, it becomes evident that, more frequently, cyberattackers are seeking to gain a foothold into a corporate network by leveraging vulnerabilities and, from there, moving laterally to extend the compromised perimeter and take control of other systems within the target company in order to gain access to critical information. Moreover, the first phase in the attack frequently involves employee behaviors manipulated through social engineering techniques.

THE HUMAN FACTOR AS A NECESSARY PART OF INFORMATION SECURITY

Historically, employees have been the source of most security issues in organizations. The first aspect is related to the insider threat, meaning any disgruntled, mischievous or deviant employee (as well as former employee, consultant or business partner) who could take advantage of information or systems' internal knowledge to damage the company. In addition to the traditional role of the insider, the oblivious employee must be considered as well and will be the focus of this article. This individual, driven by a social engineering attack, may put corporate information at risk by performing a malicious action without realizing it. Cybercriminals understand that social engineering techniques can be used to manipulate their victims to obtain sensitive information and convince them to perform certain operations, thus increasing the success rate of attacks.

As a matter of fact, some of the most recent data breaches can be considered examples of this scenario. The ICANN data breach originated from spear phishing, which allowed attackers to gain access to users' information on the centralized zone data system.[1] According to the investigations performed on the Carabank attack, which involved several banks across different countries, employees were targeted by social engineering attacks that allowed for the delivery of malware.[2]

Research confirms that the human factor is a weak point in the IT security chain. For example, it has been demonstrated that offering a reward of US $1 is enough to convince a large percentage of users to download and run a potentially malicious software, ignoring the typical security warning.[3]

Human error or misbehavior is often related to a lack of risk perception associated with nonrational factors, such as personal experience and psychological attitude, especially in cases of poor or missing awareness. A confirmation of this fact comes from the practice of phishing, which remains one of the most effective weapons for social engineering, even in a context where cyberattacks are constantly evolving and becoming more sophisticated.[4]

For all these reasons, it is no longer possible to limit the governance and management of enterprise IT (GEIT) to technological matters only. In the past, following the best guidelines when acquiring new appliances and configuring systems was enough to maintain an adequate level of security. Data breaches and other threats were just a remote thought for enterprises.

Unfortunately, this is not the present reality. The point is not whether IT security professionals of targeted companies deployed the best technology, processes and solutions (to be fully compliant with industry practices and standards). Rather, the relevant fact is that those security measures are no longer enough. Security attacks increasingly rely on human vulnerabilities; hence, it is fundamental to extend IT security governance to include the human factor into corporate risk analysis and assessment. To do this in an effective way, it is critical to understand and measure the actual risk and to propose effective and tailored countermeasures to mitigate it.

HOW TO ASSESS THE HUMAN FACTOR

Current approaches to IT security and risk management tend to underestimate—or even ignore—the human factor in the assessment models, tools, processes and legal structure. Since involving employees inside an assessment is a relatively innovative approach and is considered risky, planning the assessment in a proper way assumes an important role. First of all, IT and security departments are not the sole actors to define the assessment, because people are the targets. Therefore, it is necessary to involve all the relevant stakeholders, such as human resources (HR), legal and communications departments, in order to explain the threats, share the objectives, define the scope of the assessment and obtain commitment. Moreover, there are several ethical concerns and requirements that need to be considered when performing an assessment on the human factor.[5]

Social engineering attacks mean that an employee is deceived into violating a policy. Despite the fact that unscrupulous cybercriminals will make these attempts, enterprises must observe serious ethical and legal limitations, in particular, guaranteeing the respect of the trust relationship between employer and employee and avoiding invasion of an employee's personal sphere. Furthermore, it is necessary to consider the labor legal frameworks, which are radically different between the US and Europe, where employees are protected from any interference from the employer. For example, in Italy, the law prohibits an employer from monitoring the behavior of employees; hence, in an assessment, it is not possible to reveal the details of single users who may be involved in an attack. Despite the limitations and the presence of some legal and ethical risk, interest in this topic is increasing, even in Europe.

Since 2010, the assessment of several large European enterprises trying to overcome the difficulties related to this kind of activity has resulted in the development of the Social-driven Vulnerability Assessment methodology.[6] The aim of this assessment is to test human behavior against a spear-phishing attack simulation, in which an attacker attempts to trick users (i.e., company personnel) into performing actions that could put company assets at risk, for example:

1. Getting the employee to click on a link inside the email, visiting a possible malicious web site and, thus, exposing the organization to a drive-by-infection attack
2. Getting the employee to insert certain requested information into a web site form, thus providing critical information such as enterprise credentials

By using a controlled web site and tracking the users' behavior, it is possible to measure the inclination of employees to fall victim to such an attack, and it is also possible to estimate the level of exposure of the enterprise to technological follow-up attacks from the simulated phishing campaign (e.g., identifying unpatched services that can be exploited through a system fingerprinting).

WHAT IS THE ACTUAL RISK?

A significant number of assessments using the Social-driven Vulnerability Assessment methodology were performed in large enterprises (more than 12,000 employees) to try to gain an understanding of (or at least to have an idea about) the level of risk.

In most of these assessments, a spear-phishing campaign that relied on generic hooks (i.e., related to general topics that may be attractive for users, such as special offers or discounts for employees) was performed. Most of the attacks were just slightly contextualized to the specific company (through colors, logos, templates and proper styles of communication). In some cases, a reference to a specific company (based on publicly available information) was used. This did not significantly influence the results.

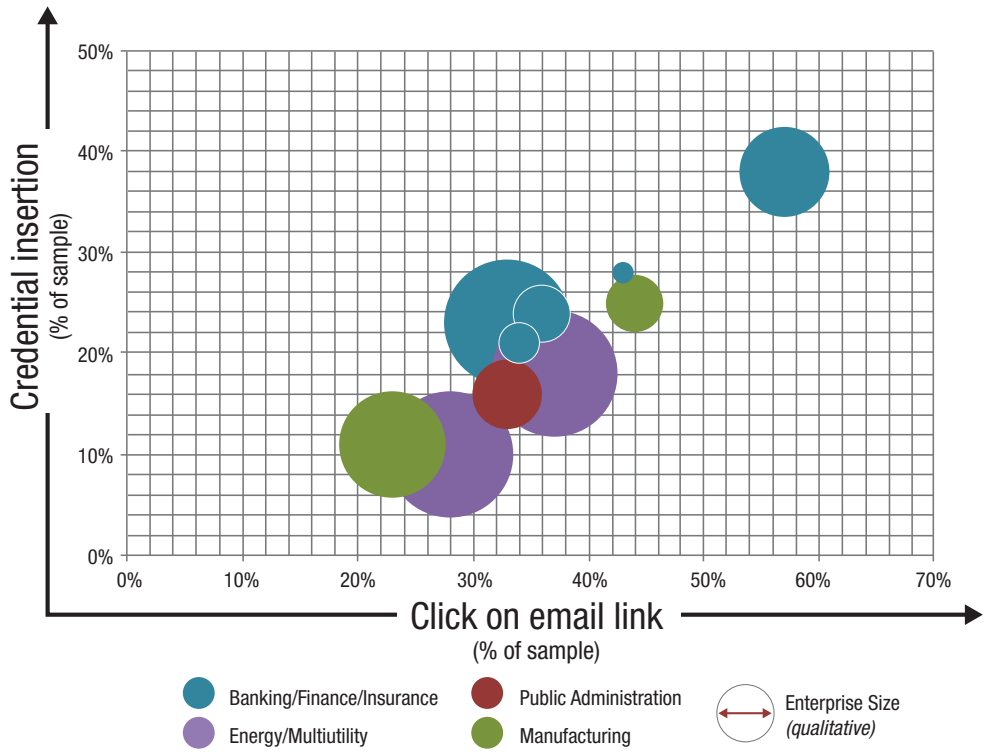
Figure 1 shows a comparison of the results of the assessments, plotting the success rate of each of the two steps described previously for the sample involved in the test: percentage of employees who clicked on a link inside the email on the x-axis and percentage of those who inserted the company credentials on the y-axis. Each circle represents an assessment performed in a company, its radius represents the size of the company itself and the color represents the industry sector. The average results are quite impressive and confirm that spear-phishing attacks actually work quite well. In these assessments, one employee out of three (34 percent) followed the link contained in a phishing email, and one out of five (21 percent) also inserted company credentials in the web site form.

These results are even more impressive when correlated to the temporal factor. According to these results, a phishing campaign is characterized by an impulsive behavior of the employee that causes a rapid growth of the success rate in the early phases, reaching a 50 percent effective rate in only 20 minutes. That means that the available time frame for an effective reaction from the information and communications technology (ICT) security function is quite short. Especially in big enterprises, there seems to be a lack of formalized processes that allow enabling countermeasures based on users' reports and, frequently, a poor level of employee knowledge with regard to how to report a security incident.

Another interesting point is that all employees are subject to this threat. There does not seem to be any particular difference when analyzing the results according to age, location, department or role. Even management and executives are often quite vulnerable. In general, it has been observed that the higher the role in the company, the lower the exposure, but the percentage of deceived managers is not marginal, posing some problems that should be considered from a risk management perspective.

Finally, through fingerprinting techniques, information was gathered on the security posture of the devices used to browse web sites (the users' workstations), and vulnerabilities were found that introduce a high level of exposure to

Figure 1—Comparison of the Results of Social-driven Vulnerability Assessments



Source: CEFRIEL. Reprinted with permission.

technological attacks. This means that using a combination of slapdash exploits, malware code and customized (yet simple) obfuscation techniques, it is possible to bypass the technological countermeasures inside a company and obtain a privileged access to the internal network, exactly the main goal of modern cyberattackers.

HOW TO MITIGATE THE RISK

From an information security governance point of view, the end goal of including the human factor into vulnerability assessment activities should be to identify suitable mitigation. The most effective countermeasures against the highlighted risk are awareness and training, which help improve the security culture of employees.

> "The end goal of including the human factor into vulnerability assessment activities should be to identify suitable mitigation."

Unfortunately, traditional awareness programs are not always effective,[7] based on the fact that some of these tests were performed just after an awareness program was put in place. No significant variations from the average results were seen in these cases. Or, at least, effectiveness of awareness programs is not usually measured.

Cybercrime enabled by social engineering is a threat that can be easily understood by nontechnical people, and having a quantitative indication of the risk could enable a better commitment and budget for corrective remediation. An objective measurement also enables the prioritization of targets for training. Furthermore, repetition of the assessment before and after training programs may help in evaluating the effectiveness of awareness programs.

The real issue is how to create long-lasting training programs that could effectively increase the security level of the company and how to then maintain this increased level of security.[8, 9] Traditional awareness programs sometimes fail because users may lack motivation to learn and to make paying attention to different signals of fake communications part of their daily habits.

Finding the right way to raise awareness is a key factor. The most promising attempts are related to using visual elements, such as video, infographics or info pills to stimulate people. Moreover, gamification is one of the most promising trends. Rewards, social engagement and direct feedback during everyday working life can help, even if the right strategy depends on different factors that must be carefully explored.

THE SOCIAL ENGINEERING RISK MANAGEMENT STRATEGY

The human factor, in particular the social engineering aspect, is a relevant vulnerability of enterprises' systems. This particular risk area is often underestimated and hard to manage. Employees may be the victims of attacks based on social engineering because they do not have the necessary training about these threats or the ability to recognize which kind of web sites or file attachments are safe to open. It is critical to conceive a strategy for including this specific human-factor-related risk in the security IT governance processes.

COBIT® 5 also considers human factors and behavior as key enablers (albeit often underestimated) for designing a holistic approach for GEIT.[10] Assessments targeting the human factor add an effective metric to measure the level of achievement of the information security goal. It is essential to establish good practices with the purpose of correcting, encouraging and maintaining the security culture throughout the enterprise. In particular, communication and security awareness and training are activities that must be performed in a proper way to increase their effectiveness.

The application of a holistic approach in this sense may be difficult. A solution should include increased internal collaboration among the stakeholders of the departments involved. This can be achieved by transferring, in a simple way with objective results and measurable figures, the perception of the actual risk to nontechnological functions, such as the communications or HR departments. This collaboration may also be valuable to redefine investment planning to contrast the highlighted risk and introduce shared budgets (not just from IT) on human-factor, security-related activities, because the actions shift from the technological to the HR field.

Collaboration among departments can support enterprises and help them to define and implement programs that effectively allow for improving the governance of information security.

CONCLUSION

Nowadays, it is not possible to reach an adequate ICT security level with only technological countermeasures, because modern cyberattacks could bypass all the defense layers, exploiting the human factor through social engineering techniques. The results discussed in this article confirm the fact that employees can be deceived to perform dangerous actions that may put the company at risk. Hence, in order to mitigate this risk, companies must develop a strategy aimed at understanding the actual extent of the problem and promoting effective actions.

> "Companies must develop a strategy aimed at understanding the actual extent of the problem and promoting effective actions."

To identify the actual level of risk, the claim that companies need to assess their employees is spreading. Due to the criticality of this step, from both ethical and normative perspectives, companies must rely on a specific and tailored methodology that can measure the potential effectiveness of a social engineering attack. Effectively applying such a specific methodology, the achieved results have proved to be useful to obtain commitment from senior management in order to implement mitigation actions, mainly related to employees' education.

In fact, to raise awareness in order to mitigate the risk, potential investments should not be focused only toward traditional education but also toward experimentation of innovative ways of awareness. This could be quite useful in effectively changing the company culture and contributing to elevation of its overall security level.

ENDNOTES

1 ICANN, "ICANN Targeted in Spear Phishing Attack. Enhanced Security Measures Implemented,"16 December 2014, *https://www.icann.org/news/announcement-2-2014-12-16-en*

2 Kaspersky Lab, "The Great Bank Robbery: The Carbanak," Securelist, 16 February 2015, APT, *http://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/*

3 Guanotronic, "It's All About The Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice," *http://guanotronic.com/~serge/papers/fc11.pdf*

4 Dhamija, R.; *et al.*; "Why Phishing Works," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2006, *www.cs.berkeley.edu/~tygar/papers/Phishing/why_phishing_works.pdf*

5 Mouton, F.; *et al.*; "Social Engineering From a Normative Ethics Perspective," *Information Security for South Africa (ISSA)*, Johannesburg, South Africa, 2013, *http://icsa.cs.up.ac.za/issa/2013/Proceedings/Full/77/77_Paper.pdf*

6 Brenna, R.; *et al.*; CEFRIEL, "Social Driven Vulnerability," *Technology*, February 2014, *www.slideshare.net/CEFRIEL/social-driven-vulnerability-english-version*

7 Kumaraguru, P; *et al.*; "Teaching Johnny Not to Fall for Phish," Journal ACM Transactions on Internet Technology, 2010

8 Kumaraguru, P.: *et al.*; "Lessons From a Real World Evaluation of Anti-phishing Training," APWG eCrime Researcher's Summit, January 2008

9 Caputo, D.; *et al.*; "Going Spear Phishing: Exploring Embedded Training and Awareness," *Security and Privacy*, IEEE, vol. 12, iss. 1, 23 August 2013

10 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/cobit*

The Time for Sustainable Business Is Now

Leveraging COBIT 5 in Sustainable Businesses

Graciela Braga, CGEIT, COBIT 5 Foundation, CPA, is vice president of the Commission for the Study of Record Systems of the Buenos Aires Institute of CPAs in the city of Buenos Aires, Argentina. She is also a researcher at the Instituto Autónomo de Derecho Contable (Autonomous Accountancy Law Institute), Argentina. She has worked on audits and internal control reviews for public and private entities using international frameworks such as COBIT, COSO and the ISO 27000 series. She has participated in the preparation and review of ISACA products and research related to COBIT, privacy and big data. She is the author of the *COBIT Focus* case study "COBIT 5 Applied to the Argentine Digital Accounting System," published in January 2015 *(www.isaca.org/COBIT/Focus).*

Stakeholders expect that businesses create value, but at what cost? In the end, stakeholders and businesses are looking for the same thing: to protect their future.

COBIT® 5 can be used to help enterprises create value for their stakeholders, including the sustainable development concept in their goals and in the governance and management of enterprise IT (GEIT).

SUSTAINABLE DEVELOPMENT AND WHY NOW

The most common definition of sustainable development is from *Our Common Future*, also known as the Brundtland Report.[1] It states that "sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs."[2]

According to the main findings of the United Nations' Sustainable Development in the 21st Century project, at the global level, "the impact of human activity on the environment, the environmental footprint, and carbon emissions and resource consumption from urbanization have been increasing. Many resources on which humanity depends for survival are at risk. Examples of efficiency gains have increased, but, historically, the environmental benefits of improved technology have been insufficient to counterbalance impacts linked with increases in population and affluence."[3]

Technology should and must be an enabler of promoting sustainable development and achieving a "balance among the economic, social and environmental needs of present and future generations…, changing unsustainable practices, and promoting sustainable patterns of consumption and production."[4]

To accomplish these goals, the sustainable use of technology will depend on a global partnership for sustainable development with the active engagement of governments, businesses, civil society and other international organizations, such as the United Nations (UN) or the Organisation for Economic Co-operation and Development (OECD).[5] UN Secretary-General Ban Ki-moon named sustainable development a priority for 2015 at a UN briefing in early January.[6]

WHAT COBIT 5 CAN DO FOR SUSTAINABILITY

One major driver for the development of COBIT 5 includes the need to "provide more stakeholders a say in determining what they expect from information technology (what benefits at what acceptable risk and cost) and what stakeholder priorities are in ensuring that expected value is actually being delivered. Some will want short-term returns and others will want long-term sustainability."[7]

Before determining these priorities, it helps to reconcile statements about progress, gaps and perspectives for sustainable development identified by the main findings of the United Nations' Sustainable Development in the 21st Century[8] project. Its goals and strategies can be adapted as follows:[9]

- Develop integrated national and international strategies and strong institutions that can guide all actors, including the enterprise and its external and internal stakeholders, toward global sustainability.
- Include sustainability into the continuing professional education policy to ensure that sustainability will be considered and put at the center of the decision-making process.
- Reorient IT investment to facilitate sustainable choices and behaviors and to achieve enterprise sustainability goals and IT-related goals.
- Put participation at the heart of decision making at all relevant levels to ensure that all stakeholders' needs are satisfied.
- Monitor, evaluate and assess performance to modify decisions, as needed.

COBIT 5 has embedded the four cross-cutting principles of the UN's sustainable development project to building institutional frameworks that are fit for the challenges of sustainable development:[10]

1. Improve governance. COBIT 5 ensures that all stakeholders are identified and their needs are evaluated in order to determine the enterprise's sustainability goals and its associated IT-related goals.
2. Improve measurement, monitoring and evaluation systems. COBIT 5 uses indicators and can adopt the existing sustainable development indicators as management tools at various levels and in various sectors in order to improve environmental monitoring and information systems at different scales.
3. Assess the roles of public and private actors. COBIT 5 recognizes different stakeholders with different needs and obligations.
4. Increase the resilience of human and natural systems. COBIT 5 suggests stakeholder needs related to sustainability and, thus, allows the use of its goals cascade to ensure the identification of enterprise goals and the evaluation of possible risk that can hurt its achievement. So, the implemented IT process will be capable of delivering outcomes even if the risk factors are materialized and the conditions are not the best.

APPLICATION OF THE COBIT 5 PRINCIPLES

COBIT 5 is based on the assumption that companies exist to create value for their stakeholders, so the governance objective of any company (commercial or otherwise) is the creation of value.

> "The governance objective of any company (commercial or otherwise) is the creation of value."

To apply the first of COBIT 5's principles, Meeting Stakeholder Needs, it is necessary to define the stakeholders and their needs:

- **Stakeholders:**
  - External—Government, regulators, society in general, shareholders, business partners, customers, suppliers, consultants and external auditors
  - Internal—Board, c-suite executives, business executives, business processes owners, IT managers and users, compliance managers, human resources managers, internal auditors, and personnel
- **Stakeholder needs, focusing on five enterprise goals:**[11]
  - Stakeholders' value of business investments, especially for the stakeholders' society
  - Compliance with external laws and regulations focusing on environmental laws and laws dealing with labor regulations in outsourcing arrangements
  - Agile response to changing business environment
  - Skilled and motivated people, recognizing that the success of the enterprise depends on its people
  - Product and business innovation culture, focusing on longer-term innovations

The second COBIT 5 principle, Covering the Enterprise End-to-end, is reflected in the definition of sustainability: needs of present and future generations.

COBIT 5 is aligned at a high level with other relevant standards and frameworks and, therefore, can be the main framework for IT governance and management in an enterprise. This is reflected in principle 3, Applying a Single, Integrated Framework.

Principle 4, Enabling a Holistic Approach, defines seven enabler categories to support the implementation of a global IT governance and management:

1. **Principles, policies and frameworks**—According to OECD Guidelines for Multinational Enterprises, "they (enterprises) should take fully into account established policies in the countries in which they operate, and consider the views of other stakeholders."[12]

   In comparing OECD policies requirements and COBIT 5 IT-related goals, it can be assumed that policies have to take into account and influence decisions related to:
   - Alignment of IT and business strategy to achieving sustainable development. This is important to set

and maintain a governance framework that considers sustainability as a core principle.

- IT compliance and support for business compliance with external laws and regulations and with internal policies and security of information, processing infrastructure and applications. Enterprises should comply with human rights; environmental and social responsibility; natural resources management; information security management; and health, safety and labor regulations. Their own policies must recognize these and strongly avoid exceptions while stipulating the consequences. It is important that educational, awareness and training activities include sustainability compliance issues. This will increase the confidence of stakeholders in the enterprise.
- Managed IT-related business risk and delivery of IT services in-line with business requirements. Sustainability requires identifying risk factors that could limit the possibility of future generations to satisfy their needs and put in place countermeasures to prevent negative impacts. It also requires satisfying business requirements. Important subjects to evaluate are external laws and regulations, best practices and international standards, internal policies, and IT and business performance goals.
- IT agility to respond in a timely and efficient manner to a changing business environment
- Competent and motivated. If personnel understand their responsibility regarding sustainability and respect future generations' rights in the current decision making or performance process, reaching sustainability objectives is most likely.
- Knowledge, expertise and initiatives for business innovation. Innovation allows for sustainability; knowledge, expertise and new initiatives focused on sustainability are critical to innovation in order to discover new and more efficient methods to protect the business environment and IT personnel.

2. **Necessary processes to manage IT activities**—COBIT 5 defines detailed mapping between enterprise goals, IT-related goals and processes. If sustainable businesses require the satisfaction of their needs while considering future needs, enterprises have to ensure that their processes consider good sustainability practices and activities in accordance with laws, regulations and internal policies. Metrics have to include the measurement of this achievement.
3. **Organizational structures**—The hierarchy that defines the responsibilities of each of the business and IT roles. These responsibilities have to consider sustainability issues.
4. **Culture, ethics and behavior of individuals and the company**—These behaviors provide the necessary basis for the company to consider and respect the needs of future generations and the importance of long-term innovation.
5. **Useful information**—This information can be used to make decisions for all stakeholders and demonstrate regulatory compliance to parties, including in legal situations.
6. **Services, infrastructure and applications**—Global Reporting presents a very useful list of relevant sustainability issues for software and services, technology and semiconductors, and telecommunications services.[13, 14, 15] It can be a guide to considering sustainability issues in service-level definition and in the life cycle of services capabilities. Some examples are the energy footprint of data centers, energy efficiency of operations, water consumption, electronic waste (e-waste), end-of-life of products, eco-efficiency and recycling, occupational health and safety risk, and customer privacy.
7. **People, skills and competencies**—Both in business and IT, people and their skills are needed to carry out activities and for decision making and corrective actions, recognizing that the success of the enterprise depends on its people.

The COBIT 5 framework establishes a clear distinction between governance and management (principle 5, Separating Governance From Management). These two disciplines cover different types of activities, require different organizational structures and serve different purposes. Both are necessary to establish and improve sustainable businesses.[16]

CONCLUSION

Sustainability is a stakeholder need and business requirement. But more than anything, it is a human responsibility.

IT plays an important role. It can be a solution or part of the problem, depending on how it is governed and managed.

For business to be sustainable, it has to consider sustainability as a strategic priority; manage risk factors; comply with external laws and regulations; be agile to respond in a timely and efficient manner to a changing business environment; focus innovation on long-term sustainability aspects; plan, build, run and monitor IT as a priority; and invest in business and IT personnel training.

COBIT 5 assists enterprises in achieving this goal.

ENDNOTES

[1] World Commission on Environment and Development (WCED), *Our Common Future*, Oxford University Press, UK, 1987, p. 43, *https://www.iisd.org/sd/*

[2] Bioenergy Promotion, "Paper providing input to the programming of the CENTRAL EUROPE Programme 2014-2020," 23 January 2014, *http://bioenergypromotion.org/bsr/publications/input-paper-central-europe-programme-2014-2020/?searchterm=central%20europe#.VNDglmjF9yw*

[3] United Nations, "Back to Our Common Future. Sustainable Development in the 21st century (SD21) Project. Summary for Policy Makers," 2012, *https://www.globalreporting.org/resourcelibrary/GRIG4-Part1-Reporting-Principles-and-Standard-Disclosures.pdf*

[4] *Ibid*.

[5] OECD, "The Organisation for Economic Co-operation and Development Guidelines for Multinational Enterprises," 2011, *www.ausncp.gov.au/content/publications/reports/OECD_guidelines/OECD_guidelines.pdf*

[6] UN News Centre, "'2015 Can and Must Be Time for Global Action,' Ban Declares, Briefing UN Assembly on Year's Priorities," 8 January 2015, *www.un.org/apps/news/story.asp?NewsID=49752#.VNDhq2jF9yw*

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

[8] *Op cit*, United Nations

[9] *Ibid*.

[10] *Ibid*.

[11] *Op cit*, ISACA

[12] *Op cit*, OECD

[13] Global Reporting, "Software and Services," *https://www.globalreporting.org/resourcelibrary/36-Software-and-Services.pdf*

[14] Global Reporting, "Technology and Semiconductors," *https://www.globalreporting.org/resourcelibrary/37-38-Technology-and-Semiconductors.pdf*

[15] Global Reporting, "Telecommunication and Services," *https://www.globalreporting.org/resourcelibrary/39-Telecommunication-Services.pdf*

[16] *Op cit*, ISACA

Evaluating Cloud Automation as a Service

Andrew Evers is responsible for the architecture and development of Cronacle™, SAP® Business Process Automation by Redwood, Report2Web, Redwood's vertical solutions and RunMyJobs. Evers' career in the software industry spans nearly 20 years and three continents (Australia, Europe and North America). Evers' experience includes product development and management for technologies in the financial services, Internet service provider and music publishing industries. He has worked on JSR 236: Concurrency Utilities for Java™ EE, JSR 237: Work Manager for Application Servers, and has participated as a speaker at JavaOne.

Organizations have already discovered how the cloud can help them share applications and information regardless of the technology in use or their location. Cloud services deliver many kinds of automation to companies every day. The use of process automation as a cloud-based service is an important next step for IT innovation. Implementation is fast, easier to connect across a wide enterprise and immediately scalable. Nevertheless, many organizations face significant challenges when implementing this kind of automation. That is because they still have a major investment in onsite data centers, systems and applications that have not yet or even cannot be migrated to the cloud. These organizations need a solution that delivers as many cloud benefits as possible while retaining necessary onsite systems. Organizations must simultaneously address the monitoring, security and networking challenges introduced by a hybrid solution while they grow and continue to implement efficient, convenient cloud solutions.

CONSISTENCY AND QUALITY

Mobile, informed, self-reliant customers and employees demand control and information at the click of a mouse or the touch of a screen. However, providing this ready access requires IT to manage and coordinate vast complexity. Onsite software solutions, legacy infrastructure, virtual machines, cloud-based applications, shared service centers, outsourced activities and other resources scattered within a wide enterprise landscape need to work together. Reliance on manual oversight alone simply is not enough to support the consistency and quality that complex organizations require.

Manual process steps completed in a complex, hybrid enterprise expose companies to significant auditing and governance risk. They are subject to human error, variable execution and the dangers inherent in the interpretation of potentially inconsistent documentation. Automated processes maintain standard process execution and can easily produce detailed audit trails as a natural by-product of process completion. But how can these processes be effectively automated across all of those technologies, locations and business silos?

In the past, the automation of processes in the enterprise depended on a patchwork of scheduling tools and vigilant manual effort to make sure that silos of technologies, business entities, departments and physical locations worked together to keep core business processes running. Large-scale enterprise resource planning (ERP) solutions promised large-scale automation, but considerable gaps remain in ERP implementations. Outside of ERP systems, multiple applications for activities such as billing, credit card processing, order taking, inventory and business intelligence reporting all work to complete specific tasks. These can be a great challenge to coordinate and execute with precision if that coordination is based solely on manual human oversight. And as a result, they are practically impossible to measure or optimize.

Automation provided as a service from the cloud ensures process consistency, accuracy and quality in a form that is quick to implement, because it does not require additional hardware or infrastructure. When automation is delivered through the cloud, it also makes connecting process steps across technologies and/or silos much easier, too. In the best cases, it helps to bring together onsite, virtual and cloud applications. But there can be big challenges to this approach, particularly in the networking and security efforts required to manage onsite applications from the cloud while retaining simplicity, usability and compliance with organizational security policies.

So, how can these challenges be overcome? A naive approach is to use a cloud service that follows a standard such as Simple Object Access Protocol (SOAP) web services through the customer's firewall. This has the advantage of being standardized and being simple for

the cloud provider to implement. However, this shifts the implementation burden to the customer, for example:

- Many systems (e.g., IBM AS/400 applications, SAP®'s ERP system and most databases) require proprietary clients to connect. While such systems can be exposed via SOAP using middleware, this involves an additional software purchase and often significant development and testing efforts to implement. Even systems that provide a SOAP interface might require a higher-level protocol when users log in, perform an action and log out. Many pass a token during the process.
- Most organizations are reticent to open their firewalls to inbound connections into the DMZ. Direct connections to the internal network are generally completely banned for security reasons. This means the customer needs to open firewall holes, which is time consuming and may be a problem with their security auditor and potentially proxy the protocol in the DMZ. While it is straightforward to proxy Hypertext Transfer Protocol (HTTP) traffic, proprietary protocols may require special software (e.g., SAProuter for RFC, OS/400 Proxy for iSeries) or not support the proxy concept at all.

> "An ideal cloud automation solution needs to provide out-of-the-box solutions."

These issues negate some of the cloud benefits, e.g., a quick project start-up, ease of use and transparent pricing. An ideal cloud automation solution needs to provide out-of-the-box solutions to these issues.

A good cloud automation solution should:

- Support a broad range of managed applications, with minimal (ideally no) middleware requirement
- Use standards-compliant protocols and formats wherever possible, e.g., Transport Layer Security (TLS) for transport security, HTTP and eXtensible Markup Language (XML). Standard protocols and formats are better scrutinized and implemented than proprietary vendor solutions.
- Provide an out-of-the-box connectivity solution that works with organizations' networks and with their security policies (e.g., firewalls, password policies, data integrity, access policies)
- Be simple to install and configure, requiring minimal knowledge about the organizational set-up and/or the cloud provider's application

- Create an automatic long-term audit trail that features detailed proof and documentation of what process steps have been completed, what irregularities have happened and why they occurred

Two important measures of success are how quickly the customer can configure the automation solution to run the first task on a single application and how quickly customers can set up a simple workflow that runs a second task elsewhere based on the successful completion of the first task. Successful cloud services should be able to implement this within a day with minimal customer involvement.

HYBRID COMPLEXITY

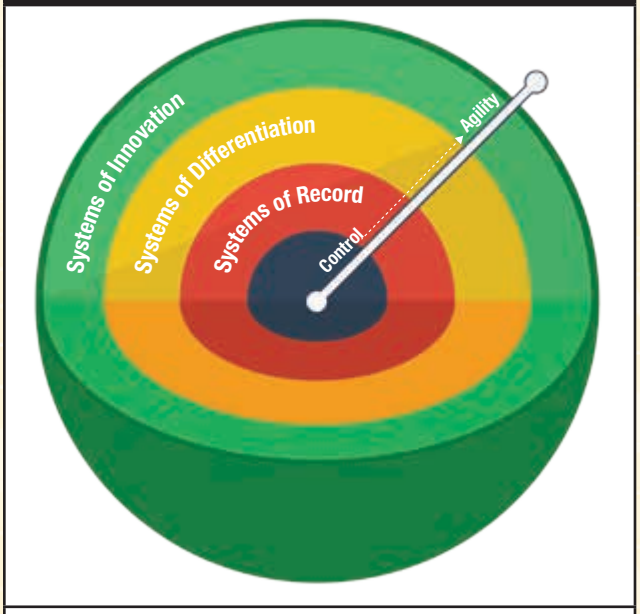
Most organizations manage an extremely complex IT enterprise that includes a mixture of legacy and recent investments and multiple data centers. A typical landscape has some applications in the cloud and some not. Applications may run on platforms not typically available in the cloud. They may also be interfaced to specific hardware, or there may be a regulatory reason why some systems need to remain in-house. Many customer sites are in a transitional stage that is neither completely cloud-based nor completely onsite. Most organizations are somewhere in the process of adopting more cloud-based solutions using what can be described as an "onion model"—multilayer. These companies start by using cloud tools for activities that are outside the core business, while core processes, such as billing or customer service, remain in onsite resources.

For example, an organization might handle sales forecasting and customer relationship management (CRM) using a cloud service. However, it may keep the core accounting and billing processes in-house. The company needs automation to ensure that the CRM and billing systems are suitably synchronized so that sales can see paid orders via CRM and services can schedule appointments for consultants based on accurate customer information. Another

organization might use a cloud-based Payment Card Industry Data Security Standard (PCI DSS)-compliant payment provider to handle payments and make sure that goods sold are, in fact, also paid for, as well as to retrieve and reconcile chargeback and fee information from its payment provider outside its core payment process. Both systems need to be coordinated through process automation.

Frequently, companies initially adopt more agile systems outside of core process activity because they perceive that agility means less control. Process automation as a cloud-based service offers both agility and control (**figure 1**).

Figure 1—Control at the Core



Source: Redwood Software Inc. Reprinted with permission.

This observation coincides with Gartner's recent Pace Layering analysis that describes "systems of record" as the core transactional systems and "systems of innovation" as those that apply to "urgent business needs."[1] Organizations currently appear to be somewhere in the middle of a transformational process, and they need a way to deliver automated processes across both kinds of systems as they continue to evolve. When that automation is delivered as a cloud-based service, it can easily bring together the entire enterprise—both old and new.

Companies continue to face constantly changing security and networking challenges. For any organization, core business processes—no matter where they happen—must be consistently secure and connected. Maintaining both of these requirements is not easy, but there are ways to do so successfully.

SECURITY

Cloud-based services must consider customer concerns about security and privacy. That means using practices such as Defense in Depth, having appropriate security protocols for everything from building security to background checks, and conducting regular internal and external security audits to ensure that these practices are being followed.

The best cloud automation services go to great lengths to always keep customer data safely behind the customer's own firewalls. Only process metadata are transferred to the cloud, keeping all of the automated processes available for use by the customer, but completely unavailable for use by anyone else.

CLOUD AUTOMATION IN PRACTICE

An organization that was interested in cloud automation had several complex revenue-based processes that include applications that are based in different locations and across several different technologies. One common human resource process must regularly fetch data from an online human resource management (HRM) system and compare these data against reports from an onsite payroll application. Initially, these processes could not be connected. One person would gather the HRM information and pass it along to the payroll department for manual comparison. As the company grew and hired more employees, the manual workload expanded. The whole process then became very tedious, plagued by latency and human error. However, by changing to automation as a service from the cloud, administrators were able to connect these disparate steps and automate the entire process end-to-end, saving enormous amounts of time and eliminating the need for constant manual effort.

> "For any organization, core business processes—no matter where they happen—must be consistently secure and connected."

Another organization, a large media company that produces newspapers and magazines in several locations around the world, needed to coordinate local and global processes so that

they could optimize printing production, ad revenue realization and delivery of their publications. With operations and data centers in North America and Europe, making sure that core processes were aligned where possible and locally compliant was a huge task. Errors were common, and the company regularly lost revenue opportunities. Using an automation service provided through the cloud, this company can now orchestrate its core processes on a global scale, monitoring its paper costs, production and distribution. Ad revenue that was previously only calculated and billed once a month is now billed daily, greatly increasing the organization's operational capital.

CONCLUSION

Automated processes provide reliability and consistent results. Automating and truly engineering complex IT tasks across heterogeneous enterprises was once a nearly impossible task. Now, thanks to the cloud, automation can be implemented across the IT landscape safely and transparently as a service, providing coordination and control on a vast scale. This, in turn, has real benefits for monitoring, transparency and governance.

Enterprises that see the value in this approach should look for a service provider that understands the unique security and auditing challenges to get the most of out of the investment. They should evaluate the level of comprehensive service provided as much as the technology that it supports. The right cloud automation service can make the hybrid enterprise's transition to the cloud smooth and successful every time—both onsite and in the cloud.

ENDNOTES

[1] Gartner, "Gartner Says by 2016 the Impact of Cloud and Emergence of Postmodern ERP Will Relegate Highly Customized ERP Systems to 'Legacy' Status," 29 January 2014, *www.gartner.com/newsroom/id/2658415*

Navigating I/O Flows/Networks to Enhance the Governance Management Cycle

Makoto Miyazaki, CISA, CPA, is the manager of the internal audit office of Toukei Computer Company. He was previously an IT auditor at The Bank of Tokyo-Mitsubishi, UFJ.

What constitutes true adoption of COBIT® 5? Is it a minimum condition that at least one principle of COBIT 5 is adopted for true adoption of COBIT 5? To answer this question, one must look at COBIT 5's principles, in other words, its *raison d'être*. The five principles of COBIT 5 are Meeting Stakeholder Needs, Covering the Enterprise End-to-end, Applying a Single Integrated Framework, Enabling a Holistic Approach, and Separating Governance From Management.[1] This article focuses on the Covering the Enterprise End-to-end and the Separating Governance From Management principles, or more specifically, how to enhance alignment of business and IT embodying the concept described by **figures 1, 2** and **3** to address the questions stated previously: Is it a true adoption of COBIT 5 to simply change the processes of COBIT® 4 into those of COBIT 5 as the basis of controls?[2]

FROM COBIT 4 TO COBIT 5

Since October 2012, members of the COBIT® study group (the "group") of the ISACA Tokyo (Japan) Chapter have been meeting to explore case studies on the adoption of COBIT in Japanese enterprises. As part of this effort, the group conducted a web-based survey of all members of the ISACA® chapters in Japan (Tokyo, Osaka, Nagoya and Fukuoka) regarding adoption and usage of COBIT in general and the use of COBIT® 5.

The results of the survey indicated:

- 48 percent of respondents' enterprises have adopted COBIT. Eighty percent of those enterprises have adopted COBIT® 4.1 or an earlier version, and 20 percent use COBIT 5.
- 61 percent of the enterprises have adopted COBIT for complying with domestic and/or overseas regulations such as the US Sarbanes-Oxley Act of 2002 (SOX) or Japan's equivalent, the revision of the Financial Instruments and Exchange Act of 2006 (J-SOX).
- 52 percent of the enterprises that have adopted COBIT® 4.1, COBIT® 4 or a previous version replied "No" or "Don't Know" when asked about upgrading to COBIT 5.[3]

How does one interpret these results? Do enterprises in Japan not understand the value of COBIT 5? The survey suggests that 65 percent of the respondents generally understand all or part of COBIT 5, and one of the most important factors contributing to the popularity of COBIT may be introducing lessons learned from the experiences of other organizations that have adopted and use COBIT.[4] Yet, in Japan, there are very few cases of adoption and usage of COBIT 5, possibly because most Japanese COBIT users depend on the Japanese versions and not much time has passed since the issuing of the Japanese version of COBIT 5.[5]

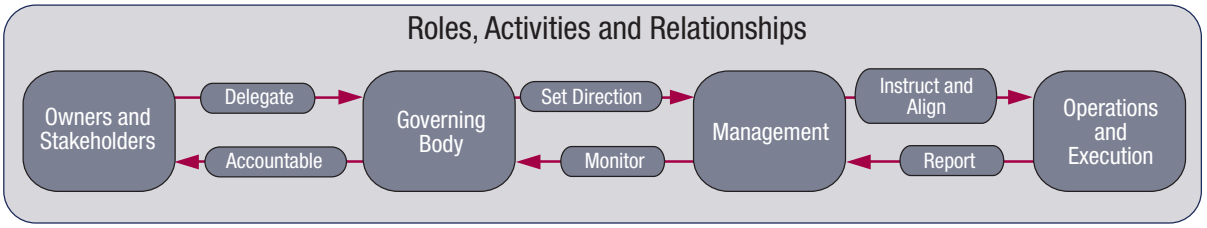
However, there is another issue to be considered: the widespread adoption of COBIT 4.1 and COBIT 4 in Japan, mentioned previously. Quite a few Japanese public enterprises have adopted COBIT 4.1 or COBIT 4 for the establishment of IT general controls in order to comply with the US or Japanese SOX acts. Thus, if an enterprise simply changes COBIT 4.1 or 4 into COBIT 5 as the basis of its controls for complying with regulation, does this mean that it has truly adopted COBIT 5, which intentionally avoids the concept of control objectives? If an enterprise has adopted COBIT 5 without the core of its principles, has it truly adopted COBIT 5? A necessary condition for true adoption of COBIT 5 would be introducing at least one principle of COBIT 5.

Of the five COBIT 5 principles, Covering the Enterprise End-to-end and Separating Governance From Management can be more easily implemented into real organizational structures of enterprises than the others.

RELATIONSHIP OF GOVERNANCE AND MANAGEMENT

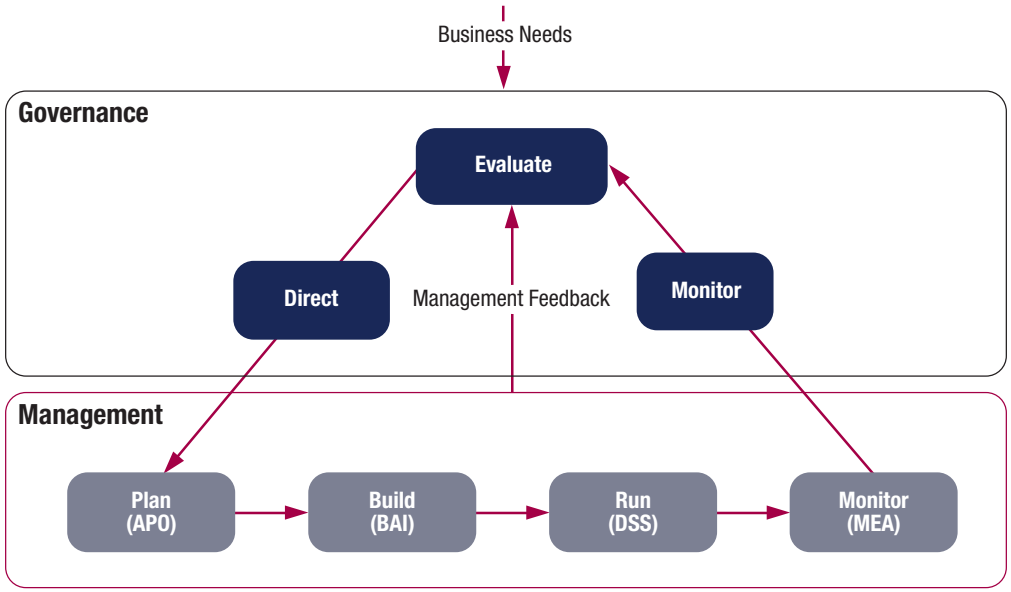
Three COBIT 5 figures illustrate the principles of Covering the Enterprise End-to-end and Separating Governance From Management (**figures 1, 2** and **3**).

Figure 1—Key Roles, Activities and Relationships



Source: ISACA, COBIT 5, 2012, *www.isaca.org/cobit*

Figure 2—COBIT 5 Governance and Management Key Areas

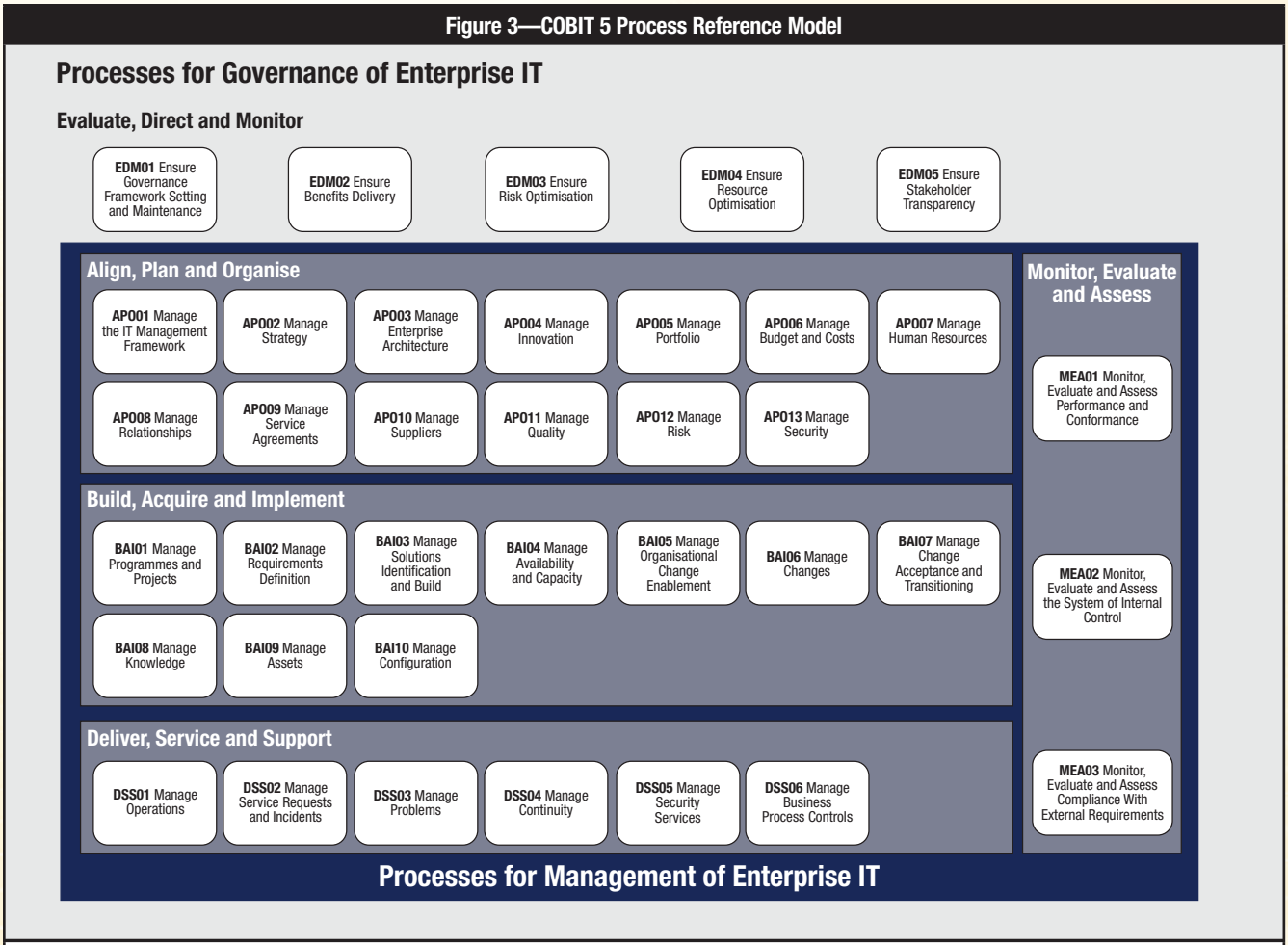


Source: ISACA, COBIT 5, 2012, *www.isaca.org/cobit*

The relationship between governance and management described in these figures is clear and provides a better understanding of the core elements of COBIT 5. So how can one adapt this concept to actual organizational functions? Especially for relationships among processes, **figure 3** reminds users to utilize input/output (I/O) flows/networks. Since its legacy versions, COBIT has explained the relationships among activities in several processes systematically and organically, showing I/O flows/networks, which is one of the strongest points of difference from other frameworks, guidelines or standards. However, COBIT 5 has transformed its I/O flows/networks, changing the unit of I/O relationships from processes in COBIT 4.1 to management practices. Thus, I/O flows/networks to support the governance management cycle must be traced back to processes as outlined in the conceptual model of business case processes in the article "The Business Case as an Operational Management Instrument—A Process View"[6] (the "article") because:

1. The business case processes discussed in the article can be used as a mechanism for improving IT-related investments in enterprises.[7,8] Through assessment of IT-related investments, business case processes are critical management mechanisms for the enhancement of alignment between business and IT, which has been the most important theme of COBIT since its legacy versions and continues in COBIT 5. This is repeatedly emphasized in its principle of Covering the Enterprise End-to-end, and it is elaborated within the goals cascade concept.[9]
2. It is important to grasp the relationships between a business case and COBIT 5 mapping business case processes to *COBIT® 5: Enabling Processes*. Indeed, COBIT 5 does not mention I/O flows/networks, but it presents a starting point for considering the flows/networks.[10]
3. The difficulty of adoption and review of business cases and their accommodation in enterprises provides an opportunity to consider how to recognize to-be activities that promote

Figure 3—COBIT 5 Process Reference Model



Source: ISACA, COBIT 5, 2012, *www.isaca.org/cobit*

and improve critical management mechanisms such as business case processes in the governance management cycle in COBIT 5.[11]

Furthermore, some elements offer double-loop learning, which is recommended for organizational learning in the plan-do-check-act (PDCA) cycle for the achievement of an organization's objectives.[12] Under the concept of double-loop learning, an organization should not only learn direct lessons from the results of its actions for achieving its objectives and take corrective actions for improving its tactics, but also reconsider the probabilities of changes of backgrounds or environments around it and the appropriateness of its strategies, which are the basis of its tactics. The organization should then modify its strategies, organizational structure and critical management mechanism if needed.

If enterprises only rotate the PDCA cycle for improving the individual investment program in which they develop, maintain and review the business cases for them, they are conducting single-loop learning. However, if they also rotate another PDCA cycle at a higher level, reconsider internal and external environments around them and their strategies, and accommodate business case processes, they are conducting double-loop learning.

COBIT 4 and 4.1 insist on a PDCA cycle for IT governance structures as a whole (the plan, build, run and monitor [PBRM] cycle); however, they do not definitively explain the definition of and difference between the two types of PDCA cycles, stated previously, as related to the concept of double-loop learning.

COBIT 5 APO05, which uses the words "business case" most out of all the processes, explains how enterprises accomplish effectiveness of investment programs using business cases. Here one can read a single-loop learning or single PDCA cycle for the assessment of an investment program; however, it may be hard to gain insight into the existence of the concept of double-loop learning with another PDCA cycle for improvement of business case processes for effectiveness of investment programs.

COBIT 5 has evolved the PBRM cycle of COBIT 4 and 4.1, deemed to be mainly applied to the IT division of enterprises, to the governance management cycle of COBIT 5

with more involvement of top management and business-side executives. Thus, the concept of double-loop learning, a PDCA cycle of monitoring backgrounds or environments around enterprises, evaluating their strategies, and directing improvement of critical management mechanisms, such as business case processes by a governing body, are more definitively recognized in COBIT 5's governance management cycle.

Based on these considerations, *COBIT 5: Enabling Processes* and its governance management cycle can be used to promote and improve business case processes. And, in doing so, one takes COBIT guidance beyond its traditional use, from COBIT 4/4.1, as a basis of controls in enterprises, as follows:

1. Trace I/O mappings from the management practices of COBIT 5 mapped from business case practices to relevant processes and management practices in the Evaluate, Direct and Monitor (EDM) domain. Because solving issues such as difficulties of implementation and promotion of a critical management mechanism (i.e., business cases) needs high-level decisions and actions, which are explained in the EDM domain, is one able to find any to-be activities or a PDCA cycle for solving these issues, elements of double-loop learning?
2. Connect the results of the trial by completing the mapping for the governance management cycle, because mapping only management practices does not provide the meaning of a strong point of the governance management cycle—in other words, a principle of COBIT 5 itself. And, these can be considered to-be activities that promote and improve business case processes.
3. Extract recommendations for establishing a governance management cycle using COBIT 5, i.e., adopting COBIT 5.

TRACING INPUT/OUTPUT FLOWS/NETWORKS

The burden for tracing I/O flows/networks of COBIT 5 has been increased drastically. To avoid the burden, the following can be applied:

- Refer to the COBIT 5 management practices that are mapped from business case practices in the article as the "starting practices."
- Trace I/O practices of the starting practices (trace level 1).
- Trace Input practices of the Input practices of the starting practices.
- Omit tracing Input practices of the Output practices of the starting practices.
- Trace Output practices of the Output practices of the starting practices.
- Omit tracing Output practices of the Input practices of the starting practices (trace level 2).
- If reaching columns of "From" for "Inputs" or "To" for "Outputs" in which content is blank or does not describe certain practices, such as "outside COBIT" or "internal," stop tracing.
- Continue tracing until reaching any of the management practices in the EDM domain in one chain of tracing from one starting practice; stop tracing.
- If reaching the management practices that are included in the flows already traced to management practices in the EDM domain, stop tracing to avoid overlapping.

Hereafter, the result of tracing I/O flows/networks in this manner is described and interpreted in the context of improving the business case processes (for more details, see **figures 4** and **5** available online only at *www.isaca.org/journal*).

COMPLETING GOVERNANCE MANAGEMENT CYCLE

As a result, one can find activities at the governance level for promotion and improvement of business case processes in the inputs of management practices of EDM03.03 *Remedial actions to address risk management deviations* and EDM04.03 *Remedial actions to address resource management deviations* by tracing I/O flows/networks from COBIT 5 management practices mapped from business case processes. The processes seem to include not only a PDCA cycle for improvement of activities for individual objectives using business cases, such as risk assessment and resource management for programs, but also a PDCA cycle for improvement of the business case as a critical management mechanism.

However, it is still unclear whether the latter PDCA cycle, or elements of double-loop learning in the governance management cycle, was developed by tracing I/O flows/networks. Nonetheless, there should be a closed governance management cycle where Output flows are connected with Input flows/networks via management practices in the EDM processes, which monitor and evaluate the effectiveness of a critical management mechanism and direct improvement of it.

Then, how should one connect management practices in processes in the EDM domain as destinations for the tracing of I/O flows/networks in the context of promoting critical management mechanisms such as business case processes?

There are several practices of business case process accommodation (BCPA)[13] to accommodate or promote business case processes. However, most of those practices are not mapped to COBIT 5 management practices. Thus, one can map BCPA practices to relevant COBIT 5 management practices to search those that could connect Output and Input flows.

When examining the content of BCPA practices and comparing several management practices of COBIT 5, certain similarities are discovered between BCPA practices and management practices in APO01, including:

- BCPA01: APO01.01 *Define the organizational structure*
- BCPA02-05: APO01.03 *Maintain the enablers of the management system*

- BCPA06: APO01.07 *Manage continual improvement of processes*
- BCPA07: APO01.03 *Maintain the enablers of the management system*
- BCPA08: APO01.04 *Communicate management objectives and direction*
- BCPA09: APO01.07 *Manage continual improvement of processes*

This is illustrated in more detail in **figure 6**.

It is possible to properly map BCPA practices to management practices in APO01, and this is a primary process to be mapped to BCPA practices, although the scope or granularity of the management practices in APO01 may be more or less broad for the special purposes of business case processes. Once there is an understanding of business cases and the business case processes enabler, one can recognize APO01.03 as the core management practice in which issues in promoting business cases converge.

With additional tracing of Input flows from the mapped management practices for confirming the closest EDM process of APO01, it can be seen that EDM01 is the common Input process of APO01.01, APO01.03, APO01.04 and APO01.07 mapped from the BCPA activities noted. EDM01 should be regarded as the process superior to APO01.

As the results of the mapping trial and additional tracing of Input practices from the mapped practices show, one would choose EDM01.01 *Evaluate the governance system*, EDM01.02 *Direct the governance system*, EDM01.03 *Monitor the governance system* and APO01.03 *Maintain the enablers of the management system* as common pieces for connecting Input and Output flows and completing a closed governance management cycle, because the business case can be one of the enablers of the management system.

Adding to EDM01 and APO01 (APO01.03), one can customize a closed governance management cycle as follows (**figures 7** and **8**):

Figure 6—Mapping BCPA Practices to COBIT 5 Practices

Business Case Practices			COBIT 5 Management Practices	
BCPA01	Establishing an adaptable business case approach	Establish an adaptable business case approach according to investment, and accept a growing maturation and granularity through its development and usage.	APO01.01	Define the organizational structure.
BCPA02	Establishing business case templates, training and guidance	Establish standard business case templates and tools, and accommodate training and guidance on what constitutes business case practices and how to employ them adequately.	APO01.03	Maintain the enablers of the management system.
BCPA03	Establishing maximum objectivity in business case usage	Maximize objectivity to support well-founded and comparable decision making without influence from politics, lobbying or institutional powers.	APO01.03	Maintain the enablers of the management system.
BCPA04	Establishing simple and dynamic business case usage	Describe and employ business case practices and their content in a simple, straightforward and dynamic manner to encourage their usage.	APO01.03	Maintain the enablers of the management system.
BCPA05	Establishing business case practices as a standard approach	Establish and evangelize business case practices as a standard way of working.	APO01.03	Maintain the enablers of the management system.
BCPA06	Ensuring business case practice improvements	Ensure business case practice improvements further through experience and continuous learning.	APO01.07	Manage continual improvement of processes.
BCPA07	Ensuring communication and involvement with stakeholders	Ensure clear communication and active involvement with all stakeholders in order to gain insight, commitment and ownership.	APO01.04	Communicate management objectives and direction.
BCPA08	Ensuring stakeholder confirmation	Ensure formal confirmation from relevant stakeholders on the (updated) business case to increase their commitment.	APO01.04	Communicate management objectives and direction.
BCPA09	Evaluating business cases regularly	Evaluate all business case documents in order to make well-founded decisions to approve, continue or stop the investment.	APO01.07	Manage continual improvement of processes.

Source: Makoto Miyazaki. Reprinted with permission.

Figure 7—Input and Output Summary

← Input ←					Starting Practices	→ Output →				
Level 5	Level 4	Level 3	Level 2	Level 1		Level 1	Level 2	Level 3	Level 4	Level 5
				Outside	BCD02 ↓ APO04.02	APO02.01	Internal			
				Outside	BCD04 ↓ APO04.03	BAI03.01	BAI04.03	APO02.02	APO12.01	EDM03.01
										APO01.03
										APO02.02
										Internal
									Internal	
							BAI05.01	Internal		
					BCD09 BCD12 ↓ APO04.04	BAI03.01				
						APO05.03	BAI01.02			
							APO06.02			
							BAI01.06			
							EDM02.01			
							BAI01.04			
						APO06.02	APO05.01			
							APO02.05			
							APO05.03			
							APO07.05			
							BAI03.11			
	EDM03.03	APO12.06	DSS04.02	APO12.02	BCD11 BCM04 ↓ BAI01.10	Internal				
		NIL	DSS05.01			Internal				
			Outside							
			NIL	BAI02.03						
			NIL	APO03.04	BCD12 BCM05 BCPA08 ↓ BAI01.02	APO05.03				
			EDM02.01	APO05.03		APO05.03				
			EDM02.02			APO05.03				
			APO03.01			APO06.05	Internal			
			APO04.04				APO02.02			
			APO06.02							
			APO06.03							
			APO09.01							
			APO09.03							
			BAI01.02							
			EDM01.02	APO07.03						
			EDM04.03							
			BAI08.03							
			BAI08.04							
			DSS04.06							
			Outside							
			APO11.03	BAI05.02						
			BAI02.01							
			BAI02.03							
			BAI03.01							
			BAI03.02							

Figure 7—Input and Output Summary *(cont.)*

← Input ←					Starting Practices	→ Output →				
Level 5	Level 4	Level 3	Level 2	Level 1		Level 1	Level 2	Level 3	Level 4	Level 5
				NIL	BCM01 BCM02 BCM03 BCM04 BCM05 ↓ APO04.06	APO02.04	EDM04.01			
							APO13.02			
							BAI03.11			
						BAI03.02	BAI04.03			
							BAI05.01			
							BAI04.02			
						APO05.04	EDM02.03			
							APO09.04			
							BAI01.06			
							MEA01.03			
				EDM02.03	BCM01 BCM02 ↓ BAI01.06	MEA01.03				
				APO05.02		EDM02.01				
				APO05.03		APO02.04				
				APO05.04		APO05.04				
				APO05.06						
				APO07.05						
				BAI05.04						
				BAI06.03						
				BAI07.05						

Source: Makoto Miyazaki. Reprinted with permission.

Figure 8—Input and Output Summary Revised

← Input ←							Starting Practices	→ Output →						
Level 7	Level 6	Level 5	Level 4	Level 3	Level 2	Level 1		Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7
						Outside	BCD02 ↓ APO04.02	APO02.01	Internal					
						Outside	BCD04 ↓ APO04.03	BAI03.01	BAI04.03	APO02.02	APO12.01	EDM03.01	EDM01.03	EDM01.01
												APO01.03		
												APO02.02		
												Internal		
_											Internal			
									BAI05.01	Internal				
							BCD09 BCD12 ↓ APO04.04	BAI03.01						
								APO05.03	BAI01.02					
									APO06.02					
									BAI01.06					
									EDM02.01	EDM01.03				EDM01.01
									BAI01.04					
								APO06.02	APO05.01					
									APO02.05					
									APO05.03					
									APO07.05					
									BAI03.11					
EDM01.02	AP001.03		EDM03.03	APO12.06	DSS04.02	APO12.02	BCD11 BCM04 ↓ BAI01.10	Internal						
				NIL	DSS05.01			Internal						
					Outside									
					NIL	BAI02.03								

Figure 8—Input and Output Summary Revised *(cont.)*

← Input ←							Starting Practices	→ Output →						
Level 7	Level 6	Level 5	Level 4	Level 3	Level 2	Level 1		Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7
					NIL	APO03.04	BCD12 BCM05 BCPA08 ↓ BAI01.02	APO05.03						
EDM01.02	APO01.03				EDM02.01	APO05.03		APO05.03						
EDM01.02	APO01.03				EDM02.02			APO05.03						
					APO03.01			APO06.05	Internal					
					APO04.04				APO02.02					
					APO06.02									
					APO06.03									
					APO09.01									
					APO09.03									
					BAI01.02									
EDM01.02	APO01.03				EDM01.02	APO07.03								
EDM01.02	APO01.03				EDM04.03									
					BAI08.03									
					BAI08.04									
					DSS04.06									
					Outside									
					APO11.03	BAI05.02								
					BAI02.01									
					BAI02.03									
					BAI03.01									
					BAI03.02									
						NIL	BCM01 BCM02 BCM03 BCM04 BCM05 ↓ APO04.06	APO02.04	EDM04.01	EDM01.03				EDM01.01
									APO13.02					
									BAI03.11					
								BAI03.02	BAI04.03					
									BAI05.01					
									BAI04.02					
								APO05.04	EDM02.03	EDM01.03				EDM01.01
									APO09.04					
									BAI01.06					
									MEA01.03					
EDM01.02	APO01.03					EDM02.03	BCM01 BCM02 ↓ BAI01.06	MEA01.03						
						APO05.02		EDM02.01	EDM01.03					EDM01.01
						APO05.03		APO02.04						
						APO05.04		APO05.04						
						APO05.06								
						APO07.05								
						BAI05.04								
						BAI06.03								
						BAI07.05								

Source: Makoto Miyazaki. Reprinted with permission.

- EDM practices in Output flows (EDM02.01, EDM03.01 and EDM04.01) deliver their activities' results regarding monitoring and evaluation of business case performance to EDM01.03 for monitoring the governance system regarding business cases.
- EDM01.03 delivers its monitoring results regarding the governance system for business cases to EDM01.01 for evaluating the governance system for business cases.
- EDM01.01 delivers its evaluating results regarding the governance system for business cases to EDM01.02 for directing the governance system for business cases.
- EDM01.02 delivers its directions regarding the governance system for business cases to APO01.03 for maintaining business cases as one of the enablers of the management system (transformation from governance into management system).
- APO01.03 delivers its activities and results regarding the enhancement of business cases to EDM practices in Input flows (EDM01.02, EDM02.01, EDM02.02, EDM02.03, EDM03.03 and EDM04.03) for their activities regarding business case usage.

CONCLUSION

COBIT 5 is intended to establish and promote governance of enterprise IT (GEIT), which is the evolution of IT governance—mainly applied only to the IT division of an enterprise—for closer alignment between business and IT. As a result, the enterprisewide PDCA cycle has also evolved to the governance management cycle in COBIT 5. Therefore, true adoption of COBIT 5 inevitably requires the establishment of the cycle in which a governing body should monitor backgrounds or environments around enterprises, evaluate their strategies and direct improvement of critical management mechanisms, such as business case processes, under the concept of double-loop learning.

For adoption of the cycle in practical use, COBIT 5 users need to explore the enabling processes and I/O flows/networks drastically expanded from those of COBIT 4.1 and COBIT 4 in order not to lose their way and to avoid too much burden.

To navigate the deep forest of I/O flows/networks and hunt for treasures in *COBIT 5: Enabling Processes*, the user should:

- Trace I/O flows/networks with the intention of determining objective policies and rules with rationales for solving certain issues that an enterprise is facing. I/O flows/networks are needed for transforming the abstract and conceptual flows/networks into practical value chains for users in the real world

- Customize the content of the relevant processes and I/O flows/networks (as simply as possible) for establishing a governance management cycle for promoting critical enablers of management systems, such as business case processes focusing on APO01.03 and other management practices in APO01

ENDNOTES

[1] ISACA, COBIT 5, USA, 2012, *www.isaca.org/cobit*, p. 13-33
[2] *Ibid*., p. 24, 32-33
[3] The result of the survey on understanding the use of COBIT in Japan. ISACA Tokyo Chapter, September 2014
[4] *Ibid*.
[5] The Japanese version of COBIT 5 was released in January 2013.
[6] Maes, K.; S. De Haes; W. Van Grembergen; "The Business Case as an Operational Management Instrument—A Process View," *ISACA Journal*, vol. 4, 2014, *www.isaca.org/archives*
[7] ISACA, *Enterprise Value: Governance of IT Investment Business Case*, USA, 2008 *www.isaca.org*
[8] ISACA, *The Business Case Guide: Using Val IT 2.0*, USA, 2010, *www.isaca.org*
[9] *Op cit*, Maes, *et al*.
[10] *Ibid*.
[11] *Ibid*.
[12] Argyris, C.; D. Schon; *Organizational Learning: A Theory of Action Perspective*, Addison-Wesley, June 1978
[13] *Op cit*, Maes, *et al.*

Toward a Secure Data Center Model

Brett van Niekerk, Ph.D., is currently employed as a senior information security analyst. He is also an honorary research fellow at the University of KwaZulu-Natal (Durban, South Africa) and is secretary of the International Federation of Information Processing Working Group 9.10 on information and communications technology (ICT) in Peace and War.

Pierre Jacobs is currently employed as a senior security specialist. He has 15 years of experience in the cybersecurity field. His focus and interests are in the security operation center and computer security incident response teams.

According to a survey by Infonetics Research, companies operating their own data centers spent an average of US $17 million on security products in 2013. The top drivers, according to respondents, were the need to protect virtualized servers, upgrade security products to match network performance and obtain new threat protection technologies.

Most modern data centers use virtualized servers. This technology allows multiple servers to run on a single hardware instance. The fact that all server instances, as well as databases, are now flat files dramatically increases the attack vector. It also opens up additional avenues of attack that could not be used in normal data centers (such as dark virtual machines [VMs] and VM sprawl).

It is also true that virtualization drives cloud, and cloud, in turn, enables and drives mobility. This has unique challenges in a military environment or high-security organizational setting where the security requirements are more stringent than those in the majority of organizations in the private sector.

While this article focuses on military-grade data centers, this does not exclude corporate data centers. For certain projects, defense contractors are required to maintain military-grade security for data centers relevant to the project. Many other corporate entities that handle sensitive or critical information or services may also choose to implement military-grade security in their data centers. Such entities may include financial companies and critical infrastructure providers such as telecommunications or power companies. Pharmaceutical companies that conduct research and development can benefit from implementing military-grade data center security to protect their intellectual property. Many of these types of companies are targeted by cyberespionage campaigns using advanced persistent threats (APTs).

DEFINING DATA CENTERS

Gartner defines a data center as a department within a business that houses and maintains its back-end IT systems, mainframe servers and databases. In the past, when centralized IT was the norm, all these systems were housed in one place. With distributed IT models, single-site data centers are still common, but less so. The term "data center," however, is still used to refer to the department that is responsible for these centers, irrespective of how dispersed they are.[1]

Data centers have also been defined as "a parallel and distributed computing system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service level agreements (SLAs) established through negotiation between the service provider and consumers."[2]

The essential characteristics of data centers include:[3]

- **On-demand access**—Users specify the service requirements (e.g., number of central processing units [CPUs] needed, storage requirements), and these are automatically provisioned by the data center.
- **Measured service**—The service requirements stated previously must be measureable so consumers can be charged for resource usage.
- **Network access**—A portal or platform should be supplied to users so they can submit and manage their jobs.
- **Resource pooling**—Resources in the data center can be shared by consumers with different SLAs.
- **Virtualization**—The data center topology should not matter to the user. Applications are easily migrated across hardware platforms as demands and usage change. This happens automatically.
- **Reliability**—Multiple redundant copies of stored content exist.
- **Maintenance**—This is handled by a professional, dedicated IT team.

The two major usage models for data centers are dedicated and shared,[4] with four distinct models—private, community, public and hybrid—as well as three service models: software, platform and infrastructure.[5]

Accenture states that by applying data center and cloud concepts to the military, costs will be reduced and operational efficiencies increased through the consolidation of systems. This also increases the effectiveness of military missions by improving business continuity, mobility and the real-time exploitation of big data.[6]

In a military environment, the data center resources could be shared across the arms of service. There could also be unique requirements such as mobile data centers,[7] as well as the ability to analyze big data in real time to provide near real-time information to commanders, allowing them to make strategic decisions. This also holds true for civilian organizations and businesses requiring business intelligence (BI) in real time.

The military should make use of dedicated data centers, allowing them to remain in control of the information and assets to ensure that their unique security requirements are enforceable and compliance can be assured with military prescripts. The same applies where commercial entities need the same level of protection.

DATA CENTER SECURITY MODEL

Data centers are fundamentally computing resources that are accessed by users. These resources consist of users using an application hosted on a platform via a protocol and transport mechanism to access a service or information offered via an application hosted on a server or mainframe platform, as implied by Cisco and Nutanix.[8, 9]

Considering the previous statement, it is clear that the following logical elements need protection:

- The protocol
- The service, information or application
- The platform (virtual or traditional)

The following physical elements also need protection:

- The network
- Physical security and physical access

All the logical and physical elements, as well as the human element, need to be properly managed according to military governance, risk and compliance (GRC) frameworks.

Using a taxonomy of physical, administrative and technical controls,[10] a proposed framework can be created for the protection of military data centers.

TECHNICAL CONTROLS

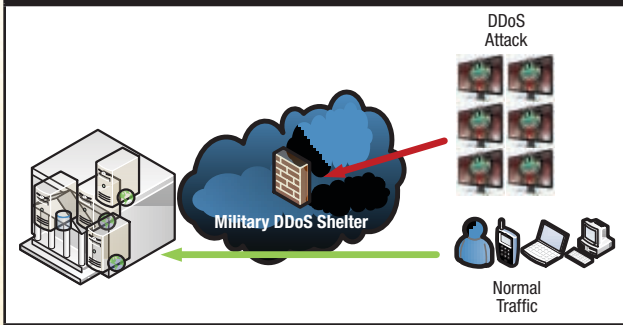
The model proposed in this article is based on the work done at the National Computing and Information Agency (NCIA) in South Korea.[11, 12] The agency has developed an eight-layer defense system to ensure security for the Korean government data center,[13] covering logical and physical elements. This system is called the Advanced National Security

Infrastructure System (ANSIS). It is combined with the eight security dimensions and threat model of the International Telecommunications Union (ITU-T) X.805[14] to provide a comprehensive model to protect the military data center. The ITU-T X.805 security planes and layers are replaced by the logical and physical elements previously identified.

The eight-layer defense model includes:

1. **Distributed denial-of-service shelter**—In a distributed denial-of-service (DDoS) attack, a multitude of compromised computers attacks a single target, causing a breakdown in service.[15] A DDoS defense and shelter system ensures that possible DDoS traffic is identified, and action is taken against the traffic. This typically happens at the virtual layer, and attacks are detected and blocked at the application layer at the system level in the virtual environment.[16] A multilayered approach should be followed, such as the deployment of web application firewalls (WAF), change of service and traffic priorities, caching of content, and identification of false requests from compromised computers launching the attack.[17]
2. **Spam and virus protection**—This service offers protection against malware at the point and network level.
3. **Intrusion protection system**—This system detects possible intrusions or DDoS attacks and alerts the monitoring staff about these attacks.
4. **Intrusion block system**—This system blocks any detected intrusions. This should not only be signature-based, but also include anomaly and heuristic-based detection.
5. **DDoS shield**—This system offers protection against DDoS traffic by redirecting the DDoS traffic to a military DDoS shelter, as depicted in **figure 1**.
6. **Web firewall**—This service protects web traffic (Hypertext Transfer Protocol [HTTP] and Hypertext Transfer Protocol Secure [HTTPS] traffic). This forms part of the protocol stack that needs protection as per the model.
7. **Server security**—This entails traditional server security but also includes virtual element security to threats unique to the virtual environment.
8. **Database (DB) security**—This service protects the service and application elements of the model.

Figure 1—DDoS Shelter



Source: Jacobs and van Niekerk, based on KrCERT/CC, 2012. Reprinted with permission.

CONSOLIDATED FRAMEWORK

The standardization sector of the ITU-T developed a security architecture for systems providing end-to-end communication. This is known as ITU-T X.805 (**figure 2**).

The architecture makes recommendations on providing security in an end-to-end network, and can be applied to various kinds of networks, but independently of the underlying technology.

The architecture identifies eight security dimensions:

- Access control
- Authentication
- Nonrepudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

The security dimensions are applied to three security layers—the application, services and infrastructure security layers—and also to security planes, the management plane, the control plane and the end-user plane.

Figure 3 shows the complete ITU-T X.805 architecture with the security dimensions and the threat model.

In the proposed model, the layers and planes will be replaced with the data center elements identified. In **figure 4**, the ITU-T X.805 security layers and planes are replaced by the elements applicable to data centers.

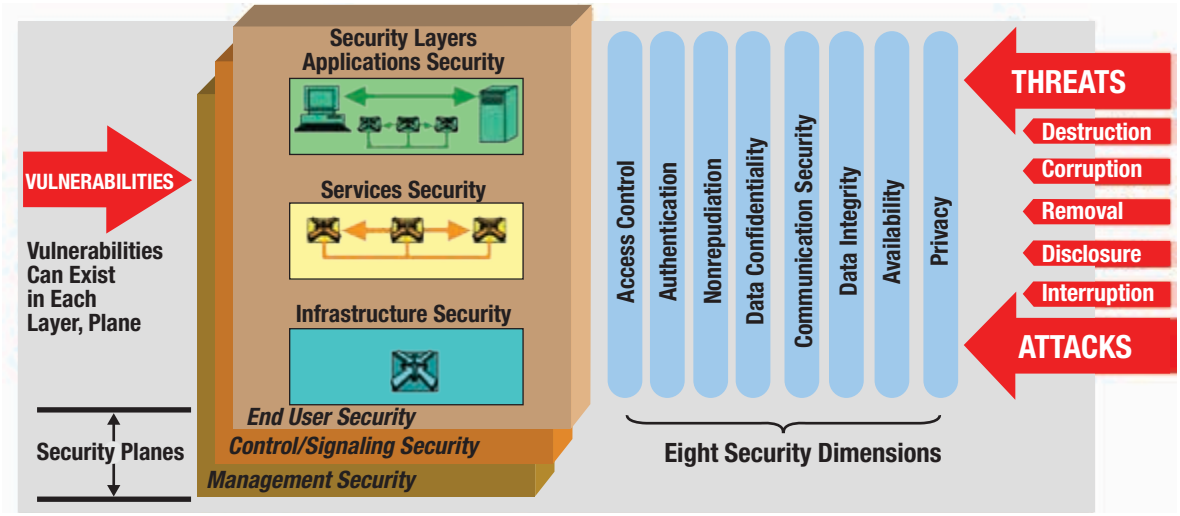
Considering the taxonomy used of physical, technical and administrative controls, it can be seen that the eight layers of the defense model fall into the technical category, and the GRC element forms part of the administrative controls. The

Figure 2—Sample Technical Control Mapping to ITU-T X.805 Security Dimensions and Eight-layer Defense

	Access Control	Authentication	Nonrepudiation	Data Confidentiality	Communication Security	Data Integrity	Availability	Privacy
Physical environment								
Protocol				Web firewall	Web firewall	Web firewall	DDoS shelter	
Network	Intrusion protection/ prevention						DDoS shelter	
Service, application or information				Web firewall/ DB FW		Web firewall/DB FW	DDoS shelter	Web firewall/ DB FW
Platform	Server security	Server security	Server security	Spam and virus protection/ Server security		Spam and virus protection/ server security	DDoS shelter	Server security

Source: Jacobs and van Niekerk. Reprinted with permission.

Figure 3—ITU-T X.805 Security Architecture

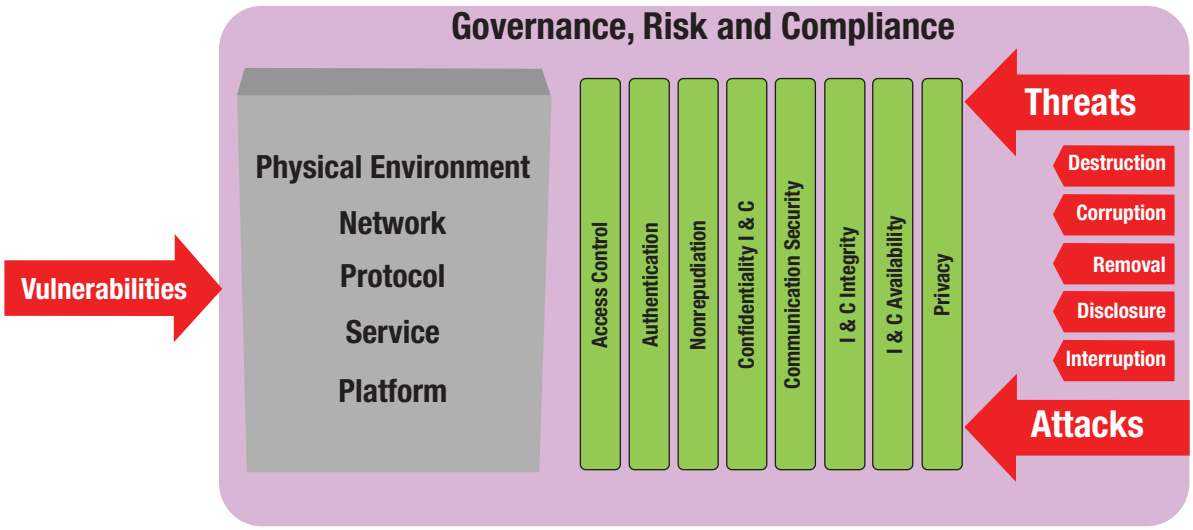


Source: International Telecommunication Union, "ITU-T X.805 Security Architecture for Systems Providing End-to-end Communications," 2003, *www.itu.int/rec/T-REC-X.805-200310-I/en*. Reprinted with permssion.

eight-layer defense model will be further augmented with additional technical controls to ensure that all ITU-T X.805 security dimensions are addressed.

It is clear from looking at **figure 2** that gaps exist when using the model. All of the blocks would have to be filled with defense mechanisms according to military standards, such as the US Department of Defense (DoD) Manual 5105 21 volume 2,[18] which deals with physical security and visitor control, or other requirements as mandated in the South African Department of Defence Instruction (DODI) and/or Defence Information and Communication Architecture (DICTA). However, what is clear is that all eventualities are addressed from a security perspective.

Figure 4—Proposed Data Center Security Model



Source: International Telecommunication Union, ITU-T X.805 Security Architecture for Systems Providing End-to-end Communications, 2003, *www.itu.int/rec/T-REC-X.805-200310-I/en*. Reprinted with permssion.

ADMINISTRATIVE CONTROLS

From an administrative control perspective, all elements are covered by military GRC frameworks. Alternatively, a standard such as ISO/IEC 27001:2005[19] could be used to ensure that all administrative aspects are covered.

ISO/IEC 27001:2005 consists of 11 security control clauses containing 39 security categories. Each category, in turn, consists of a single control objective that contains, in most cases, high-level administrative controls.[20]

In many cases, the administrative controls are supported by technical controls. It is worth mentioning that only controls applicable or required by the military should be implemented. These controls should be determined by following a risk management process such as that described in ISO/IEC 2005:2011[21] or ITU-T X.1055 *Risk management and risk profile guidelines for telecommunication organizations*.[22]

The complete model can be depicted with ISO/IEC 27001:2005 serving as guidance for administrative controls and ITU-T X.805 serving as guidelines for technical controls.

RATIONALE FOR SELECTION OF THE STANDARDS

A deliberate decision was made to limit the number of standards in the model and avoid an alphabet soup approach. The reasons for this decision included:

- A model based on many standards requires a very large amount of effort and expense to maintain and keep current as the standards involved get updated and change over time.
- Human resources that are familiar with a wide variety of standards are difficult to find and keep.
- If the effort to keep the model up to date is not expended, the framework may become less relevant over time.
- The approach taken by different standards bodies toward network security may change in the future and result in potential inconsistencies in the model.
- Limiting the number of standards used in the model, therefore, provides for a lean approach, which requires less effort and expense to maintain and is less likely to become inconsistent over time.
- ITU and ISO standards were chosen as the baseline standards for the model.

ITU and ISO standards were chosen as baseline standards for a number of reasons:

- ITU security standards cover eight security dimensions as opposed to only the confidentiality, integrity and availability triad.
- ISO security standards are the most widely accepted and used standards globally.

- The ITU and ISO work together and have standards equivalence, e.g., many ITU X.800 series and ISO 10181-x series standards are verbatim copies of each other.
- ISO standards are usually accepted as-is by the South African Bureau of Standards as South African National Standards (SANS) and can be replaced as shown in **figure 5**.
- ITU-T X.805 *Security architecture for systems providing end-to-end communications* was selected as the basis for the model since it was most relevant for the purposes of the model.
- ITU-T X.805 will be used with consideration of ITU-T Y.2701, which looks at applying X.805 to next generation networks (NGNs).
- The use of the ITU X.805 standard enables the use of other ITU X and Y series standards that address various aspects of network security. The reason is that the standards form a family and were designed to be used with each other.
- This ensures consistency and ease of maintenance of the model in the future, because it is extremely unlikely that ITU will update any particular standard in a way that is inconsistent with the others.
- The ITU standards, however, do not apply to every aspect of data center security. Where something is not covered, ISO standards, DODIs or DICTAs are used. As a last resort, other applicable standards are used.

Other standards and frameworks are not applicable. For example, COBIT® would not be applicable because it focuses on processes and does not address technical details in-depth. Similarly, the Information Technology Information Library (ITIL) focuses more on operations and addresses effectiveness and efficiency, not information security in-depth.

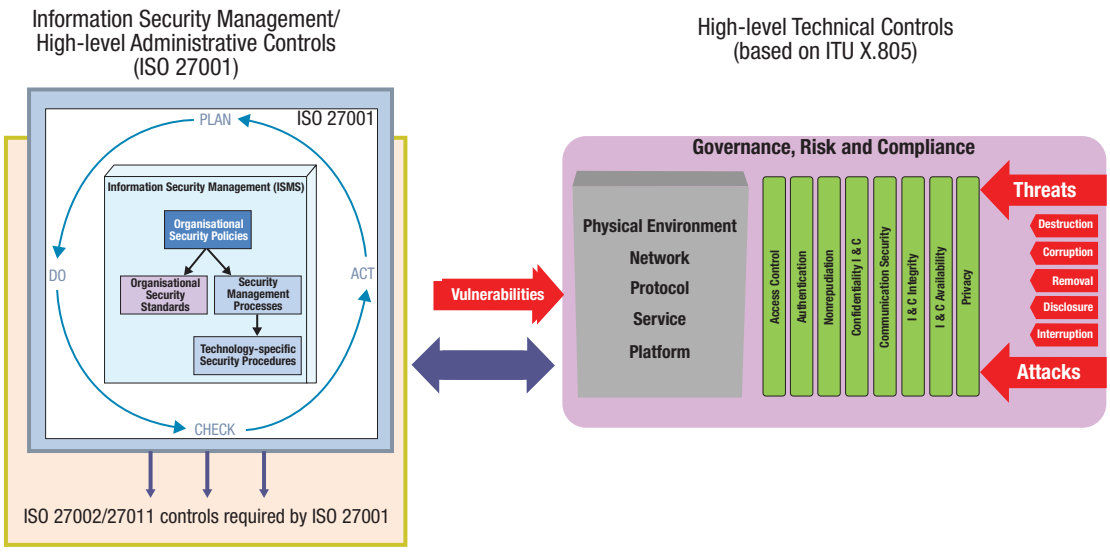
The different standards and frameworks and their relation to information security are depicted in **figure 6**.

RISK-BASED MODEL

It was decided to use the ISO/IEC 27005:2011 *Information security risk management* standard[23] as opposed to ITU-T X.1055 *Risk management and risk profile guidelines for telecommunication organizations*.[24] ISO/IEC 27005 is based on the generic ISO/IEC 31000 *Risk management—Principles and guidelines*[25] but tailored to, and aimed at, information security risk management. ITU-T X.1055 is aimed at telecommunications organizations.

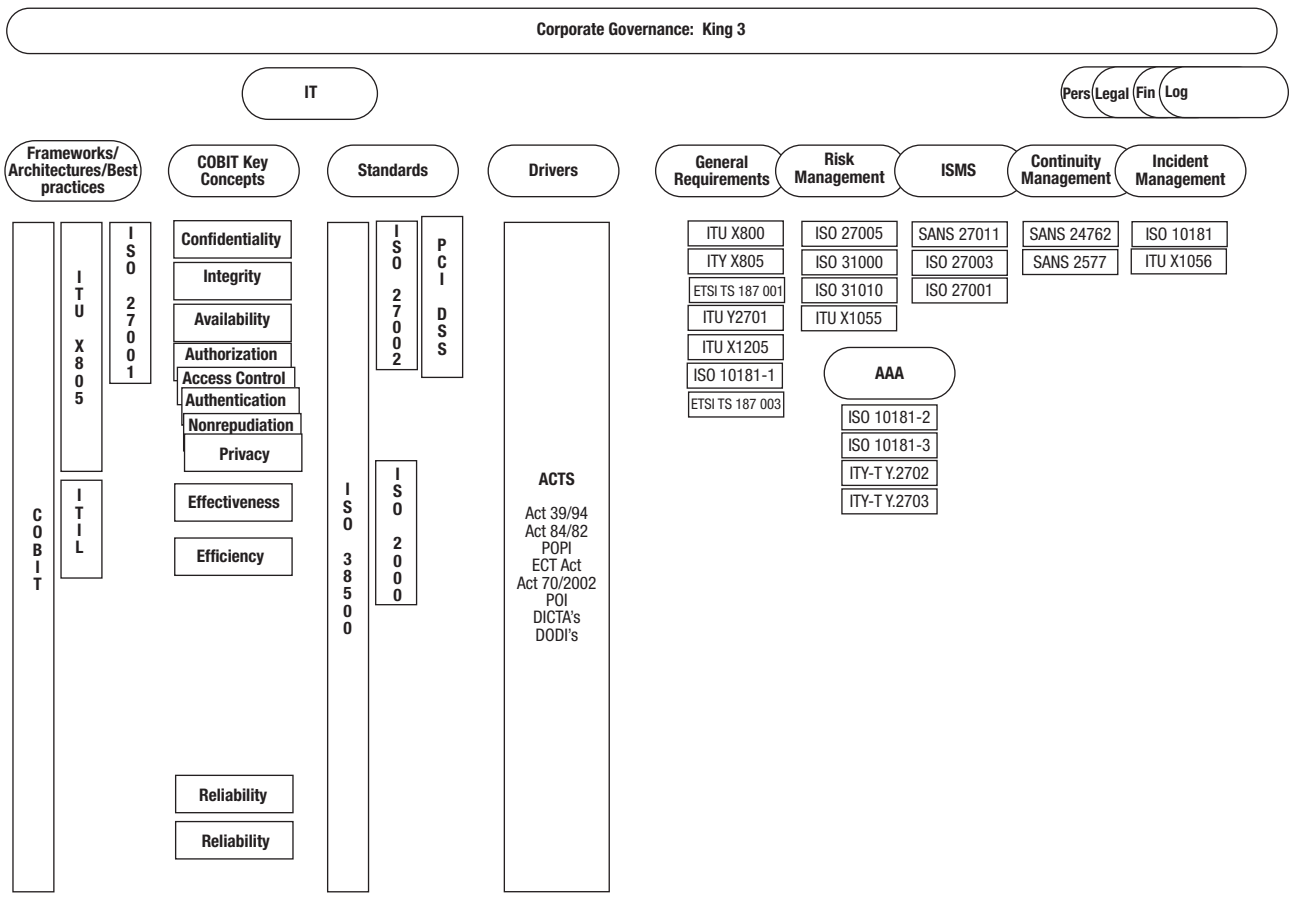
ISO/IEC 27005:2011 also augments and compliments ISO/IEC 27001:2005,[26] which is used for identifying and defining administrative controls. The ISO/IEC 27005 standard

Figure 5—Consolidated Model



Source: International Telecommunication Union, ITU T X.1055 *Risk management and risk profile guidelines for telecommunication organizations*, 2008, *www.itu.int/rec/T-REC-X.1055-200811-I/en*. ISO/IEC, ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*, 2005, *www.iso.org/iso/catalogue_detail?csnumber=42103*. Reprinted with permission.

Figure 6—Relation of Different Standards and Frameworks to IT Key Concepts



Source: Jacobs and van Niekerk. Reprinted with permission.

also closely correlates with the US National Institute of Standards and Technology (NIST) SP 800-39 Managing Information Security Risk, which was developed for the US DoD. ISO/IEC 27005:2011 does not cover organizational risk, whereas NIST SP 800-39 does. The correlation between the NIST SP 800-39 and ISO/IEC 27005:2011 processes is illustrated in **figure 7**.

The ISO/IEC risk management process is cyclical and consists of the following processes:

- Context establishment
- Risk assessment
- Risk treatment
- Risk acceptance
- Risk communication and consultation
- Risk monitoring and review

Figure 7—Correlation Between NIST SP 800-39 and ISO/IEC 27005:2011

NIST SP 800-39	ISO/IEC 27005:2011
Risk framing	Context establishment
Assessing risk	Risk assessment
Risk response	Risk treatment
Risk monitoring	Risk monitoring and review

Source: National Institute of Standards and Technology, SP 800-39, USA, March 2011, *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.* Reprinted with permission.

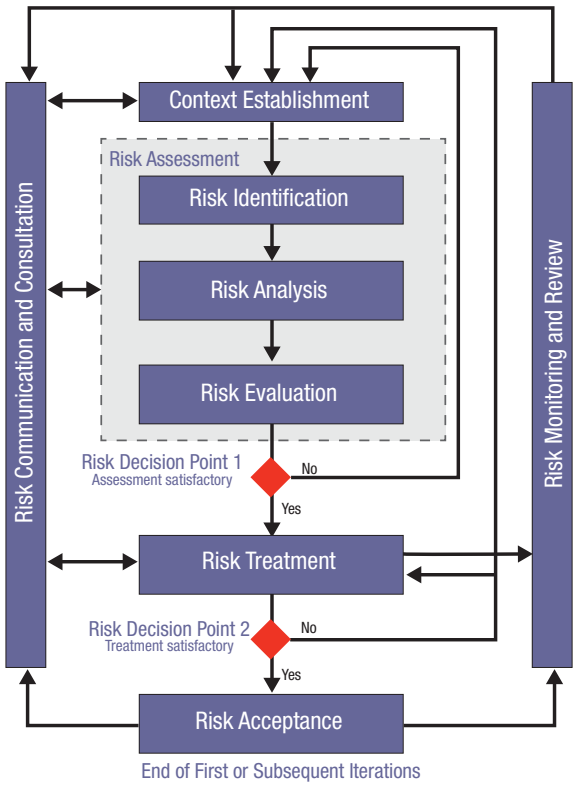
The processes are illustrated in **figure 8**.

The ISO/IEC 27005:2011 risk management process should be applied as part of the ISO 27001:2005 administrative controls and should encompass the secure data center model. The ITU-T X.805 security domains and threat model should be used as technical input to the risk management process for the identification of vulnerabilities and threat sources. The consolidated model is depicted in **figure 9**.

CONCLUSION

The proposed model caters to all aspects of data center security, making use of deeply entrenched and tested frameworks and architectures. The ITU-T X.805 focus is specifically on information security from a technical perspective, and ISO/IEC 27001:2005 is from an information security administrative perspective. ISO/IEC 27005:2011 is used as a risk management model. Using these frameworks provides a baseline for military-grade data center security and provides an internationally recognized best practice against which to implement and audit risk and security requirements. This level of security can aid enterprises in protecting their sensitive information from espionage and other malicious activities.

Figure 8—ISO/IEC 27005:2011 Risk Management Process



Source: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27005:2011, *Information technology—Security techniques—Information security risk management*, 2011, *www.iso.org/iso/catalogue_detail?csnumber=56742*. Reprinted with permission.

ENDNOTES

1 Gartner IT Glossary, "Data Center," 2013, *www.gartner.com/it-glossary/data-center/*

2 Buyya, I. B. R.; C. Yeo; S. Venugopal; J. Broberg; "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," *Future Generation Computer Systems*, vol. 25, iss. 6, June 2009, p. 599-616

3 Yang, Li; "Network-aware Job Placement in Data Center Environments," University of Calgary, 2014

4 Abts, D.; B. Felderman; "A Guided Tour Through Data-center Networking," *ACM Queue*, vol. 10, 3 May 2012, p. 10-23, *http://queue.acm.org/detail.cfm?id=2208919*

5 Mell, P.; T. Grance; "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, USA, September 2011, *http://csrc.nist.gov/publications/PubsSPs.html#800-145*

6 Accenture, "A New Era: Cloud Ushers in Insight-driven Defense," 2013, *www.accenture.com/SiteCollectionDocuments/PDF/Accenture-A-New-Era-Cloud-Ushers-in-Insight-Driven-Defense.pdf*

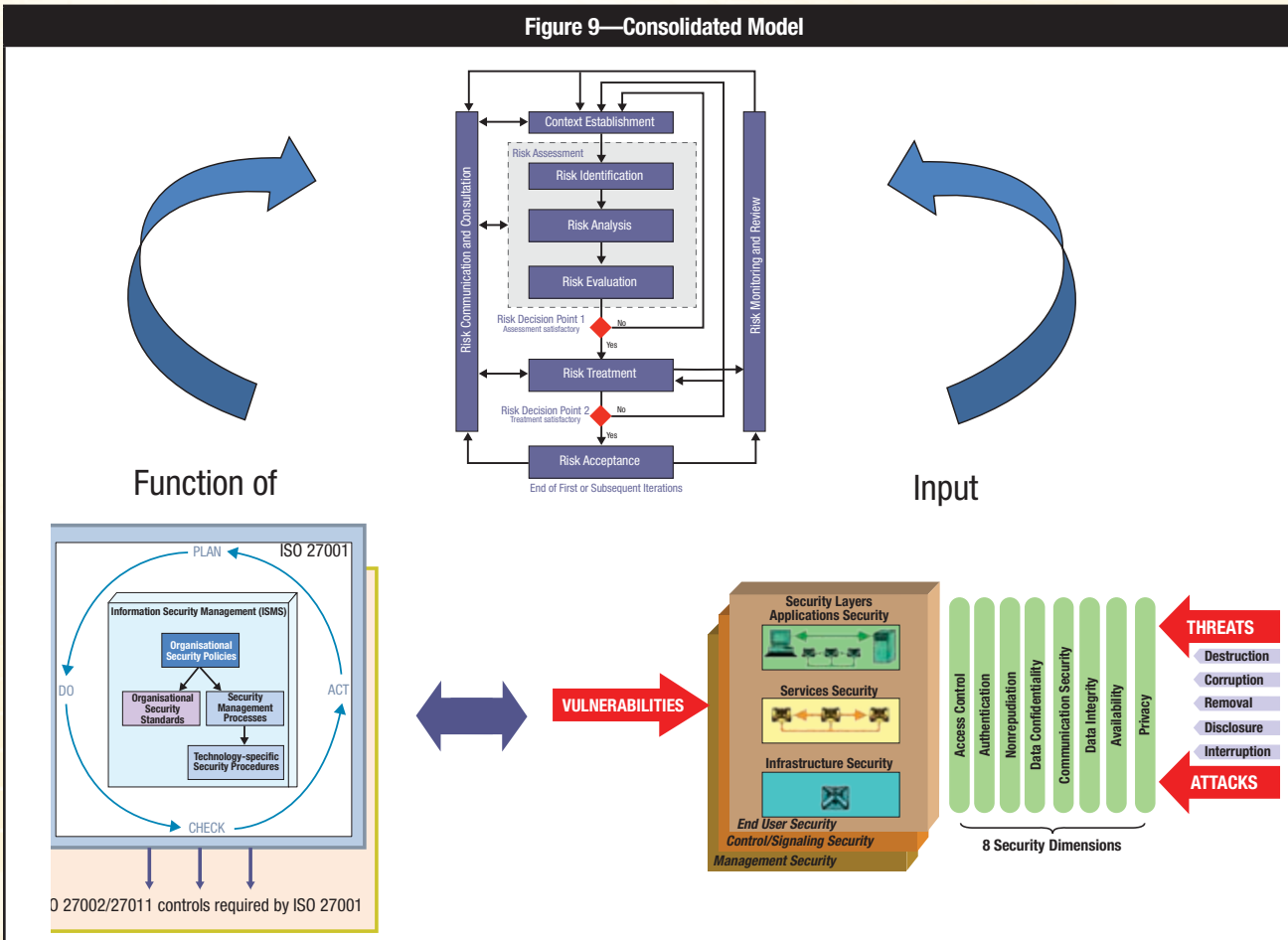
7 Wait, P.; "Dell Launches Military Data Centers-In-A-Box," *InformationWeek*, 18 July 2012, *www.informationweek.com/architecture/dell-launches-military-data-centers-in-a-box/d/d-id/1105382*

8 Cisco Systems, "Data Center Architecture Overview," 2014, *www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_1.html*

9 Nutanix, "8 Strategies for Building a Modern Datacenter," 2013, *http://go.nutanix.com/rs/nutanix/images/WP_8_Strategies_for_Building_a_Modern_Datacenter.pdf*

10 Tipton H. F.; M. Krause; *Information Security Management Handbook, 5th Edition*, CRC Press, 2012, p. 179-182

Figure 9—Consolidated Model



Based on: ITU-T X.805, *www.itu.int/rec/T-REC-X.805-200310-I/en. ISO/IEC 27001:2005, www.iso.org/iso/catalogue_detail?csnumber=42103. ISO/IEC 27005:2011, www.iso.org/iso/catalogue_detail?csnumber=56742.* Reprinted with permission.

11 Chernicoff, David; "Korea Sets the Standard for Government Datacenters," ZDNet, 30 December 2011, *www.zdnet.com/blog/datacenter/korea-sets-the-standard-for-government-datacenters/1161*

12 National Computing and Information Agency (NCIA), Korea, *www.ncia.go.kr/eng/about/about_01.jsp*

13 NCIA, "Security," *www.ncia.go.kr/eng/key/key_02.jsp*

14 International Telecommunication Union, "ITU-T X.805 Security Architecture for Systems Providing End-to-end Communications," 2003, *www.itu.int/rec/T-REC-X.805-200310-I/en*

15 Rouse, M.; "Distributed Denial-of-service (DDoS) Attack," SearchSecurity, May 2013, *http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack*

16 KrCERT/CC, DDoS Shelter Service, Korea, *http://eng.krcert.or.kr/service/ddos.jsp*

17 *Ibid.*

18 US Department of Defense, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," no. 5105.21, vol. 2, 19 October 2012, *www.dtic.mil/whs/directives/corres/pdf/510521m_vol2.pdf*

19 International Organization for Standardization (ISO)/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*

[20] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27002:2005, *Information technology—Security techniques—Code of practice for information security management*," 2005, *www.27000.org/iso-27002.htm?*

[21] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27005:2011, *Information technology—Security techniques—Information security risk management*, 2011, *http://www.iso.org/iso/catalogue_detail?csnumber=56742*

[22] International Telecommunication Union, ITU T X.1055, *Risk management and risk profile guidelines for telecommunication organizations*, 2008, *www.itu.int/rec/T-REC-X.1055-200811-I/en*

[23] International Organization for Standardization (ISO), ISO/IEC 27005:2011 *Information security risk management*, 2011, *www.iso.org/iso/catalogue_detail?csnumber=56742*

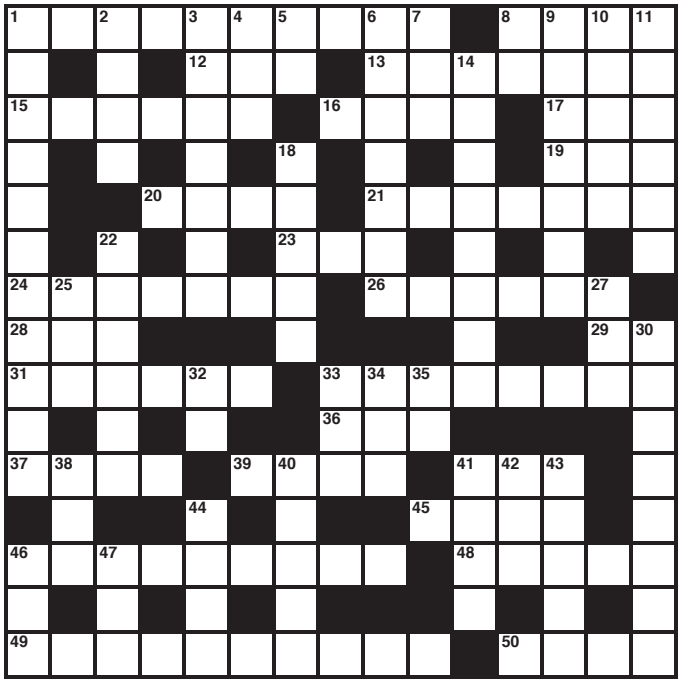
[24] International Telecommunication Union, ITU T X.1055, *Risk management and risk profile guidelines for telecommunication organizations*, 2008, *www.itu.int/rec/T-REC-X.1055-200811-I/en*

[25] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO 31000, *Risk management*, 2009, *www.iso.org/iso/home/standards/iso31000.htm*

[26] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27005:2008, *Information security risk management*, 2011, *www.iso.org/iso/catalogue_detail?csnumber=42107*

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1 Boundaries or entry points to new experiences
8 One of ISACA's information security qualifications
12 ___ negotiable
13 Stone that was the key to understanding Egyptian hieroglyphs
15 The last word in a famous Pittsburgh university with a highly ranked computer school
16 ____ desk
17 Network where computers are distantly connected, abbr.
19 Scrap of food
20 Value ____ (extra products or services making the overall offering more valuable)
21 More established and proven
23 Note from one in the red
24 Coordinated with other forces or interests
26 Standard for the credit card industry, abbr.
28 More in Spanish
29 Eric Holder's position
31 Scope
33 See 41 down
36 Pascal-based language
37 Think ___
39 Virtual space where software can be tested securely (goes with 41 across)
41 See 39 across
45 Visit
46 Theoretical model
48 Makes a sketch or outline
49 The learnable skill of deal making
50 Terrorist group making cyberthreats

DOWN

1 Trait that is hard to change
2 Function
3 Heroic defender of privacy rights or traitor?
4 Part of a British title, for short
5 Operating
6 Invent (2 words)
7 Spanish sun
8 This, in French
9 Good motto for a tech company? (2 words)
10 It may be fixed or blank
11 Often repeated phrase
14 Observing
18 Something said in confidence
22 The ability to do this well is one of the top communication skills
25 Undisciplined
27 Droop
30 Brilliant minds
32 Doctor created by Ian Fleming
33 Linked computers acronym
34 Include
35 Sodium symbol
38 Payment percentage, for short
40 Take on as new policy
41 Nonverbal cues (goes with 33 across)
42 Jointly owned
43 Diagnostic aids
44 Governance of enterprise professional, abbr.
46 Enthusiast
47 Summer month, for short

(Answers on page 58)

CPE Quiz

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

Take the quiz online:

QUIZ #160

Based on Volume 1, 2015—Analytics and Risk Intelligence

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

TRUE OR FALSE

SEHGAL ARTICLE

1. Information security is possibly one of the most vibrant areas in the IT sector, in which technical innovation constantly paves the way to defeat emerging threats.
2. The attempt to execute the threat in combination with the vulnerability is called fracking.
3. Due to a sharp increase in the number of published vulnerabilities in 2013-14, many organizations had to set up emergency response teams to respond to cyberthreats and incidents.
4. Cyberthreat assessment is currently recognized in the industry as red hatting, which is the practice of viewing a problem from an adversary's or competitor's perspective.
5. To make the organization more resilient against cyberthreats, focus should be kept on addressing the root cause and not merely fixing the security flaws discovered during the exercise.

LUU ARTICLE

6. The US Government Accountability Office (GAO) cites that from 2006 to 2012, the number of cyberincidents reported by federal agencies increased by 782 percent.
7. In November 2014, the US Office of Management and Business (OMB) issued memorandum M-14-03 requiring all federal departments and agencies to establish an information security continuous measuring (ISCM) program.
8. The Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) reference architecture consists of a sensor subsystem, a database/repository subsystem, an analysis/risk-scoring subsystem, and a presentation and reporting subsystem.
9. An ISCM solution has a broad set of stakeholders (e.g., chief information officers [CIOs], chief information security officers [CISOs], program managers, system administrators), and they all need to be trained to properly operate and use the capabilities provided.

VLACHOS ARTICLE

10. Ninety-two percent of data breaches are caused by employee error, and more than 76 percent of data breaches involve stolen credentials.
11. User activity monitoring solutions follow authenticated users as they travel the network, access files and use applications while also recording every keystroke, preference and option they select.
12. Organizations need a policies and procedures document that clearly defines what the company monitors, how that information is used and what constitutes acceptable behavior.
13. In communicating with employees and trusted third parties, communication is not essential to ensure that they fully understand corporate initiatives, policies or procedures.

HENDERSON, SHEETZ AND WALLACE ARTICLE

14. A software metric provides a quantitative indication of some attributes of software, such as size, complexity or quality. Examples of software metrics include function points, cyclomatic complexity and source lines of code.
15. Resistance to software metrics has resulted in inappropriate use and high failure rates for software metric initiatives. More than 89 percent of software metric initiatives fail within the first 12 months.
16. The potential of software metrics to mitigate risk during the software development process, coupled with the IS auditor's responsibility to ensure that the development process is timely and cost-effective, makes the appropriate use of software metrics a concern for IS auditors.
17. IS auditors should ensure that members of a development team appreciate the value of software metrics. IS auditors can accomplish this task via observation, inquiries, and taking an active, yet independent, role in the systems development process.
18. Efforts should not only be directed toward education and training, but also toward developing software metrics that more practitioners perceive as predictive and prescriptive.

ISACA Journal

CPE Quiz

Based on Volume 1, 2015—Analytics and Risk Intelligence

Quiz #160 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC #_____

Quiz #160

True or False

SEHGAL ARTICLE

1._____

2._____

3._____

4._____

5._____

LUU ARTICLE

6._____

7._____

8._____

9._____

VLACHOS ARTICLE

10._____

11._____

12._____

13._____

HENDERSON, SHEETZ AND WALLACE ARTICLE

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.

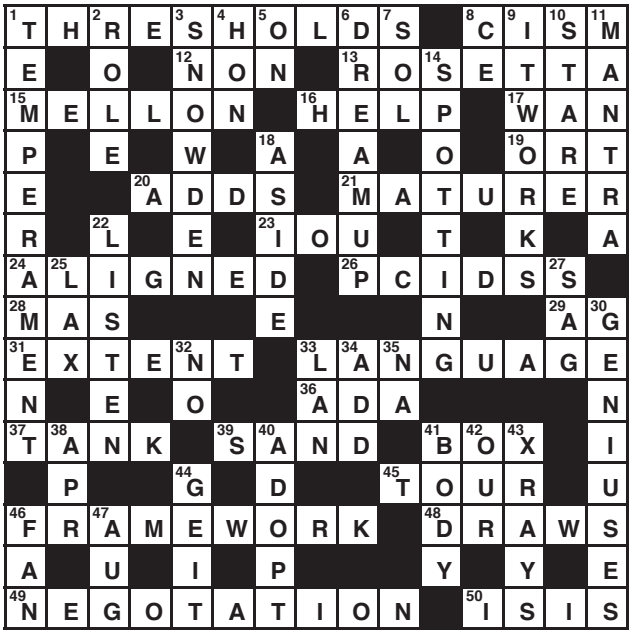
Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

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) $80.00
All international orders: one year (6 issues) $95.00. Remittance must be made in US funds.

ISSN 1944-1967

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

INSIGHTS AND RESOURCES FOR THE CYBERSECURITY PROFESSIONAL

FEATURED CATEGORY:
CYBERSECURITY BOOKS BY ISACA®

- CSX Cybersecurity Fundamentals Study Guide
- Implementing the NIST Cybersecurity Framework
- Advanced Persistent Threats: How to Manage the Risk to Your Business
- Transforming Cybersecurity
- Responding to Targeted Cyberattacks
- Securing Mobile Devices

CSX™
CYBERSECURITY NEXUS

ANNOUNCING NEW ONLINE DATABASE SUBSCRIPTIONS FOR CISA AND CISM

NOW AVAILABLE IN ISACA'S BOOKSTORE—CISA AND CISM ONLINE DATABASE SUBSCRIPTIONS!

CISA®
Certified Information Systems Auditor®

CISM®
Certified Information Security Manager®

Need help preparing for your CISA® or CISM® certification exam?
ISACA study resources can help you prepare to finish strong.

Browse over 450 publications featuring the latest research and expert thinking on standards, best practices, emerging trends and more at ***www.isaca.org/bookstore-Jv3***

FEATURED CATEGORY:

CYBERSECURITY

Cybersecurity Fundamentals Study Guide by ISACA

Product Code: CSXG1
Member/Nonmember:
$45.00/$55.00

eBook Product Code: WCSXG1
Member/Nonmember:
$45.00/$55.00

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.

Implementing the NIST Cybersecurity Framework by ISACA

Product Code: CSNIST
Member/Nonmember:
$35.00/$60.00

eBook Product Code: WCSNIST
Member/Nonmember:
Free/$60.00

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.

Transforming Cybersecurity by ISACA

Product Code: CB5TC1
Member/Nonmember:
$35.00/$60.00

eBook Product Code: WCB5TC1
Member/Nonmember:
FREE/$60.00

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.

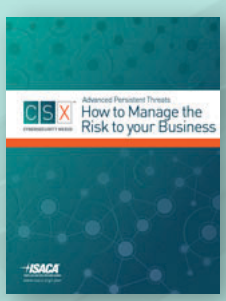
This publication applies the COBIT® 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents,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

2 EASY WAYS TO ORDER:

1. Online—Access ISACA's bookstore online anytime 24/7 at ***www.isaca.org/bookstore-Jv3***

2. Phone—Contact us by phone M–F between 8:00AM – 5:00PM Central Time (CT) at 847.660.5650

Advanced Persistent Threats: How to Manage the Risk to Your Business by ISACA



Product Code: APT
Member/Nonmember:
$35.00/$60.00

eBook Product Code: WAPT
Member/Nonmember:
Free/$60.00

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.

Responding to Targeted Cyberattacks by ISACA

Product Code: RTC
Member/Nonmember:
$35.00/$59.00

eBook Product Code: WRTC
Member/Nonmember:
Free/$59.00

The threat environment has 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

Securing Mobile Devices by ISACA

Product Code: CB5SMD1
Member/Nonmember:
$35.00/$75.00

eBook Product Code: WCB5SMD1
Member/Nonmember:
Free/$75.00

Securing Mobile Devices should be read as a companion to 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 devices 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.

NEW PUBLICATIONS

ISACA®
Trust in, and value from, information systems

Announcing New Online Database Subscriptions for CISA and CISM—Now Available in ISACA's Bookstore!

CISA Online Database—12 month subscription

Product Code: XMXCA15-12M
Member/Nonmember: $185.00/$225.00

CISM Online Database—12 month subscription

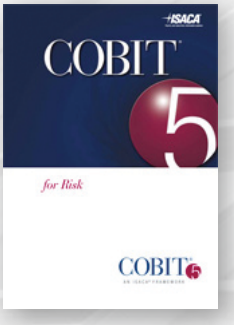
Product Code: XMXCM15-12M
Member/Nonmember: $185.00/$225.00

The *CISA* and *CISM Review Questions, Answers & Explanations Databases* are each a comprehensive pool of questions that combines the questions from the *Review Questions Answers & Explanations Manuals* and the *Supplements*.

Subscribe to the CISA® or CISM® exam online review course to:

- Have access to study at home, work or anywhere that best suits your needs
- Take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing you to identify your strengths and weaknesses and focus your study efforts accordingly.
- And much more!

When you choose an online database, your subscription includes the exam preparation information from the *Review Questions, Answers & Explanations Manual* and *Supplement*.



COBIT 5 for Risk by ISACA

Product Code: CB5RK
Member/Nonmember: $35.00/$80.00

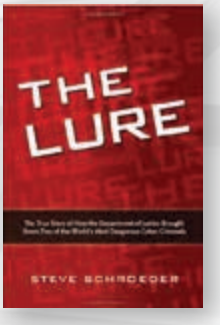
eBook Product Code: WCB5RK
Member/Nonmember: $35.00/$75.00

Risk is generally defined as the combination of the probability of an event and its consequence. *COBIT 5 for Risk* defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

Anti-Hacker Took Kit, 4th Edition by Mike Shema

Product Code: 38MAH
Member/Nonmember: $50.00/$60.00

Fully revised to include cutting-edge new tools for your security arsenal, *Anti-Hacker Tool Kit, Fourth Edition* reveals how to protect your network from a wide range of nefarious exploits. You'll get detailed explanations of each tool's function along with best practices for configuration and implementation illustrated by code samples and up-to-date, real-world case studies.



The Lure: The True Story of How the Department of Justice Brought Down Two of the World's Most Dangerous Cyber Criminals by Steven C. Schroeder

Product Code: 19IT
Member/Nonmember: $15.00/$25.00

THE LURE is the true, riveting story of how Russian hackers, who bragged that the laws in their country offered them no threat, and who mocked the inability of the FBI to catch them, were caught by an FBI lure designed to appeal to their egos and their greed. The story of the sting operation and subsequent trial is told for the first time here by the Department of Justice's attorney for the prosecution.

Secrets and Lies: Digital Security in a Networked World, 15th Edition by Bruce Schneier

Product Code: 115WSL
Member/Nonmember: $24.00/$34.00

This anniversary edition, which has stood the test of time as a runaway best-seller, provides a practical, straight-forward guide to achieving security throughout computer networks. No theory, no math, no fiction of what should be working but isn't, just the facts.

2 EASY WAYS TO ORDER:

1. Online—Access ISACA's bookstore online anytime 24/7 at ***www.isaca.org/bookstore-Jv3***

2. Phone—Contact us by phone M–F between 8:00AM – 5:00PM Central Time (CT) at 847.660.5650

2015 ISACA® Training Week

ADD NEW **KNOWLEDGE**.

ADVANCE YOUR **CAREER**.

Earn up to
32 CPE HOURS

SAVE $200 USD
Early Bird Discount Available

Choose the Course that Fits Your Role Today and Your Goals for Tomorrow

COBIT 5: Strategies for Implementing IT Governance
Chicago, Illinois | 4 – 7 August
Scottsdale, Arizona | 7 – 10 December

Cloud Computing: Seeing through the Clouds—What the IT Auditor Needs to Know
Chicago, Illinois | 9 – 12 November

Fundamentals of IS Audit and Assurance
Scottsdale, Arizona | 7 – 10 December

Foundations of IT Risk Management
Chicago, Illinois | 4 – 7 August
Scottsdale, Arizona | 7 – 10 December

Governance of Enterprise IT
Chicago, Illinois | 4 – 7 August
Scottsdale, Arizona | 7 – 10 December

Healthcare Information Technology
Dallas, Texas | 20 – 23 July

Information Security Essentials for IT Auditors
Mexico City, Mexico | 15 – 18 June
(taught in Spanish)
Miami, Florida | 21 – 24 September

Introduction to Information Security Management
Chicago, Illinois | 4 – 7 August

Introduction to Privacy and Data Protection
Atlanta, Georgia | 5 – 8 October

Social Media in Your Enterprise: Mitigating the Risk and Reaping the Benefits
Seattle, Washington | 24 – 27 August

Taking the Next Step: Advancing your IT Auditing Skills
Boston, Massachusetts | 19 – 22 October

REGISTER TODAY OR LEARN MORE AT
www.isaca.org/train15-jv3

ISACA®
Trust in, and value from, information systems

Introducing CSX Skills-Based Cybersecurity Training and Certifications.

CSX™
CYBERSECURITY NEXUS

More and more cybersecurity professionals are turning to Cybersecurity Nexus™ [CSX] for the knowledge, tools and guidance they need to be successful in their jobs. CSX is your premier source for education, training, research, industry events and community — and now, for cutting-edge certifications and training courses. Our new, skills-based programs are designed to help you build, test and showcase your skills in critical areas of cybersecurity. Because it's not enough anymore to show you have the knowledge, it's about proving you have the technical skill and ability to do the job from day one.

Visit www.isaca.org/cybercert-jv3 for more information.

ISACA®