Volume 6, 2016

ISACA Journal

Performance Measurement Metrics for IT Governance

Assessing Security Controls—Keystone of the Risk Management Framework

Delivering Personal Data Protection Compliance on a Global Scale

ISACA®
Trust in, and value from, information systems

www.isaca.org

Taking an ISACA® certification exam just got a lot more convenient!

Experience the difference starting in 2017.

What does this change mean for you?

- > More opportunities to take an exam
- > Larger test center network
- > Faster exam results
- > Test centers designed specifically for testing

Be part of this exciting transition to computer-based testing and be one of the first to take an ISACA® certification exam in 2017! Take the first step towards obtaining a globally respected ISACA certification and becoming recognized as one of the most-qualified professionals in your field of information systems.

Register today at: ***www.isaca.org/2017exams***

ISACA®

Trust in, and value from, information systems

Learn the essentials of managing compliance & ethics programmes

INTERNATIONAL

BASIC COMPLIANCE & ETHICS ACADEMIES

FROM THE SOCIETY OF CORPORATE COMPLIANCE & ETHICS®

28 NOV–1 DEC | MADRID, SPAIN

PLAN NOW TO TAKE THE CCEP-I® CERTIFICATION EXAM AFTER YOU COMPLETE THIS INTENSIVE TRAINING

GET CERTIFIED
ENROLL NOW

9,100+
COMPLIANCE PROFESSIONALS
HOLD A COMPLIANCE CERTIFICATION BOARD (CCB)® CREDENTIAL

CLE APPROVED

CCEP-I®
INTERNATIONAL
Certified Compliance & Ethics Professional

REGISTER EARLY TO RESERVE YOUR PLACE
LIMITED TO 75 FOR EACH ACADEMY

SCCE Academies. Training more than 3,600 compliance and ethics professionals around the world.

www.corporatecompliance.org/academies

Questions: lizza.catalano@corporatecompliance.org

ISACA Journal

FEATURES

PLUS

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 November and December 2016.

Achieving Excellence in Supplier Risk Management
Shirali Vyas, CA, ICAI

The Domains of Data and Information Audits
Ed Gelbstein, Ph.D.

The New EU General Data Protection Regulation
Eva Sweet, CISA, CISM

The Tone at the Top
Gary Roboff

Discuss topics in the ISACA® Knowledge Center: *www.isaca.org/knowledgecenter*
Follow ISACA on Twitter: *http://twitter.com/isacanews*; Hashtag: #ISACA
Follow ISACA on LinkedIn: *www.linkedin.com/company/isaca*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

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

Read more from these *Journal* authors...

Journal authors are now blogging at *www.isaca.org/journal/blog*. Visit the *ISACA Journal* blog, Practically Speaking, to gain practical knowledge from colleagues and to participate in the growing ISACA community.

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**?

Get up-to-date security skills with Capella University's Master's in Information Assurance and Security (MS-IAS).

Specializations include Digital Forensics, Network Defense, and Health Care Security.

Along the way to your MS-IAS, earn up to 3 NSA focus area digital badges showcasing your mastery of skills in specific cybersecurity areas.

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. **CAPELLA.EDU/ISACA** OR **1.866.933.5836**

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

ACCREDITATION: Capella University is accredited by the Higher Learning Commission.
HIGHER LEARNING COMMISSION: https://www.hlcommission.org, 800.621.7440
CAPELLA UNIVERSITY: Capella Tower, 225 South Sixth Street, Ninth Floor, Minneapolis MN 55402, 1.888.CAPELLA (227.3552)

Capella University

information security matters

The G7 and Cyber Security

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 click on the Comments link to share your thoughts.

I first learned the term MEGO in a column by the great conservative pundit, William Safire.[1] In his *Safire's Political Dictionary*,[2] he defines the term as an acronym for "my eyes glaze over" and "something that is undeniably important and paralyzingly dull."[3] There are few topics so MEGO as G7 meetings, the gatherings of the leaders of the world's industrialized democracies. You know they happen; you know they are important. But can you name all seven G7 nations,[4] much less their leaders? Do you have any idea what they talk about or accomplish?

With this stirring introduction, your eyes are probably starting to mist and you have your hand on the corner of the page, about to turn. Please stay awhile for a MEGO you should know about. In May 2016, the G7 leaders met in Ise-Shima, Japan, and produced a document that has real meaning for all of us who care about cyber security.

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

The G7 Ise-Shima Leaders' Declaration

The formal communiqué of the meeting[5] contains an introductory paragraph under the heading of Cyber. It is essentially a declaration of principles and contains the following statement: "We strongly support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity." Like many readers of this journal, I have spent my entire career trying to build accessible, open, interoperable, reliable and secure information systems, so I found this acknowledgment by world leaders to be especially gratifying.

The fact that this issue reached the G7 agenda[6] is recognition that cyberspace is not secure; it is insecure enough that their individual and collective interests are imperiled. To put this in context, the other topics addressed in the communiqué are the world economy, migration and refugees, trade, infrastructure, health, women, anticorruption, climate, and energy. Cyber security, as a global concern, has reached quite a high level indeed.

State Behavior

The expanded section of the communiqué[7] elaborates on the theme and contains the following sentence:

> We commit to promote a strategic framework of international cyber stability consisting of the applicability of existing international law to state behavior in cyberspace, the promotion of *voluntary norms of responsible state behavior during peacetime*, and the development and the implementation of practical cyber confidence building measures between states.[8]

I have italicized the phrase in the quote because it is so laden with meaning. It calls for "norms," which I understand to mean standards. I have previously bemoaned the lack of standards for cyber security,[9] so I found this call to be very heartening. These norms will necessarily be "voluntary" because there is no international body to enforce them. But, much as with other supranational declarations

(e.g., European Union directives), it is implicit that such norms should be incorporated into the laws and regulations of the nations that have made this commitment. The reference to "responsible state behavior" implies that countries that engage in state-to-state cyberattacks are acting irresponsibly. The qualifier "during peacetime" leaves unsaid that cyberattacks are legitimate actions in time of war.

The G7 leaders restricted themselves to the actions of states, although "non-state actors, including terrorists" are included as well. It is hard to imagine that ISIS or Al Qaeda are going to be impressed by a statement by the leaders of the world's industrialized nations. Perhaps, rather importantly, including non-state actors is a *de facto* declaration of cyberwar on terrorist groups and individuals. That would be just fine with me, since terrorists have clearly declared cyberwar on the world.

More open to interpretation is the effect on the nations that were not invited to the meeting. Recent research[10] indicates that, as recently as 2011, none of the G7 nations, except the United States, has been seen to have perpetrated state-to-state cyberattacks. It is not clear, at least to me, whether the G7 statement is a direct rebuke to the countries that engage in cyberattacks or acceptance that at least one of the G7 nations is already carrying out attacks on other states it considers to be adversaries.

G7 Principles and Actions on Cyber

Accompanying the communiqué, and referenced within it, is an annex titled "G7 Principles and Actions on Cyber."[11] It is a brief document, barely three bullet-pointed pages, that, for the most part, is a recitation of lofty goals with little or no mention of how they would be achieved. These include:

- Fair and equal access to cyberspace
- Respecting and promoting privacy, data protection and cyber security
- A multistakeholder approach to Internet governance
- Promoting and protecting human rights and principles of rule of law online

Nonetheless, there are a few assertions that could have real impact if the G7 countries adhere to them. Chief among these is the statement that "cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law." So far, there have been no incidents in which cyberattacks have led to shooting, although it is evident that such attacks have been used as adjuncts to warfare already underway, specifically the war between Russia and Georgia in 2008.[12] Former US Secretary of Defense Leon Panetta has warned of the possibility of a "cyber Pearl Harbor."[13] Acceptance of this concern by the other six nations as a *casus belli* is, to my mind, a necessary, but rather frightening, step.

The Principles contain a statement so specific that its inclusion among the platitudes comes as a bit of a shock: "We also welcome proactive approaches such as 'Privacy by Design' which take privacy and protecting personal data into account throughout the engineering process." The term "Privacy by Design" was originated in the 1990s by Ann Cavoukian, who had been Ontario's Information and Privacy Commissioner.[14] It has since become a widely accepted global privacy standard, which the mention by the G7 certainly affirms.

The seven national leaders committed their countries to cooperation among national computer security incident response teams. (Well, actually they did not commit themselves. They promised to "endeavor.") These teams, better known as national CERTs, such as CERT-FR, US-CERT and CERT-UK, are repositories of information about cyberattacks and providers of assistance to those in their nations who have been attacked. International cooperation on cyber security is not new, but recognition of the need for nations to work together to combat cyberattacks by heads of government is new. Just as no one company alone can solve the problem of cyber security (whatever "solve" means in this context), the G7 is saying that no one country can do it either.

The G7 pronouncements on cyber security have not been widely publicized, perhaps because too many editors' eyes glazed over. They are not a treaty; they

Enjoying this article?

- **Learn more about, discuss and collaborate on information security management in the Knowledge Center.** *www.isaca.org/Information-Security-Management*

have no force of law; and too few countries agreed to them. But they are an important assertion that the issue of cyber security has reached a level of concern that presidents and prime ministers must address. We security professionals who are doing the work to build adequate protections against cyberattacks may take some comfort in knowing that our efforts are not going unrecognized by the world's leaders.

Endnotes

1 Safire, W.; "MEGO," *The New York Times*, 6 September 1973, *www.nytimes.com/1973/09/06/archives/mego-essay.html?_r=0*
2 Safire, W.; *Safire's Political Dictionary*, Oxford University Press, UK, 2008
3 *Ibid*., p. 423
4 Canada, France, Germany, Italy, Japan, the United States and the United Kingdom
5 G7 2016 Ise-Shima Summit, "G7 Ise-Shima Leaders' Declaration," 26-27 May 2016, *www.mofa.go.jp/files/000160266.pdf*
6 Full disclosure: My colleague at Risk Masters International, Allan Cytryn, is also an executive board member of the Boston Global Forum, which contributed to the agenda for the Cyber portion of the Ise-Shima meeting, *http://bostonglobalforum.org/2016/05/the-bgf-g7-summit-initiative-ise-shima-norms/*.
7 *Op cit*, G7 2016 Ise-Shima Summit
8 *Ibid.*
9 Ross, S.; "Frameworkers of the World, Unite, Part 2," *ISACA® Journal*, vol. 3, 2015, *www.isaca.org/Journal/archives/Pages/default.aspx*
10 Valeriano, B.; R. C. Maness; "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," *Journal of Peace Research*, vol. 51, iss. 3, 2014, p. 347-360
11 G7 2016 Ise-Shima Summit, "G7 Principles and Actions on Cyber," 26-27 May 2016
12 Markoff, J.; "Before the Gunfire, Cyberattacks," *The New York Times*, 12 August 2008, *www.nytimes.com/2008/08/13/technology/13cyber.html*
13 Department of Defense, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," USA, 11 October 2012, *http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136*
14 Cavoukian, A.; "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, August 2009 (revised in January 2011), *https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf*

IS audit basics

The Soft Skills Challenge, Part 6

Barriers to Learning to Learn

Previous columns have explored how to facilitate the process of learning to learn, covering knowledge acquisition, the taxonomy of knowledge, and tools such as mind mapping and document deconstruction.

While it is clear that continuous learning is essential, there are many barriers to achieving it. The most common barriers are explored in this column and, wherever possible, hints and suggestions on how to overcome them are provided.

Procrastination

Natural, almost instinctive, procrastination is the "Never do today what you can leave for tomorrow" philosophy. The definition of "tomorrow" varies in many distinct cultures and locations. It may not mean the day after today, but rather an unspecified future time.

Regardless of the specifics, procrastination is a powerful enemy of progress and success. It takes considerable discipline to overcome the temptation to avoid doing now what needs to be done now. A quick Internet search on "techniques to avoid procrastination" will reveal many sources of tactics that can help overcome the temptation to procrastinate. The key is to do the search and start taking action—now.

The Lazy Brain

While the brain accounts for, on average, only 2 percent of body weight, it consumes 80 percent of the typical person's energy intake and is amazingly busy controlling everything people do, feel, say and think.

Nature has made provisions for this by forcing the brain to rest in several ways, including dozing, sleeping and building routines. Routines are like a railroad track causing the brain to follow well-defined paths created over the years to reduce its workload, a process referred to as "unconscious competence."

The process of learning pushes the brain toward unknown, uneven paths and only repetition, going over this new path many times, will reinforce it to the point that it becomes usable and retained in long-term memory. This represents a progression from unconscious incompetence (where the learner does not know what he/she does not know) to conscious incompetence (a stage at which the new knowledge has not yet been fully acquired).

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 click on the Comments link to share your thoughts.

Ed Gelbstein, Ph.D., 1940-2015
Worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late '60s and early '70s, and managed projects of increasing size and complexity until the early 1990s. In the '90s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi)retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. Thanks to his generous spirit and prolific writing, his column will continue to be published in the *ISACA® Journal* posthumously.

Stefano Baldi
Is an Italian career diplomat and an early adopter of information systems and communications, as well as a driving force for the more extensive use of online learning. Baldi is the director of training at the Italian Ministry of Foreign Affairs. His diplomatic postings have included serving as the permanent representative of Italy at the UN in Geneva, Switzerland, and, subsequently, New York City, New York, USA, and at the European Union in Brussels, Belgium. Baldi has authored and coauthored several books on diplomacy-related topics and has run courses for diplomats from around the world on topics such as information management and information security.

If the progression does not continue beyond conscious incompetence, the learning will be quickly forgotten (e.g., a foreign language learned many years ago and only very slightly retained now). Short-term memory is quickly erased (e.g., the common experience of searching for car keys or your spectacles used just moments earlier).

Even if conscious competence has been reached, it will degrade if not maintained by continuous practice as long-term memory is overwritten by other topics. Common knowledge suggests that riding a bicycle is a skill that, once learned, is never forgotten; common wisdom would suggest not putting this to the test in heavy traffic.

To find out more about the mechanisms of the brain, the book *Brain Rules*[1] is a good start. Two other authors who have made valuable contributions to the processes of thinking and learning are Edward de Bono and Tony Buzan. Discovering more about their work can be rewarding. After all, the human brain does not come with an owner's manual, so it is not always obvious how to make the best use of its capabilities.

Work/Life Balance

Job satisfaction, a sense of creating value and being recognized are vital to remain engaged in one's work. Outside work, each of us has a different set of values, aspirations, commitments and relationships. When all these are balanced, quality of life is enhanced.

Learning a new topic disrupts this balance and requires compromises that, left unresolved, could turn into stress, even when such learning is essential for professional survival.

The learning process is most likely to be successful when the individual is organized and motivated and maintains a healthy lifestyle that includes quality sleep and physical exercise. Ancient Romans advocated a *mens sana in corpore sano* (sound mind in a healthy body). These days, neurologists and psychologists fully agree.

Difficulty in Making Time for Concentration and Thinking

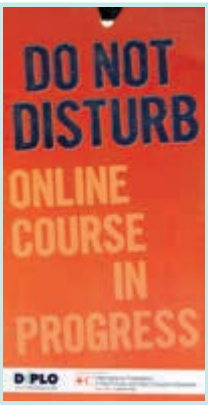
Perhaps among the prevalent challenges in many societies is the relentless pressure in the workplace to attend meetings, handle assorted administrative trivia, be contactable 24/7, and respond immediately to email and quickly to mini-crises. This creates an environment of artificial urgency.

For those who wish to learn from their home, the challenges are just as demanding: the domestic timetable of events (dinner, visitors, domestic activities) and, most important, human needs for contact and support from the other members of the household.

However, without making time to study and think (finding time is unlikely), learning becomes impossible.

One of the organizations with which the authors have collaborated provides online training to diplomats in full-time employment. The study modules are designed to offer compelling content in a concise way to allow their completion in a relatively short time. Hundreds of copies of the card shown in **figure 1** have been distributed to the courses' students, who are also advised to discuss and agree on their time needs with their bosses and their families.

Figure 1—Making Time to Study Aid



Source: DiploFoundation. Reprinted with permission.

Distractions and Interruptions

Most people are inundated with requests on a daily basis ("When will you be home?," "Do you have a minute?"). These requests, albeit legitimate and warranted, interfere with the state of mental flow that learning requires. Sometimes it is easy enough to ask if the request can wait until later, sometimes not. A "do not disturb" sign is often useful. Ultimately, it is up to individuals to protect their learning time from disruptions, which requires good skills in the art of saying "no." An Internet search will point to many sources concerning this skill.

Creating an appropriate level of isolation and concentration while learning may require the learner to exercise the willpower to go offline and avoid all devices (e.g., smartphones, tablets, email). Unfortunately, many appear incapable of doing so. This inability is common enough to have acquired a name (or two): fear of missing out (FOMO) and the inability to switch off (ITSO) syndrome.

Poor or No Support at Work or Home

There are many permutations of factors that support or hinder learning work-related tools and techniques. In an ideal situation, the organization has policies that encourage individuals to acquire such skills during working hours.

These may include lunchtime or early evening seminars or workshops, encouraging access to online learning material (the company's own or someone else's), group discussions on specific topics, and in-house training led by an instructor or facilitator. Of course, these may be matched by a formal requirement for the employee to acquire and retain the appropriate certifications.

Other, less supportive organizations consider the acquisition of new knowledge the employee's personal responsibility and do not provide any of the learning options mentioned earlier or even consider supporting participation at evening classes, conferences or association meetings, e.g., the local ISACA® chapter meetings. Trying to study in the home environment is not always ideal unless there is a room where the learner can hide for hours without the risk of alienating the rest of the household.

Quality of the Didactic Material

The ideal didactic material should be concise, contain "just in time" rather than "just in case" material, make extensive use of illustrations, be structured in manageable modules and include tests to validate the extent to which the reader has comprehended the module.

Unfortunately, this is not always the case, as some of the material is designed to be a 500-page or more comprehensive guide to a topic. The content may be brilliant, but going through it is akin to reading a dictionary as if it were a novel. While mind mapping and document deconstruction may help in reformatting the material into digestible chunks, the learning process is handicapped when the authors of the material are unfamiliar with how to construct didactic material.

Personal Engagement to Learning

This is absolutely essential. The Nigerian proverb "Not to know is bad; not to wish to know is worse"[2] is worth bearing in mind at all times by those who wish to keep their knowledge fresh, up to date and relevant to their professional activities. The same is true, of course, for material related to personal interests, ranging from changes in taxation legislation to the arts.

For those who have such engagement, there are fascinating opportunities to explore some exceptional material available, mostly free of charge, from several massive open online course (MOOC) providers.

Personal Learning Skills

Part 1 of this column, which was published in the *ISACA® Journal*, volume 3, 2015, discussed the ways in which people acquire information and what

it takes to turn it into knowledge that can be applied to specific situations. The reader is invited to reflect and experiment with various formats such as audio books, online learning, visual material, interacting with others, and personal trial and error to identify which of these, or which combination of them, is the most effective for the individual.

Conclusion

It is hoped that the reader will accept the dual notions that acquiring and maintaining skills are essential for professional survival. If so, doing nothing is not a real option. The reader is encouraged to develop a personal learning plan and put it into effect. Ideally, the result will be the realization that acquiring new knowledge is a pleasure, not a problem.

Endnotes

1 Medina, J.; *Brain Rules (Updated and Expanded): 12 Principles for Surviving and Thriving at Home, Work, and School*, Pear Press, USA, 2014, *www.brainrules.net*

2 Boston University Pardee School of Global Studies, African Studies Center, Massachusetts, USA, *www.bu.edu/africa/outreach/resources/np/*

CYBER STRONG.

Claim your future in the high demand Cybersecurity and information assurance/security fields. Students will be educated in the technical aspects of Cybersecurity systems and will be prepared for the management, operations and oversight of these systems.

Classes are forming now in our state-of-the-art Cybersecurity laboratory and online.

SAINT LEO UNIVERSITY®

Saint Leo University offers competitive degree programs designed to train students in the field of cybersecurity.
B.S. Computer Science - Information Assurance
B.S. Cybersecurity
M.S. Cybersecurity

800.707.8846 | SaintLeo.edu

National Security Agency and the Department of Homeland Security have designated Saint Leo University as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) through academic year 2021.

Marcus Chambers, CISM, CGEIT, CEng
Is an experienced information security professional who has worked in a variety of different sectors across a wide range of enterprises. He has worked at a senior level for a number of years, including in the financial services sector, and is experienced in navigating challenging issues and dealing with senior stakeholders. Chambers has created road maps and delivered significant security improvement programs in several multinational corporations. He takes great personal satisfaction in effective delivery and sound governance of change programs.

Q: How do you think the role of the information security professional is changing or has changed?

A: We are now able to base investment decisions on evidence from events that have occurred. Clients often ask if they are spending too much or too little money in comparison to their industry peers, and we can now generate a benchmark of spend across different industries to inform clients' balance of investment decisions in a way not previously possible, as information security was not considered of sufficient importance to warrant its own budget.

The proliferation of technology means more people are able to understand our challenges. It will become easier to translate threats and risk using a common lexicon and thereby more effectively gain buy-in, understanding and compliance from people across an entire organization. I think we will see increasing benefit from our ability to work together, across multiple sectors, sharing information on threats and on how different organizations in different industries and potentially in different countries have responded.

Q: How do you see the roles of information security and, specifically cyber security, changing in the long term?

A: I think we will see a greater interest from the general public in keeping their personal information secure. Now, if people are asked for their personal details, even if they are just registering with, for example, a new dentist or a social group, they are likely to ask: "If I pass my personal information to you, are you able to guarantee its security?" I think more consumers should ask this question whenever they are asked for their name, address and date of birth.

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

A: I would not have gotten my current role without the Certified Information Security Manager® (CISM®) certification and I am proud to have a qualification that is so widely recognized.

The main certifications I look for are the CISM or CISSP qualifications, and most information security job specifications will detail either of those two as being mandatory. I also look for an interest in the profession and a keenness to learn, to stay abreast of current topics and understand the context in which we are operating. It is important to be able to relate security issues to risk, so suitable qualifications such as Certified in Risk and Information Systems Control® (CRISC®) are also highly regarded.

Q: What do you think are the most effective ways to address the cyber security skills gap?

A: This is a complex problem and it will take time to address. In the UK, we are doing more by teaching coding in school and promoting science, technology, engineering and mathematics (STEM), but it will take some years for the fruits of these labors to be realized. In the shorter term, we need to broaden our recruitment base to

the network

ensure greater gender parity and we also need to make certifications more accessible to those who are new to the industry. ISACA® is doing good work here with the Cybersecurity Fundamentals Certificate.

Q: The UK is widely considered the cyber security hub of Europe with the largest talent pool of cyberprofessionals. What do you think the long-term impact of Brexit will be on European and global cyber security?

A: The UK is currently solidly entrenched as a primary hub for the international business community and has also yet to invoke Article 50, meaning the short- to medium-term impact is likely to be low. There is a potential risk to longer-term cyber security cooperation with the EU, although obstacles here would be in no one's interest.

In terms of the UK's position in Europe, a relevant example is the planned introduction of the EU's General Data Protection Regulation, which will still affect UK-based organizations that handle EU data post-Brexit. If the UK does not enact a similar act under UK legislation (concerning data held within the UK for UK citizens), I fear the UK may lose out if its data protection standards are perceived to be lower than those of EU countries. Levels of data privacy and security are valid concerns and consumers may choose the best location to have their data stored, or the most customer-friendly regime within which to operate. The UK must remain the optimum choice in this marketplace.

Q: You have considerable military experience. What role do you think the military will play in combating the threats of cyberterrorism and cyberwarfare?

A: Cyberwarfare, or at least state-on-state cyberinterferences, have already taken place, and I have no doubt that Western militaries are working with other government bodies to share information to ensure an appropriate level of protection. Conventional Western militaries are very good at using existing frameworks, such as the North Atlantic Treaty Organization (NATO), for increased international cooperation and threat deterrence. The use of international organizations as a vehicle for greater cooperation should act as an exemplar for commercial and nonstate bodies to work together to combat threats, share information and learn from each other.

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

A: My transition from the military was a significant challenge. To overcome the challenge, I took advice from colleagues who had left the military before me, I networked and I ensured that I had appropriate qualifications to showcase my skill set. I made the challenge a little harder as I wanted to break into the commercial world, rather than work in the defense or public sector with which I was more familiar, but I am very happy with the result, have learned a tremendous amount and I enjoy each day's new challenges.

1 What is the biggest security challenge that will be faced in 2017? How should it be addressed?

Enforcing international law against cybercriminals who operate across international boundaries. Ensuring it is safe to operate online in an international, rule-based system where the laws apply to all remains *the* enduring challenge.

2 What are your three goals for 2017?

- Complete my third and final Masters degree, an MSc in information security
- Learn to play the guitar (after the summer MSc exams)
- Do a handstand push-up (see the final question!)

3 What is your favorite blog?

- Krebs on Security
- US National Institute for Standards and Technology's (NIST) security updates
- *The Wall Street Journal* and the *Financial Times*' technology articles

4 What is on your desk right now?

My water bottle, MacBook Air and A5 Bullet Journal notebook

5 What is your number-one piece of advice for other information security professionals?

Get the basics right and everything else follows.

6 What is your favorite benefit of your ISACA® membership?

Access to the research materials, frameworks and white papers

7 What do you do when you are not at work?

I read as widely as possible, military and political history as well as a wide range of fiction, and I love to exercise. Recently, I have become a CrossFit addict, but I try not to talk about it!

Information Ethics in the Mid-21st Century

This is the final installment of the Information Ethics column. ISACA® wishes to acknowledge with deep gratitude this column's author, Vasant Raval, for his significant contribution of thought leadership to the *ISACA® Journal* and readers worldwide through the years. The column will remain archived on the ISACA web site for your reference.

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 click on the Comments link to share your thoughts.

In his book *Code*,[1] Lawrence Lessig talks about the two first-generation theorists of cyberspace who delivered stories about cyberspace's future in 1996. One envisioned that the future will be a pact between two forces of social order—code and commerce—while the other emphasized how the Internet will deliver more control to the government. The passage of some 20 years since these predictions has brought tectonic shifts in both code and commerce, impacting the social order along the way. In such a short period of time, we have precipitously ushered in the second generation of cyberspace.

There are significant differences between the first and the second generations of cyberspace. The first generation was dedicated to sharing of information, especially in academia and mainly for research. Security, confidentiality and user authentication were nominally important; the primary excitement sprung from the ability to network and share projects, exchange information in real time, and work with peers and professionals remotely. The second generation saw the migration of the code to the world of commerce, where economic value creation, efficiency, authentication and information security gained prime importance. Speed to market, globalization, scaling to the masses—these took over the agenda for priority setting and resource allocation in businesses. Nonissues of the first generation of cyberspace became significant concerns of the second generation.

In tandem with first-generation cyberspace observers, a community of ethicists evolved to give shape to moral issues in the increasingly dominant information space. When one predicted the impact of computers on society early on, several thought leaders followed the thread, including one who defined computer ethics as "a field concerned with *policy vacuums* and *conceptual muddles* regarding the social and ethical use of information technology (emphasis added)."[2]

> **"The emergence of cyberspace has produced a new crop of rather difficult-to-resolve dilemmas, although the precepts and paradigms to address them remain the same."**

It is important to examine the possible connection between the arrival of cyberspace and an increased level of interest in ethics of information. Ethical issues are derivatives of changes in the concerned domain that bring about new sets of dilemmas. The emergence of cyberspace has produced a new crop of rather difficult-to-resolve dilemmas, although the precepts and paradigms to address them remain the same. Thus, the practice of ethics is challenged while the underlying ethical principles remain stable. Absent cyberspace, information in existence at the time was controlled, and the sharing of information was guarded and purposefully intentional. With the advent of cyberspace, the shareability of information has reached astronomical heights (and there is farther to go!). Questions about who controls the shared information suddenly made available in cyberspace and how such control might be used

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

by those who possess the information are central to issues of justice, equity, fair treatment, privacy, confidentiality and so forth. How these questions will be addressed carries a value connotation and, as a result, ethical consequences.

Even in the cyberspace age, the ethical dilemmas vary in degree of criticality. The use of Roomba to vacuum my home has limited or no ethical issues, while the use of drones to target insurgents is a different value-ridden exercise.[3] Moreover, the cyberspace age works both ways: At times, it helps sort out an ethical dilemma while, in other situations, it may create a new one with which we must deal. For example, in camel races in Doha, when global positioning system (GPS)-enabled, automated robots replaced enslaved and starved Sudanese boys as jockeys,[4] the atrocities rendered to kidnapped children were ameliorated. In the same cyberspace, the classic trolley problem, "Is it ethical to kill one person to save five?"[5] resurfaces as a puzzle on the drawing board of the logic that will govern fully automated cars.

In one analysis, the GPS-enabled, automated robot jockeys would be an example of the logical malleability of cyberspace. "The logic of computers can be massaged and shaped in endless ways"[6] to create economic benefits—a supreme force that leads to innovations such as Facebook, Airbnb and Uber. Given the same information resources of cyberspace, creativity may be the only limit to unleash powerful new business models. Once a business idea is born, its information processes can be structured to support the new model using logical malleability. This is how transportation as a service is born with Uber and hospitality as a service with Airbnb. Evidently, devices are necessary; however, it is logical malleability that creates value.

Social Order

The cyberspace leveraged by commerce creates a complex web of interactions among stakeholders, which impact the social order. Because social order is the face of humanity, it mirrors acceptance of and respect for value-centric behavior on the part of individuals and organizations. Social order, in other words, is where the litmus test of practiced human values is apparent.[7]

"The cyberspace leveraged by commerce creates a complex web of interactions among stakeholders, which impact the social order."

It can be argued that values are of two sorts: structural and substantive. According to one ethicist, the US Constitution and the Bill of Rights are indicative of these values, respectively.[8] While both are critical and complementary in value judgments, it is the substantive aspect of cyberspace that constantly changes, creating new economic realities and presenting new ethical challenges. By providing a platform for ride hailing, Uber and its competitors have changed the substantive dimension of cyberspace. The provider does not need a dedicated vehicle called "taxi" and the traveler does not need to look for a taxi. Ride-hailing platforms in cyberspace arrange to have the provider meet the customer—a new service orientation to the old industry, thanks to the logical malleability of cyberspace.

When disruptive innovations enter the market, they throw the social order out of balance. For example, with Airbnb and Uber, their traditional rivals face possible job cuts while others who need extra income flock to the idea of part-time work. Ultimately, full-time jobs in the space may shrink considerably and part-time work with hardly any associated fringe benefits will grow. With driverless cars, even the traditional taxi business does not need a person at the wheel, making the scenario more complex. These structural shifts in

the job market are not value-neutral forces. If anything, ethical dilemmas of the present-day cyberspace business models could prove far more challenging to sort out.

The irony is that while traditional careers face sunsetting, there will be new skills in demand, creating flourishing careers in domains such as data analytics. However, time, resources, skills and aptitude necessary for the transition could be a major handicap for most people in need. As a result, many could suffer, demanding justice and fairness for their treatment.

> **"There are no good answers to the question of how to regulate the radically new versions of the old ecosystems."**

Regulation is the provider of stability in the midst of chaos. In this sense, it is the closest ally to business ethics. As industries mature, regulations become more effective and predictable in their outcomes. They provide the lowest common denominator of norms of behavior. However, in second-generation cyberspace, society is constantly buffeted by considerable changes. Also, these changes are nonlinear to a degree that any learning from the established regulatory framework is not very helpful.

The remarkably different chemistry of cyberspace makes much of the regulation meaningless; its translation is neither simple nor effective. After almost 20 years of providing due diligence to cyberspace, the US government is giving up control over the domain naming system managed by the Internet Corporation for Assigned Names and Numbers (ICANN), effective 1 October 2016.[9] What this will do to the globally present structural dimension of cyberspace is, at best, uncertain.

We see the regulatory struggle in the hospitality industry, the ride-hailing business, drone deployment and fully autonomous cars. There are no good answers to the question of how to regulate the radically new versions of the old ecosystems. The financial technology (FinTech) revolution reinforces the same puzzle; it is difficult to determine how, and how much of, the elaborate regulatory structure of the banking and financial services industry could be applied to the new players in the electronic payment industry. The quote, "There is no substitute and no better 'regulator' than the *moral point of view* with its attention to the needs and concerns of others (emphasis added),"[10] emphasizes that greater dependence on reflective morality would be more beneficial than unreflective obedience to law.

The Future of Information Ethics

As logic makes machines deliver more, an increasingly responsible role is assigned to the machine in a man-machine allocation of tasks. Over time, more complex machine-learning systems are designed, leaving very little for humans to do except at the design and coding stage of the system. This seemingly limited human role is, nonetheless, extremely important to information ethics. This is because value judgments are exercised and embedded in cyberspace by people, not machines. The morality of a machine is close to the moral grounding of the humans who create the machine, at least for now. As machines learn, the classic Trolley problem may be addressed by the machine itself.

The rise of bad elements will continue, primarily due to two reasons. First, humans are gullible and error prone. They make mistakes and are subject to judgment errors. The rise of social engineering presents irrefutable evidence that people succumb to fraudsters, including Ponzi schemes[11] and con artists. Second, when technology obviates human judgment

in a situation creating an ethical dilemma, humans are often tempted to commit a compromise.[12] This is, perhaps, because of the remoteness of the impact of their decision. Ashley Madison is a graphic example of how this might happen; because it is presented through technology, having an extramarital affair does not seem to be problematic for many. As another example, studies on e-signature suggest that people signing electronically do not own their responsibility as much as they would had they signed on paper or sometimes when they did not sign at all.[13]

Cyberspace will continue to create very powerful businesses with enormous reach. Some of these companies will be quite young, endowed with low organizational maturity or a weak will. These businesses will be bigger in their economic impact than some national economies (Alphabet, Facebook and Uber are good examples of businesses with exceedingly large economic impacts). The need to ensure some measure of fairness seems to be increasing across these vastly influential technology platforms.[14] These enterprises will become the *de facto* guardians of privacy, confidentiality, public interest and other values important for maintaining the social order. Because they create, they know much more about it than those who guard the guardians. It makes sense, therefore, to depend on these influential businesses at the leading edge to lead the way to ethical behavior. It remains to be seen as to how well they will individually and collectively meet this tall order. Presumably, material goals take precedence in a business compared to related nonmaterial goals[15] and this is unlikely to change in cyberspace. If anything, the urge to be first in the marketplace actually could become more feverish. Already, we see the signs of racing companies that amass unprecedented market wealth and soon garner the influence of a near-monopolistic player in the global space. Interestingly, despite their size, no single player will have the influence to mute others in the space. Their individual efforts could probably be considered as best practices.

One other encouraging source for seeking guidance on the code of conduct is institutions that represent various professions at the core of the cyberspace revolution. Indeed, they should have knowledge and influence to harness collective insights to frame the rules of conduct in this space. It is difficult to predict whether this will materialize. The International Ethics Standards Board for Accountants recently released *A Handbook of the Code of Ethics for Professional Accountants*.[16] However, the publication heavily emphasizes compliance, when we require much more from the professions to cope with seismic changes in the substantive cyberspace.

The structural dimension of cyberspace has marginalized the significance of national and regional boundaries. There is much more that a business, or any group of people, can do today with little concern for national boundaries. Yes, nations have their say in controlling the region's destiny; however, it will be difficult for a region to prosper going against the tide of the substantive cyberspace revolution. Thus, the future is a mixed blessing; collaborating across boundaries while managing the destiny of the nation will be a balancing act for future political leaders. In the process, ethical meltdowns may happen when shortcuts are taken to gain an edge on national goals.

Enjoying this article?

- **Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center.** *www.isaca.org/information-security-policies-and-procedures*

Now, nations ponder whether they can live with some sacrifice of privacy in the interests of society. While investigating crime scenes, German law enforcement has recently found that it does not capture enough surveillance data to track the movement of people. In the larger interests of society, a nation that is a staunch defender of privacy is now reconsidering whether some privacy can be sacrificed to hunt down criminals.[17]

> **"Information ethics is discretionary and, by itself, may not produce value, at least in the short run."**

The situation in Syria epitomizes a whole new migratory wave of people from the Middle East to various countries in Europe and beyond. This is not a direct result of cyberspace; however, it bears a significant impact on the future of identity verification and authentication. Thus far, individuals have looked to national authorities to provide identification and authentication certificates (e.g., passports). Refugees may not have any of these if they lost them or could not bring such personal belongings. And, if they do possess identifying documents, it is still difficult to identify people by relying only on papers from their country of origin. An alternative is to use block chain technology to provide identity and authentication data that would transcend national boundaries and local authorities.[18] The idea merits experimentation and, in the long run, could provide more effective and humane global means of identity and authentication.

And, finally, regulators cannot effectively regulate what they do not know or cannot predict. For this reason, they will have to work with industry leaders to understand the new dynamics and, thus, decipher risk factors to be mitigated. A collaborative approach to developing regulations is the only way. In the United States, regulators have echoed this sentiment when, in the case of guidelines for drone use, they diverged from the past by seeking a collaborative, incremental approach to the development of drone use regulations. On the matter of autonomous cars, US regulators have embraced the thought that if driverless cars could save many lives, why not sooner rather than later?[19] Regulators are prepared to work with automakers and their electronic collaborators to learn more about related risk and how to mitigate it in the new world of transportation.

Information ethics is discretionary and, by itself, may not produce value, at least in the short run. Even for the courageous ones who want to do the right thing, past experience may not be enough to identify ethical dilemmas, let alone solve them. It will take significant effort to protect human values as material progress keeps chugging along. We may be held hostage by the devices and means of efficiency, thus, more comfortable, but not happy.

This thought sums it up well: "Humanity is messy and the cleanup falls to us."[20]

Endnotes

1 Lessig, L.; *Code*, Basic Books, USA, 1999
2 Moor, J. H.; "What is Computer Ethics?" *Computers and Ethics*, 1985, p. 266-275, *http://web.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html*
3 *Washington Post,* "How Drone Strikes Get the OK," article reprinted in *Omaha World-Herald*, 8 August 2016, 3A
4 Raval, V., "Machine Ethics," *ISACA® Journal*, vol. 5, 2014, *www.isaca.org/Journal/archives/Pages/default.aspx*
5 Dockser Marcus, A.; "The Refurbished Trolley Problem," *The Future of Everything*, *The Wall Street Journal* supplement, June 2016, p. 76-79
6 *Op cit,* Moor, p. 3
7 *Ibid*.
8 *Op cit,* Lessig
9 McKinnon, J. D.; "Obama Administration to Privatize Internet Governance on Oct. 1," *The Wall Street Journal* supplement, 16 August 2016, *www.wsj.com/articles/obama-administration-to-privatize-internet-governanceon-oct-1-1471381820*

10 Spinello, R. A.; "Code and Moral Values in Cyberspace," *Ethics and Information Technology*, vol. 3, 2001, p. 137-150

11 Securities and Exchange Commission, "Ponzi Schemes," USA, *https://www.sec.gov/answers/ponzi.htm*

12 Ariely, D.; *The Honest Truth About Dishonesty*, Harper-Collins, USA, 2013

13 Chou, E. Y.; "What's in a Name? The Toll E-signatures Take on Individual Honesty," *Journal of Experimental Social Psychology*, vol. 61, 2015, p. 84-95

14 Fisman, R.; T. Sullivan; *The Inner Lives of Markets: How People Shape Them and They Shape Us*, PublicAffairs, USA, 2016

15 Raval, V.; "Moral Dialogue on the IT-leveraged Economy," *ISACA Journal*, vol. 3, 2016, *www.isaca.org/Journal/archives/Pages/default.aspx*

16 International Federation of Accountants, *2015 Handbook of the Code of Ethics for Professional Accountants, www.ethicsboard.org/iesba-code*

17 Turner, Z.; "Germans Reconsider Tough Privacy Laws After Terrorist Attacks." *The Wall Street Journal,* 24 August 2016, *www.wjs.com/articles/germans-reconsider-tough-privacy-laws-after-terrorist-attacks-1471628581*

18 Warden, S.; "A Digital Fix for the Migrant Crisis," *The Future of Everything, The Wall Street Journal* supplement, June 2016, p. 46-47

19 Stoll, J. D.; "US Won't Impede Self-drive Cars," *The Wall Street Journal*, July 2016, p. 23-24

20 Parish, S.; "A Far-Out Affair," *The Future of Everything, The Wall Street Journal* supplement, June 2016, p. 17-21

TOMORROW'S SECURITY IS HERE

Evolve your security and see what you're missing.

ATTACK SURFACE VISIBILITY

- Bring hybrid IT environments, geographic locations and business units into a single, interactive view
- Quickly spot Indicators of Exposure (IOEs) and proactively identify root causes of risk
- Neutralize critical attack vectors
- Meet regulatory and compliance requirements through improved auditing and reporting

SKYBOX™ SECURITY

www.skyboxsecurity.com

Modeling | Simulation | Security Analytics

Solve complex challenges in vulnerability and threat management and security policy management — with one platform.

Performance Measurement Metrics for IT Governance

Disponible également en français
www.isaca.org/currentissue

During the past 30 years, enterprises have been embracing new methods to transform their operations to use IT and related technology to provide a higher level of customer service. The pace at which enterprises are adopting these new methods is rapid. To handle the speed of this transformation, management relies on technology resources and vendors, resulting in an increased dependency on technology and skilled resources. The pace and dependencies can create a lack of enterprise control; therefore, enterprises use key performance indicators (KPIs) to measure the performance of IT service delivery.

Although many enterprises today conduct return on investment (ROI) analysis of new IT projects and sometimes incorporate the total cost of ownership (TCO) calculation into the business case that they present to the board of directors for approval, only about 25 percent of enterprises conduct ROI analysis after the completion of a project.[1, 2, 3] However, ROI and TCO are not the only criteria for approving IT projects; they are only two of the many considerations in the decision-making process. A positive ROI does not necessarily mean that the project will be approved. It is a strategic decision that is based on business requirements and stakeholder expectations. Therefore, enterprises should conduct a cost-benefit analysis that may require quantitative and qualitative indicators.

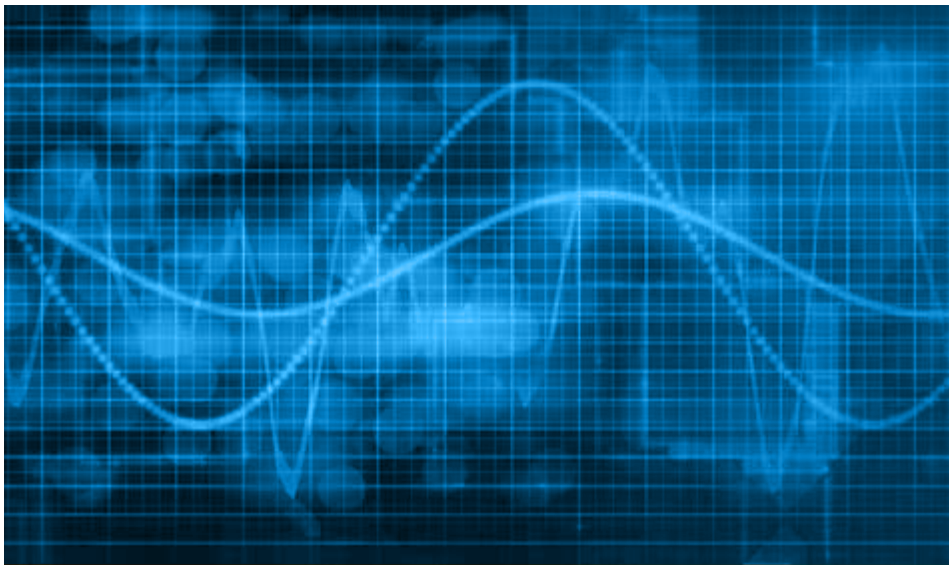
Enterprises that want to effectively monitor the activities of IT so that they are in line with the business goals use KPIs or key measurement metrics. Performance indicators/metrics not only help to monitor achievements compared against goals, but also help to evaluate the effectiveness and efficiency of business processes. Metrics also help enterprises allocate and manage resources. Performance metrics enhance and influence decisions that are related to business such as budgets, priorities, resourcing and activities.

KPI and metrics are essential tools for management that are implemented in all areas of the business. Today, enterprise use of IT and related technology requires huge investments in IT. Therefore, stakeholders are interested in confirming that IT investments are strategically aligned, managed effectively and help the achievement of common business goals. To ensure stakeholder expectations are met, management uses IT governance practices that are defined by the global standard from the International Organization for Standardization (ISO) ISO 38500 and COBIT® 5.

IT Governance and Metrics

The IT governance mechanism ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives. IT governance also ensures that direction is set through prioritization

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 click on the Comments link to share your thoughts.



Sunil Bakshi, CISA, CGEIT, CISM, CRISC, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty at the National Institute of Bank Management in India.

and decision making and that performance and compliance are monitored against agreed-on direction and objectives. Management plans, builds, runs and monitors activities in alignment with the direction that is set by the governance body to achieve the enterprise objectives.[4]

The IT governance processes are evaluate, direct and monitor (EDM). Metrics are a monitoring mechanism and help management monitor the achievements of the enterprise's business-related goals and IT-related goals. Appropriate metrics help the governing body provide direction that is based on defined goals and an evaluation of metrics. Metrics help enterprises answer valuable questions, such as:[5]

- Is IT performance better than last year?
- What is the enterprise getting from IT investments?
- How can the enterprise benchmark performance?
- What should the enterprise do in the absence of measureable metrics? Can it use risk management, loss expectancy, attack vectors or correlation?

Metrics describe a quality and require a measurement baseline, e.g., 87 percent of incidents reported were resolved within two hours. These measurements demonstrate workloads and activity. Metrics are useful for evaluating compliance and process effectiveness and measuring success against established objectives.
Enterprises expect positive outcomes from IT and IT resources, including skilled human resources. To manage the performance of IT, management is interested in getting the answers to the questions in the first column in **figure 1**. The second column shows the type of indicators that are required to get the answers to these questions.

Developing Performance Metrics

Developing performance metrics usually follows a process of:

1. Establishing critical processes to meet customer requirements (This helps enterprises with developing manageable metrics.)
2. Identifying specific, quantifiable outputs of work from the identified processes in step 1.
3. Establishing targets against which results can be scored

Developing metrics includes defining a balanced set of performance objectives, metrics, targets and benchmarks. Metrics should cover activities and outcomes that are measured using lead and lag indicators and an appropriate balance of financial and nonfinancial measures. The metrics should be reviewed and agreed on with IT, other business functions and other relevant stakeholders.[7]

Metrics and indicators are based on information received from operations. When this information represents the measurement of performance, it is

Figure 1—IT Performance Questions

Questions to Which Management Needs Answers	Indicator Type That Can Help to Provide Answers
Are stakeholder expectations from IT achieved?	Lag indicators: • Can be monitored only after activity/process is partially or fully complete. They provide after-the-fact assurance. • Can be quantified
Are business goals achieved? How did IT support the achievement of business goals?	
Do IT resources follow the life cycle?	Lead indicators: • Provide assurance based on a plan/documented processes and implemented best practices • Are primarily qualitative and difficult to quantify
Are the processes in place to monitor the life cycle of IT resources?	
Does the enterprise comply with global and industry-level best practices?	

Source: S. Bakshi. Reprinted with permission.

referred to as means-based metrics. Metrics that are designed to monitor the achievement of objectives are called ends-based metrics. Ends-based metrics may include:

- Changes in an enterprise's inventory of risk exposure (use risk profile report)
- Comparing defined goals of business growth with investment in IT and establishing relationship

Means-based metrics may include:

- The number of application vulnerabilities over one year
- Percentage of automated teller machine (ATM) downtime during active hours (must be less than two percent of active hours)
- Percentage of incidents that are resolved within the SLA time (including escalated incidents)

The following recommendations should be observed while developing metrics and identifying performance indicators:[8]

- **Normalize metrics to a common attribute parameter**—To understand trends properly, normalize metrics to a common parameter; for example:
  - Time—Is time defined as per year occurrence, transactions per second/minute/hour, average interval between events, mean time between failures (MTBF)
  - Cost—Is cost per unit or per million?
- **Understand the characteristics of a good metric**—A good metric allows accurate and detailed comparisons, leads to correct conclusions, is well understood by everyone and has a quantitative basis. A good metric helps to avoid erroneous conclusions. A good metric is linear, reliable, repeatable, easy to use, consistent and independent.
- **Avoid comparisons against other similar enterprises**—Each enterprise is different and may have different goals and objectives. The exception to this is metrics for benchmarking performance. Develop metrics that focus on specific quantified comparisons of documented operational activities that are responsible for contributing to outcomes. Use routines and ratios and avoid wholesale comparisons of business lines because this comparison is subjective and often broad and qualitative.
- **Minimize cost-related comparisons**—Limit cost-related metrics to measure only the benefits (value) from IT. A comparison with the industry or other enterprises may not be relevant. The challenge that enterprises face often is quantifying the outcomes for comparison against costs. For example, a service for improving customer satisfaction may cost enterprises; however, quantifying improved satisfaction of customers may not be possible. In such cases, indirect indicators, e.g., repeat/more business opportunities, may be more useful.

  Another problem is common costs, both internal and external, that include allocations for multiple operations or business lines that cannot be segregated for charging to a specific operation or business line.

"The challenge that enterprises face often is quantifying the outcomes for comparison against costs."

- **Focus on work activities and outcomes**—While developing metrics and indicators, the focus should be on processes and activities for generating and providing data, e.g., the number of cash-related

Enjoying this article?

- **Learn more about, discuss and collaborate on governance of enterprise IT (GEIT) in the Knowledge Center.** *www.isaca.org/governance-of-enterprise-it*

transactions on an automated teller machine (ATM) or the percentage of servers that were patched during a month.

- **Keep metrics to a manageable quantity**—Top management may not be interested in a multipage analytical report or dashboard. Although a large amount of relevant data might be collected during activities, only the most critical metrics should be included in the management report/dashboard.

What Are Good Metrics?

Good metrics generally satisfy the following criteria:[9]

- **Consistently measured**—Metrics must provide similar analysis over a period of time.
- **Easy-to-gather data**—The cost of collecting data for metrics should be low, and the data must be collected through routine operational processes. However, this data collection must satisfy the requirement of being contextually specific. Some service metrics for IT may need more effort and, hence, cost to get data, e.g., how many customers could not be serviced due to an ATM that was not working?
- **Expressed as numbers, percentage or unit of measure**—Numbers and percentages are easy to understand and compare; therefore, as much as possible, metrics should be represented as a number or a percentage.
- **Contextually specific**—IT metrics must measure the achievement of goals or objectives of business; therefore, the metrics must represent the context.

Types of Indicators and Metrics

The need for metrics and indicators is underlined by many organizations, such as the Information Technology Infrastructure Library (ITIL), ISACA® (COBIT 5) and ISO. Although ISO expects a measurement of performance, it does not prescribe any specific indicators. Measurement methods may be defined by organizations.

ITIL defines three types of metrics: technology metrics, process metrics and service metrics. Note that technology and process metrics are also referred to as operational metrics.[10]

Technology Metrics

Technology metrics measure specific aspects of the IT infrastructure and equipment, e.g., central processing unit (CPU) utilization of servers, storage space utilized, network status (e.g., speed, bandwidth utilization) and average uptime (availability of technology).

Most technology metrics provide inputs on IT utilization, which is a very small part of service, to the chief information officer (CIO) or data center manager; however, unless this metric is compared with another metric, it may not provide meaningful information for top management. For example, consider a network response of 100 milliseconds, (i.e., a message reaches its destination in 100 milliseconds). If management expects network response to be 10 milliseconds, the response time requires attention, and if management expects network response to be 300 milliseconds, the response time is more than satisfactory.

Process Metrics

Process metrics measure specific aspects of a process, e.g., number of changes that are rolled back within a month, average incident response time in a month, percentage of employees who attended to task on time, average time to complete a process.

Process metrics provide information about the functioning of processes. These metrics are generally used for compliance conformance that is related to internal controls. However, too many process metrics may not serve the purpose of monitoring. Metrics that are related to critical processes may be considered for management reporting.

Service Metrics

The primary focus of ITIL is on providing service. Service metrics are essential metrics for management

to monitor. They provide an end-to-end measurement of service performance. Defining service metrics can be difficult due to the intangible nature of service levels. Service metrics are more like assessments about what is already known about a problem and are measured in a way that provides ballpark results.[11] When it is difficult to measure the service levels due to associated uncertainty (e.g., unpredictable human behavior) such uncertainty in measuring service levels can be reduced at indicative levels and can be brought within ballpark measurements.

Examples of service-level metrics include the following:

- Results of a customer satisfaction survey indicating how much IT contributes to customer satisfaction
- Cost of executing a transaction (banks use this metric to measure the cost of a transaction that is carried out via different service channels, such as Internet, mobile, ATM and branch)
- Efficiency of service, which is based on the average time to complete a specific service. A service is not just a process; a service can consist of multiple processes.

Many types of metrics are required for a comprehensive understanding of the health of service management throughout the enterprise.

COBIT 5

COBIT 5 is primarily an IT governance framework. Effective governance management must be able to manage risk and meet stakeholder expectations by optimizing resources. COBIT 5 identifies the following seven enablers that help to achieve governance objectives:

- Principals, policies and frameworks
- Processes
- Organizational structures
- Culture, ethics and behavior
- Information (data)
- Services, infrastructure and applications
- People, skills and competencies

Stakeholder expectations help management to arrive at a method for benefits realization, which helps to determine enterprise goals. Because enterprises deploy IT, these goals cascade into IT-related goals, which cascade into enabler goals (see **figure 2**).

To monitor goal achievement, management uses indicators and metrics. COBIT 5 identifies two types of indicators:

- Lead indicators are activities that predict the achievement of goals. These indicators are not measurable, e.g., implementing global or industry best practices or following the life-cycle approach for resources (enablers).
- Lag indicators are measurable and help measure the achievement of goals. Most metrics are defined for lag indicators.

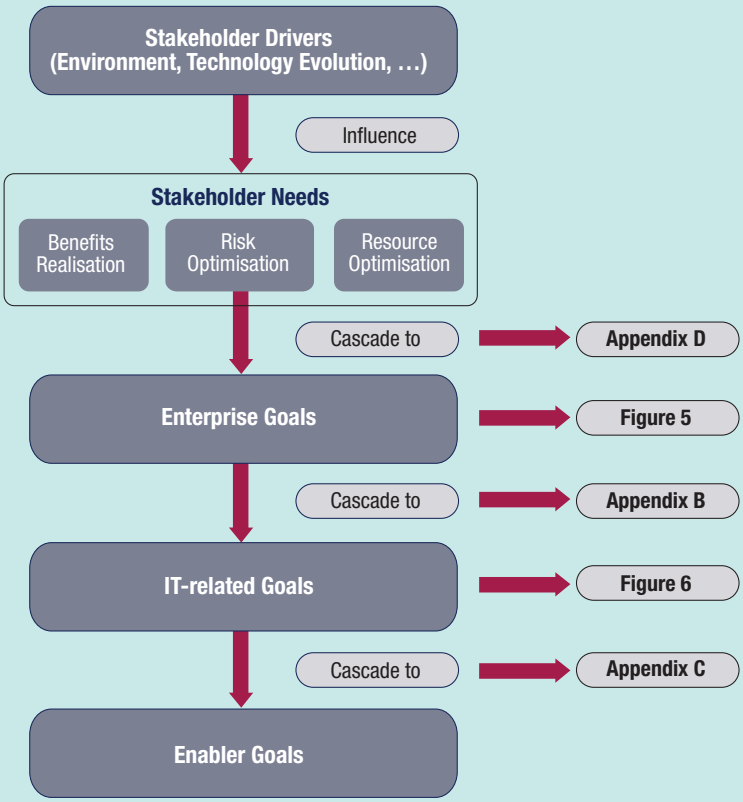
COBIT 5 identifies three levels of metrics: enterprise goal metrics, IT goal metrics and process goal metrics.[14]

Enterprise Goals and Sample Metrics
COBIT 5 identifies 17 generic enterprise goals that are based on dimensions of a balanced scorecard (BSC). These dimensions are financial, customer, internal, and learning and growth.

Generic metrics for IT goals and process goals are defined in the process description for each COBIT 5 process. The COBIT 5 process reference model identifies 37 IT-related generic processes. Metrics can be defined using COBIT 5. Consider the enterprise goal of customer-oriented service culture. COBIT 5 suggests using the following metrics:

- Number of customer service disruptions due to IT service-related incidents (reliability)

Figure 2—COBIT 5 Goals Cascade Overview



Source: ISACA, COBIT 5, USA, 2012

- Percent of business stakeholders satisfied that customer service delivery meets agreed-on levels
- Number of customer complaints
- Trend of customer satisfaction survey results

Depending upon the organization's customer services offered using IT solutions, the following metrics (which shall be a subset of metrics defined previously) may be considered:

- Impact on customer satisfaction due to service disruptions because of IT-related incidents
- Percent of business stakeholders satisfied that customer service delivery meets agreed-on levels
- Reduction or increase in number of customer complaints related to nonavailability of IT-based services

There are two IT-related goals that primarily map to the enterprise goal of customer-oriented service culture.[15] They are IT-related goals 01, Alignment of IT and Business strategy and 07, Delivery of IT services in line with business requirements. Metrics suggested for IT-related goal 07 from COBIT 5 are (for simplicity, only those IT goals that primarily map to the enterprise goal in the example have been considered):

- Number of business disruptions due to IT service incidents
- Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels
- Percent of users satisfied with the quality of IT service delivery

Based on business requirements, the following metrics may be considered:

- Number of IT incidents affecting business service
- Percent of IT incidents affecting business service to total IT incidents
- Number of customer complaints related to service delivery due to issues related to IT

COBIT 5 suggests metrics for each process in the process reference model. The next step is to identify the processes that are associated with the IT-related goal 07. Delivery of IT services in line with business requirements and select the metrics for processes. The following processes depend upon this IT goal:

EDM01, EDM02, EDM05, APO02, APO08, APO09, APO10, APO11, BAI02, BAI03, BAI04, BAI06, DSS01, DSS02, DSS03, DSS04, DSS06 and MEA01.[16]

> **"Every enterprise has unique objectives and, thus, unique metrics."**

Conclusion

Developing, implementing and monitoring performance measurement metrics is key for implementing monitoring mechanisms for goals and objectives that are set by the IT governance processes. Performance measurement metrics should not be copied from similar enterprises. Every enterprise has unique objectives and, thus, unique metrics. This uniqueness is due to many reasons, including business strategy and objectives, enterprise culture, difference in risk factors, risk assessment results, and geopolitical and economic situations.

Enterprises can use generic metrics that are provided by global standards and frameworks such as ITIL and COBIT 5 to define enterprise-specific metrics, which should be mapped to enterprise objectives and goals.

Endnotes

1 Jeffery, M.; "Return on Investment Analysis for E-business Projects," Northwestern University, Evanston, Illinois, USA, *www.kellogg.northwestern.edu/faculty/jeffery/htm/publication/roiforitprojects.pdf*
2 Myers, R.; "Measuring the Business Benefit of IT," CFO.com, 20 October 2004, *http://ww2.cfo.com/strategy/2004/10/measuring-the-business-benefit-of-it/*
3 Bidgoli, H.; *The Internet Encyclopedia, Volume 3,* John Wiley & Sons, USA, April 2004
4 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/cobit/pages/default.aspx*
5 Jaquith, A.; *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, USA, 2007
6 *Op cit,* ISACA, COBIT 5
7 OpsDog, Inc., "What are KPIs & Benchmarks?" 2016, *https://opsdog.com/tools/kpis-and-benchmarks*
8 *Ibid*.
9 *Op cit,* Jaquith
10 Scarborough, M.; "Three Types of Metrics Defined by ITIL," Global Knowledge Training LLC, 12 December 2013, *http://blog.globalknowledge.com/PROFESSIONAL-DEVELOPMENT/ITIL/THREE-TYPES-OF-METRICS-DEFINED-BY-ITIL/*
11 Hubbard, D.; *How to Measure Anything: Finding the Value of Intangibles in Business*, John Willey & Sons, USA, 2007
12 ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*
13 *Op cit,* COBIT 5
14 *Op cit, COBIT 5: Enabling Processes*
15 *Ibid*.
16 *Ibid*.


HISCOX
business insurance
“My business runs on big ideas. And a tiny budget.”
Get a fast, free quote at Hiscox.com/planonit or call our licensed insurance agents at 866-941-2565 Mon–Fri, 8:00am–10:00pm ET. Your policy could start as low as $22.50/mo.
#encouragecourage.
© 2016 Hiscox Inc. All rights reserved.

Assessing Security Controls

Keystone of the Risk Management Framework

feature

CISOs and CSOs need to ensure that their enterprise risk management programs have a solid foundation—the enterprise risk management framework. This framework should provide a disciplined and structured process that integrates risk management activities into the system development life cycle and enables risk executives to make informed decisions. The US National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is such a framework. Commitment to a risk management framework and robust risk principles are critical for a successful risk management program.

Making informed risk decisions involves risk-decision fidelity and steps to determine risk acceptance. A good recipe for making risk decisions includes a mixture of:

- Objective data
- Pass/fail test results
- Mitigations
- Qualitative analysis
- Subjective data
- A healthy portion of intuition

The subjective data may raise eyebrows. This ingredient considers probability and questions who provides the data, as the data source could be important. The intuition portion is also not as objective as facts such as test results. Intuition does not lend itself to a quantitative risk model, rather, qualitative analysis is a key ingredient in the decision-making recipe.

Practitioners inherit a variety of risk management programs in various states over their careers. Some are actually quite good, some are adequate and others are complete disasters. Regardless of the state of the program, sticking to a framework and solid risk principles is critical.

During the last five years, the NIST RMF has gained extensive use across the United States and several other nations. NIST developed and published the elements that an enterprise needs to implement and manage a robust risk management program. The NIST RMF includes the system development life cycle phases and the steps that risk management organizations should follow (**figure 1**).

Test, Test, Test

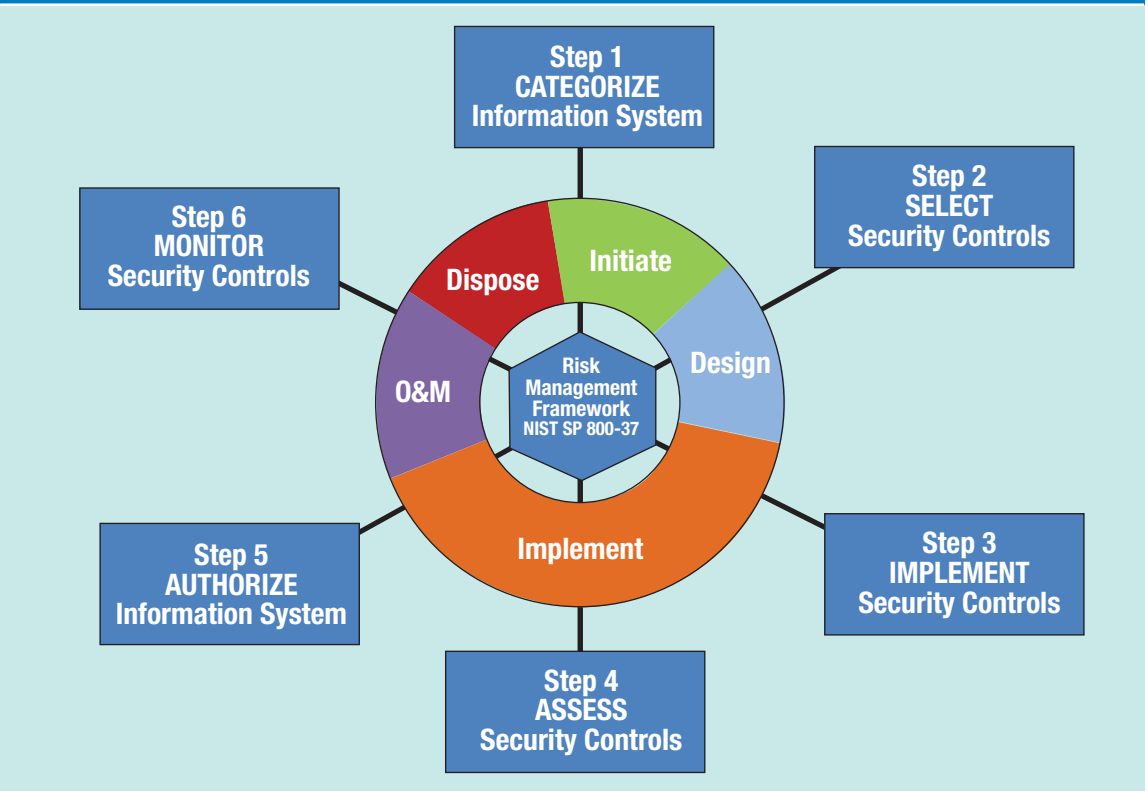
Although all of the steps of the NIST RMF are important, Step 4: Assess Security Controls is the most critical step of a risk management program. Testing the system thoroughly and then performing ruthless configuration management to maintain the security are essential. If the system is tested properly, it will be fundamentally secure. If the enterprise maintains a secure system configuration, the system basically stays at the same level of security. Often, enterprises do not adequately test systems, and the mechanisms to verify accurate auditing of security assessments and other controls are lacking. Nothing can substitute for assessing security controls. Some of the reasons for this lack of security controls assessment are:

- Leadership not providing clear expectations for assessing controls/testing schedules
- Inadequate oversight of the risk management program
- Lack of skilled test managers and testers/security assessors
- Leadership pressure to condense the testing cycle due to the schedule having a higher priority than the security of a system

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 click on the Comments link to share your thoughts.

Lance Dubsky, CISM, CISSP
Is chief security strategist, global government, at FireEye and has more than two decades of experience planning, building and implementing large information security programs. Before joining FireEye, he served as the chief information security officer for two US intelligence agencies, where he led global security programs. In the realm of risk management, Dubsky has served as a senior risk executive, authorizing official, certification official and security control assessor. He managed the transformation to the US NIST Risk Management Framework at two organizations, optimized risk processes by merging risk and system development life cycles, and established a risk assessment process for satellite platforms.

Figure 1—NIST Risk Management Framework



Source: National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems,* NIST Special Publication 800-37, Revision 1, February 2010, figure 2-2. Reprinted with permission.

How testing is audited is also a challenge for enterprises implementing a risk management program. Quality assurance or compliance oversight is often underfunded or lacks the experience to identify the red flags.

The Basic Security Assessment Process

In NIST RMF Step 4: Assess Security Controls, NIST guidelines recommend testing all of the applicable security controls in NIST Special Publication 800-53[1] for which the system has been categorized. The only way to know whether a security control works or not, or passes or fails, is to test it. Testing security controls cannot be achieved through a vulnerability scanning tool, which only checks a small number of security controls. A vulnerability scan often tests a fraction, approximately five percent, of the security controls.

> **"The only way to know whether a security control works or not, or passes or fails, is to test it."**

The role of the security assessor/tester is to test all key security controls for a system and account for all of the security controls for which the system was categorized in step 1 of the NIST RMF. The role may also include the development and execution of the

test plan for the system. The test plan includes all controls for which the system has been categorized. The security assessor executes the test plan with the system owner and records the results. The results of the NIST RMF step 4, which is also referred to as the security assessment phase, include:

- A list of applicable security controls
- A test plan encompassing all of the applicable security controls
- A test report (pass/fail)
- Mitigations for any failed controls

These results are the outcome of a basic security assessment process and provide the risk executive with the information that is required to make a risk decision. Within the US intelligence community, the risk executive is designated by the agency director and is often the chief information officer (CIO), deputy CIO, chief information security officer (CISO) or director of risk management; however, enterprises may designate the risk executive in a different way.

If an enterprise security assessment process does not have this level of integrity and fidelity, risk decisions are being made basically without the necessary information. A great risk management program follows the security assessment process and performs penetration testing after the system is risk accepted and in operation. However, as a risk executive, the most important, the most revealing and the most objective step of the risk management framework is the assessment of security controls. If this risk management phase is not performed correctly, the ability to legitimately accept the risk is virtually impossible.

What Is an Auditor to Do?

Each year, the public sector submits metrics and measures in support of government compliance and reporting requirements. Some of these many metrics include:

- The number of systems that the enterprise operates
- The number of enterprise systems that have an authorization to operate
- The number of enterprise systems that have risk acceptance

The fidelity of measuring the effectiveness of a risk management program rests in whether the security controls are being tested and retested periodically, and whether a record of test results exists.

In the US intelligence community, many auditors and compliance officers, as a normal course of their duties, perform an annual audit of the agency's risk management program and processes to validate whether the program is being run according to standards and to validate the accuracy of the metrics that are being reported. The auditors use a relatively small team, sometimes a third party, to perform the audit. The auditor reviews a subset of the agency systems, because most agencies have hundreds to thousands of systems. Some of the subsets are a small .001 percent of the total number of agency systems. This method does not reveal the true state of the agency risk management program and whether the steps of the RMF, especially testing, are being performed. Too few systems are reviewed and the review is often time consuming.

Audit teams should pivot and focus on a broader set of systems and a more detailed review of the integrity of testing. To broaden the set of systems, the teams will have to be less in-depth on the

Enjoying this article?

- **Learn more about, discuss and collaborate on risk management in the Knowledge Center.** *www.isaca.org/risk-management*

overall review of the system and focus on the most revealing step of the RMF—the available evidence to determine the integrity of step 4. If the organization has 1,000 systems, the organization should have 1,000 test plans and the test results for each system. The exception would be if the systems use centralized security services available from the enterprise. If audit teams can determine the existence of system test plans and test results and interview the security assessors, the teams can accurately determine whether the system was tested completely and whether the risk executive has the most objective data to make a risk decision. If the system is not tested or inadequately tested, the risk acceptance or authorization to operate should be invalidated.

> **"If the system is not tested or inadequately tested, the risk acceptance or authorization to operate should be invalidated."**

Enterprise leadership needs to set expectations for the enterprise risk management program and how the program will be measured, especially the security assessment phase of the risk management framework. For auditors, asking the right questions is crucial to discovering the true state of how the risk management program is working and the integrity of the program. The following specific requests can reveal a great deal to an audit team, to a CISO and to the CIO:

- Archive of test plans for each system, with test result, per system. A test plan will have all security controls for which the system was categorized.
- How many of the security controls were tested manually? Who performed the test?
- How many of the controls were tested with a tool or application? Which tools were used and what specific controls did each tool test?
- Of the total number of security controls, how many passed?
- Of the total number of security controls, how many failed? What were the compensating mitigations? Was the mitigation tested?
- Where is this system physically set in the enterprise and to what is it connected?
- Does the system security documentation reflect all of the above?

If an enterprise uses the NIST RMF and the risk management program can successfully answer the questions for each of its systems, the foundation of the risk management program is solid. No program is perfect; however, if an enterprise is assessing security controls with a high degree of fidelity and the auditor can verify this fidelity, then the enterprise risk management program is in good, if not great, shape.

Endnotes

1 National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, USA, April 2013, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

Delivering Personal Data Protection Compliance on a Global Scale

Disponible également en français
www.isaca.org/currentissue

On 4 May 2016, after four years in the making, the European Union (EU) General Data Protection Regulation (GDPR) was published in the *Official Journal of the European Union*[1] and officially set an application date.[2] While the regulation entered into force on 24 May 2016, it applies going forward beginning on 25 May 2018. The GDPR is working in conjunction with, and expanding upon, the EU Directive regarding the processing of personal data to achieve the common goals of personal data protection, crime investigation and prosecution. This partnership is unveiling sweeping updates to data protection rules of which the world has not seen the likes in more than 20 years.

> *The vast majority of respondents (84 percent) indicated that they anticipate that the GDPR will impact their organization.*[3]

The new GDPR, put forth by the European Commission in 2012 and generally agreed upon by the European Parliament and Council in December of that same year, is set to replace Data Protection Directive 95/46/EC. Over the past four years, proactive companies have implemented the necessary privacy processes and procedures that comply with Directive 95/46/EC. Companies will need to do the same once again for the new protections for EU data subjects when the GDPR begins to be enforced. Substantial fines and penalties will be imposed on companies with noncompliant data controllers and processors.

The impact of this new regulation is completely pervasive. Companies with more than 250 employees that process personal data of EU citizens will be subject to the GDPR. Not only that, but GDPR applies to all private sector personal data processing by organizations of the EU and organizations outside the EU that target EU residents. Wherever such organizations transfer personal data to the EU, the GDPR's impact will be felt. Rest assured, the export regime will make sure of that. Companies meeting these definitions will be forced to comply or abandon any opportunity to engage with the significant audience of EU customers. Stiff penalties for noncompliance include fines greater than €20 million, or approximately US $23 million, and 4 percent of the company's global revenue.

Although companies of all sizes will be challenged, the GDPR most significantly impacts global companies with a broad international presence. These challenges arise from companies having to expand the scope of already very complex IT landscapes and from the cross-border transmission of personal data.

Turning Cost Into Value

Usually, any compliance is perceived as a cost. Effective companies and their leaders successfully generate value for businesses and their customers by designing and deploying responsive data privacy and compliance programs.

For example, the leading global energy management and automation provider proposed three major objectives for its worldwide personal data protection compliance initiative:

1. Put the US $1.2 billion risk of breaching personal data protection regulations[4] under control in the EU and other countries where the company operates.

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 click on the Comments link to share your thoughts.

Ilya Kabanov, Ph.D.
Is an information technology expert with 15 years of experience in enterprise IT. He has held leading transformation roles in IT strategy, technology project management, security and data privacy in companies ranging from a successful start-up to a global US $36 billion enterprise. Currently, Kabanov provides leadership to a global applications security and personal data privacy compliance initiative for a top global energy management and automation provider. In 2013, *Kommersant Magazine* recognized him as Russia's best chief information officer in the logistics and transportation industry. Kabanov is a member of the Institute of Electrical and Electronics Engineers and the International Association of Privacy Professionals and serves as a judge at the MIT Sloan CIO Symposium.

2. Enable and support the growth of revenue and a rich customer experience in the area of mobile solutions and connected Internet of Things (IoT) solutions the company offers:

How leaders generate value through compliance:
- Expand customer satisfaction and build trustful relationships with clients
- Enable revenue growth
- Lower the cost of compliance

3. Achieve a reduction in the cost of compliance with personal data protection legislation. One way to do this is by utilizing binding corporate rules through the application of different compliance methods, including self-certification, with respect to the risk profile of IT applications and systems involved in personal data processing.

In addition, the company believes its global responsibility goes beyond regulatory compliance. The company has solid principles of conducting business ethically, sustainably and responsibly around the globe. Responsibility is the key objective at the heart of the company's corporate governance. This determines the commitment of the company to set and meet the highest standards in ethics and privacy, and enables it to shape the future of the industry by introducing tomorrow's best practices today.

> **"Every company's goal is compliance, but also to seek it in such a way that sustains growth and profitability."**

Every company's goal is compliance, but also to seek it in such a way that sustains growth and profitability. This is not an easy task, as each company will face multiple challenges in an attempt to reach compliance.

Challenges

The GDPR and national personal data protection regulations push the need for organizations to develop and deploy risk and compliance frameworks that span numerous internal departments, including legal, security and IT, all while staying in accordance with differing legislations across multiple jurisdictions around the world. While there are different views on the processes that global organizations can adopt to establish and manage regulatory and compliance risk factors, the challenges that enterprises need to consider are actually very common. They are:

- **Complexity**—The volume and increasing complexity of the personal data protection regulatory landscape have gained momentum, particularly in the EU, the United States and some emerging countries. Global companies need to comply with a variety of regulatory legislation on national levels and ensure compliance across all business dimensions such as countries, data types and volumes, and various residencies of data processors.
- **Agility and consistency**—Agility is a necessary factor. Laws and regulations change constantly, and the time it takes for new IT products to reach the market is shrinking. Compliance with these changes must also reflect a condensed time frame to be effective. Companies must bring consistency to their compliance structures. It needs to be in real time and accurately reflect changes in rules and new regulations. Each company needs to develop and be aligned with rapid delivery cycles of IT systems and products. Compliance with new regulations means making sure that multiple systems and multiple processes are compliant, not only at implementation, but throughout the structure's life cycle.
- **Experts' capacity and availability**—The lack of IT security expertise and the scarcity of experts in the personal data protection field slow down and complicate the process of building compliance frameworks. Global companies fight for the limited number of experts who can lead complex data protection compliance programs and often experience challenges in educating employees about personal data protection.

Although companies face daunting challenges such as scale, geographic diversity, competing priorities and communications, the outlook for these companies is not all bleak. There are certain factors that will help forge a compliance framework with a great chance for success.

Real-life Frameworks

One of the examples of successful compliance frameworks was demonstrated by a global company that introduced the certification framework to ensure the security and compliance of IT applications and systems, thus guaranteeing clients, customers and employees the adequate protection of their personal and corporate data, entitlement to rights granted by legislation, and compliance with corporate and industrial standards and policies. The framework was designed to cover more than 1,000 software applications released annually, which store billions of records of structured and unstructured data and are accessed by millions of people worldwide.

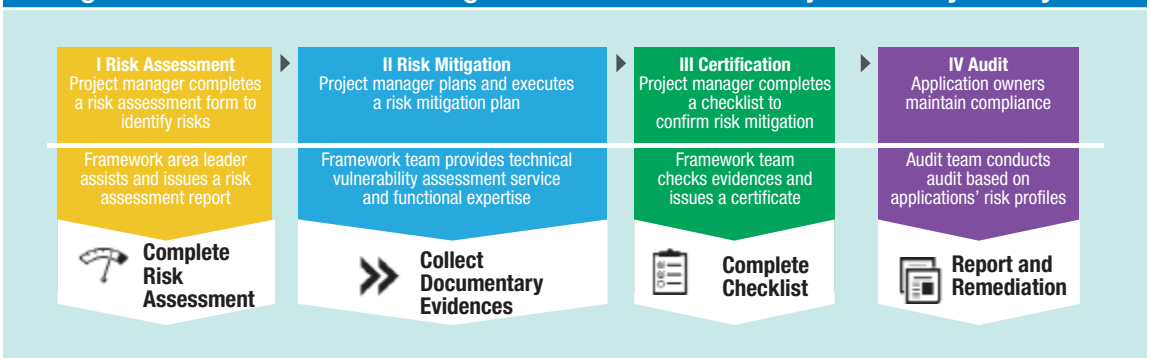
At an early stage of framework development, it was recognized that the compliance process should comprehensively cover the application's journey along the whole life cycle from idea to retirement and ensure the privacy-by-design concept and data protection at every stage. The framework is based on a four-step process including risk assessment, risk mitigation, certification and post-certification audit phases (**figure 1**).

> *Once we estimated that we needed to educate 2,500 key stakeholders on a process change to achieve a high level of awareness, we collaborated with our internal communication department to design and run a yearlong multi-channel communication campaign. We leveraged internal social media, webinars, and e-learning to drive the framework's adoption, data privacy, and security risk awareness culture globally. Our goal was not only to embed the framework we designed into existing processes, but ensure that compliance becomes a part of the professional knowledge of project managers, and application delivery and operations teams.*
>
> – Enterprise Architecture Director

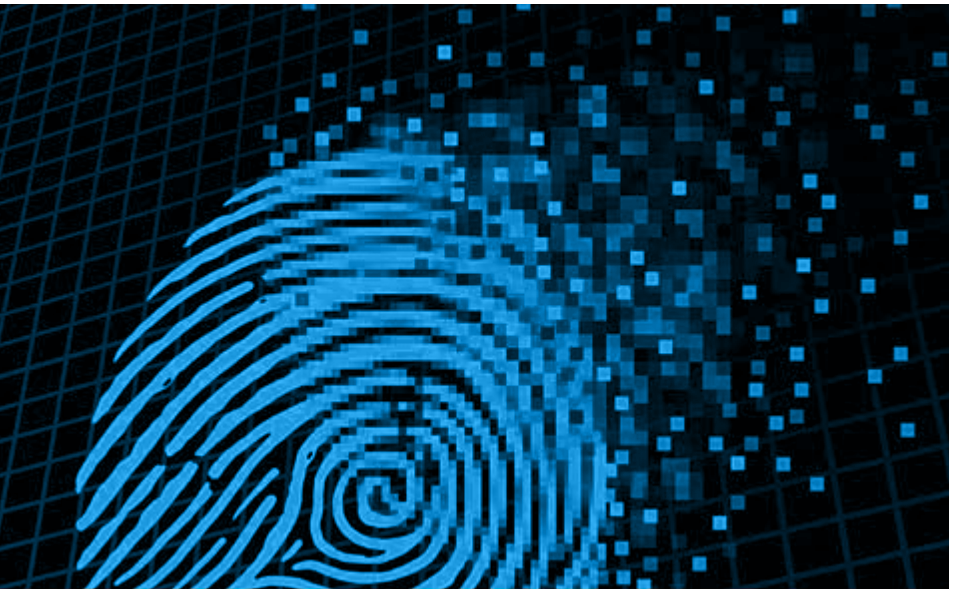
There are four main challenges in driving the framework design adoption:

1. The complexity of the external and internal regulatory environments. The framework had taken more than 200 laws, policies, standards and guidelines into account and then simplified them into applicable risk assessment procedures, recommendations and controls.
2. The initial maturity of policies required intensive involvement of experts for assessing risk, guiding project delivery teams on implementation and applying controls. This was a serious

Figure 1—The Phases of Ensuring Data Protection in the Project Delivery Life Cycle



Source: I. Kabanov. Reprinted with permission.



impediment for scaling the framework, therefore, the team tackled the challenge by applying an experimentation approach. This enabled the team to develop best practices and document them in the forms of hands-on guidelines for project delivery teams and application owners.

3. The complexity of an existing IT landscape where the data are processed became an additional challenge. Because of this hurdle, the team put a lot of effort into learning about the existing architecture and mapping data.
4. The large scale of the program's implementation, diverse geography of deployment and the inconsistent level of awareness about data privacy among 2,500 key stakeholders spread across all 24 time zones created a significant challenge for the rapid deployment of the framework.

The framework was the result of perfectly orchestrated and consolidated work of team members from all continents representing key functional verticals. The team has worked tirelessly across cultures, languages and time zones, all while staying focused on designing and deploying this framework.

Factor of Success

Design and deployment of compliance programs vary greatly. Each organization needs to ensure that compliance is properly embedded into current organizational processes. The more complex the organization, the more difficult it will be to ensure that privacy programs or initiatives are integrated into, or throughout, the organization.

The highest level of integration of a compliance framework into existing project and program management processes guarantees the robustness and comprehensiveness of its free-of-redundancy controls. As an example, the framework needs to be aligned with processes that may have different names in organizations, such as end-to-end project excellence and software development life cycle governance. This will help make sure that applications processing data follow the framework to ensure security and compliance at every stage of the life cycle, along with executing privacy-by-design and security-by-design principles.

Communication is a critical part of successful integration of the framework into a company's operations and projects delivery routine. Communication at the large scale of the project is a challenging exercise. To achieve success, teams need to partner with a variety of stakeholders, then design and drive a multiwave communication campaign as part of a change management process to raise awareness about the framework and educate project delivery teams on key data privacy and security risk.

Communication supports collaboration, which a recent International Association of Privacy Professionals (IAPP) survey of 550 privacy, IT and information security professionals indicated as critical in addressing data breaches. Indeed, 90 percent of those surveyed considered collaboration among the privacy, security and IT departments, together with a strong data breach response team, as most important for mitigating the risk of a data breach.[5]

Compliance to personal data privacy issues is not solely the purview of IT departments. All facets of an organization must be committed to implementing any new rules and regulations and integrating those new factors throughout every department and at every organizational echelon of the company.

Beyond Compliance

Company leaders demonstrate ethical leadership in their industries and use ethical conduct as a profit driver and competitive differentiator. A compliance framework can serve as a key component of the global cyber security and compliance portfolio of initiatives. It aims to enable and support revenue growth and provide flawless, safe and secure customer and employee experiences. While customers ask for improved productivity, precision and efficiency, companies should answer those needs through trustworthy relationships guaranteeing to customers and partners the highest level of data privacy, as well as confidentiality, integrity and availability of the information.

In addition, compliance frameworks can play a crucial role in reducing project and product delivery life cycles to support strategic business growth in primary market target areas of mobile solutions and connected IoT offerings.

Conclusion

Companies of all sizes are likely to find that GDPR compliance and implementation will not be easy. It will require thorough and flawless integration into each company's unique processes, which, in turn, will require emphasis on adequate communication and regulatory education. Most global companies are already looking to build strong compliance frameworks based on International Organization for Standardization (ISO) standards[6] and are waiting for publication of ISO/International Electrotechnical Commission (IEC) 29151:2015 Information technology—Security techniques—Code of practice for personally identifiable information protection[7] and ISO/IEC DIS 29134:2016 Information technology—Security techniques—Privacy impact assessment–Guidelines.[8]

Volatility of the regulatory environment and rapid, unpredictable geopolitical changes demand that global organizations have truly robust compliance frameworks to address possible changes in the organization's compliance needs, as well as evolving external requirements. Brexit is a perfect example of how the UK leaving the EU, coupled with the GDPR, will make compliance more challenging for global firms.

Because the UK's actual exit from the EU will take place after 25 May 2018, it is important to note that EU companies will still need to comply with GDPR. All companies processing data of UK citizens at that time will be required to comply with the UK legislation.

> **"A compliance framework can serve as a key component of the global cyber security and compliance portfolio of initiatives."**

Steve Wood, interim deputy commissioner at the UK Information Commissioner's Office (ICO), says, "The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to the British government to explain our view that reform of UK data

protection law remains necessary."[9] Essentially, this means the UK will be evolving data protection laws and demanding organizations serving UK customers to ensure compliance in addition to the GDPR.
It is important to remember that personal data protection regulations are mostly designed to help organizations achieve best practices for data protection; they are actually a good set of rules to follow. Fundamentally, the majority of personal data protection compliance requirements demand privacy by design, good information management policies, and reasonable security measures, procedures and technologies to minimize possible data loss incidents. Therefore, organizations that have designed and deployed robust compliance frameworks with a reasonable granularity of controls will be able to apply them widely, while also addressing possible regulatory changes and shifting compliance needs, to safely protect personal data and enable business opportunities.

Endnotes

1 Official Journal of the European Community, *www.ojec.com/*
2 Official Journal of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," 4 May 2016, *http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*
3 Baker and McKenzie, "Preparing for New Privacy Regimes: Privacy Professionals' Views on the General Data Protection Regulation and Privacy Shield," April 2016, *http://f.datasrvr.com/fr1/416/76165/IAPP_GDPR_and_Privacy_Shield_Survey_Report.pdf*
4 European Commission, "Protection of Personal Data," *http://ec.europa.eu/justice/data-protection/*
5 International Association of Privacy Professionals, "How IT and Infosec Value Privacy," *https://iapp.org/resources/article/how-it-and-infosec-value-privacy/*
6 International Organization for Standardization, ISO/IEC 27018:2014 *Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*, 1 August 2014, *www.iso.org/iso/catalogue_detail.htm?csnumber=61498*
7 International Organization for Standardization, ISO/IEC DIS 29151 Information technology—Security techniques—Code of practice for personally identifiable information protection, 5 July 2016, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62726*
8 International Organization for Standardization, ISO/IEC DIS 29134 *Information technology—Security techniques—Privacy impact assessment—Guidelines*, 18 July 2016, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289*
9 Wood, S.; "GDPR Still Relevant for the UK," Information Commissioner's Office, 7 July 2016, *https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/*

Enhancing the Audit Follow-up Process Using COBIT 5

COBIT® 5 for Assurance builds on the COBIT® 5 framework by providing detailed and practical guidance for assurance professionals on how to use COBIT 5 to support a variety of IT assurance activities.

One of the key IT assurance activities is ensuring that risk has been mitigated. *COBIT 5 for Assurance* requires that, where appropriate, recommendations should include provisions for timely monitoring and follow-up.[1]

Implementing an audit follow-up process using the COBIT 5 enablers and ISACA's Information Technology Assurance Framework (ITAF)[2] provide value to the enterprise.

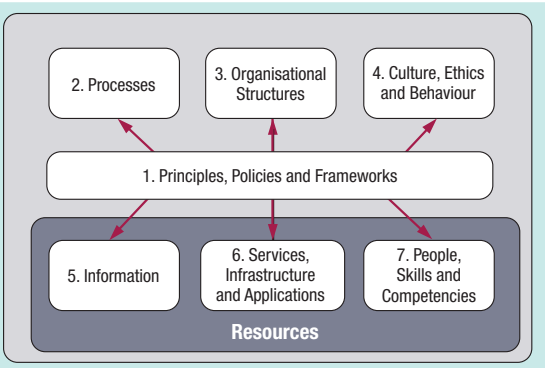
COBIT 5 Enablers and the Audit Follow-up Process

Enablers are factors that, individually and collectively, influence whether something will work. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve.[3] The COBIT 5 framework describes seven categories of enablers (**figure 1**). *COBIT 5 for Assurance* reviews each of these enablers, highlighting the assurance perspective. This article follows a similar methodology focusing on the audit follow-up process.

Principles, Policies and Frameworks
Principles, policies and frameworks are the vehicles to translate the desired behavior into practical guidance for day-to-day management.[4]

Practical guidance for audit follow-up activities are included in ITAF. Specifically, standard 2402, Follow-up Activities,[5] requires IS audit and assurance professionals to monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations.

Figure 1—COBIT 5 Enterprise Enablers



Source: ISACA, COBIT® 5, USA, 2012

Processes
Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.[6]

Processes require good practices. These are provided by the ITAF guideline 2402,[7] which documents guidelines on confirming the actions taken in response to audit recommendations. Processes should also have a life cycle. This is documented in the 2402 guideline as:

- 2.1 Follow-up process
- 2.2 Management's proposed actions
- 2.3 Assuming the risk of not taking corrective action
- 2.4 Follow-up procedures

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 click on the Comments link to share your thoughts.

Ian Cooke, CISA, CGEIT, CRISC, COBIT Foundation, CFE, CPTS, DipFM, ITIL Foundation, Six Sigma Green Belt
Is an IT audit manager based in Dublin, Ireland, with more than 25 years of experience in all aspects of information systems. A member of ISACA's Communities Working Group, he is also the topic leader for the Oracle Databases, SQL Server Databases and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke welcomes comments or suggestions at *Ian_J_Cooke@hotmail.com* or on the Audit Tools and Techniques topic in the ISACA Knowledge Center.

- 2.5 Timing and scheduling of follow-up activities
- 2.6 Nature and extent of follow-up activities
- 2.7 Deferring follow-up activities
- 2.8 Form of follow-up responses
- 2.9 Follow-up by professionals on external audit recommendations
- 2.10 Reporting of follow-up activities

The steps suggest that audit recommendation items have different statuses as they flow through the life cycle. **Figure 2** summarizes the statuses that an action may have through its life cycle.

Organizational Structures

Organizational structures are the key decision-making entities in an enterprise.[8] Good practices here include defining the operating principles, the span of control, the level of authority, the delegation of authority and the escalation procedures for audit recommendation items. The best way to do this is using a responsible, accountable, consulted and informed (RACI) chart. A suggested RACI chart for the audit follow-up process can be seen in **figure 3**.

Culture, Ethics and Behavior

Culture, ethics and behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.[9] For the audit follow-up process, the focus is on confirming the implementation of audit items. Good practices are discussed in **figure 4**.

Figure 3—Audit Follow-up RACI Chart

Responsible	Auditee—Issue manager
Accountable	Auditee's manager—Issue owner
Consulted	Risk management, compliance, legal, etc.
Informed	Board, audit committee, external audit

Source: Ian Cooke. Reprinted with permission.

Information

Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and properly governed.[10]

Information about the audit follow-up items should be captured in an assurance findings register. This is a register of issues/findings raised during assurance activities. It is maintained and followed up on to

Figure 2—Audit Recommendation Statuses

Status	Description	Related Date
Draft	The action has yet to be agreed upon with management.	Date raised
Outstanding	The action has been agreed upon with management, but has not yet been implemented.	
Partially implemented	The action is a work in progress; some elements have been implemented.	
Fully implemented	Management has indicated that all elements of the agreed-upon action have been completed.	Fully implemented date
Confirmed	Internal audit has confirmed, via follow-up procedures, that the agreed-upon action has been completed.	Date closed
Deferred	The action has been deferred until a later date (e.g., it may be dependent on another action, activity or upgrade).	Date closed
Disagreed	Management has decided against implementing the agreed-upon action.	Date closed

Source: Ian Cooke. Reprinted with permission.

ensure that significant issues/findings have been acted on as agreed upon in assurance reports.[11] **Figure 5** shows the data items that should be captured at a minimum.

Figure 4—Culture, Ethics and Behavior Good Practices

Communication	The purpose of the audit follow-up process should be documented and communicated to all employees, but especially those identified in **figure 3**.
Champions	Employees who are willing and/or able to champion the follow-up process should be identified.
Enforcement	There may be a need for enforcement. For example, there may be a need for a human resources (HR) policy stating that any misrepresentation by auditees will result in disciplinary action.
Incentives and rewards	Completion of audit recommendations items could form part of the auditee's incentives schemes.

Source: Ian Cooke. Reprinted with permission.

Figure 5—Assurance Findings Register Minimum Data Items

A unique reference number
The report reference
A description of the item/risk
Significance—denotes the level of perceived risk
A description of the proposed solution/mitigation
The proposed implementation date

Source: Ian Cooke. Reprinted with permission.

However, it is advantageous to add additional data items. *COBIT® 5: Enabling Information* describes information attributes. Specifically, semantics refers to the meaning of information.[12] One can add to the meaning of information by adding data items (**figure 6**).

Other items may be applied that add meaning to the enterprise.

Figure 6—Assurance Findings Register Suggested Additional Data Items

Recommendation theme
Company, division
Country
Related framework/regulation

Source: Ian Cooke. Reprinted with permission.

Services, Infrastructure and Applications
Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.[13]

From an audit follow-up perspective, what is really required is a facility to store the assurance findings register and produce reports based upon the same. This may be an application (e.g., audit management software) or Microsoft Excel/Access. Workflow-type applications may also be helpful for requesting and following up on the recommendations.

People, Skills and Competencies
People, skills and competencies are required for the successful completion of all activities and for making correct decisions and taking corrective actions.[14]

The auditor must be competent and have the necessary skills to confirm the implementation of the audit item. The auditor should know or have an idea in advance of what would be acceptable to confirm implementation. This may vary depending on the significance of the item. A Certified Information Systems Auditor® (CISA®) qualification and familiarity with ITAF would also be of benefit.

Bringing It All Together—The Audit Follow-up Process in Action

Management's Proposed Actions
The follow-up process begins with the creation of the audit report, specifically, at the time recommendations are made and management's proposed actions[15] are documented. **Figure 7** documents what should be captured at this stage.

Enjoying this article?

- Read *Information Systems Auditing: Tools and Techniques—IS Audit Reporting.* *www.isaca.org/tools-and-techniques*
- Learn more about, discuss and collaborate on using COBIT® 5 in the Knowledge Center. *www.isaca.org/cobit-5-use-it-effectively*

Figure 7—Sample Audit Recommendation Item

Data Item	Reference	Example
A unique reference number	**Figure 5**	3434
The report reference	**Figure 5**	2016/05
A description of the item/risk	**Figure 5**	There was no service level agreement (SLA) defined….
Significance—denotes the level of perceived risk	**Figure 5**	3 (1 is highest)
A description of the proposed solution/mitigation	**Figure 5**	An SLA will be defined….
The proposed implementation date	**Figure 5**	09/30/2016
Auditee—issue manager	**Figure 3**	IT manager 4
Auditee's manager—issue owner	**Figure 3**	Executive 2
Status	**Figure 2**	Outstanding
Date raised	**Figure 2**	06/30/2016
Fully implemented date	**Figure 2**	
Closed date	**Figure 2**	
Recommendation theme	**Figure 6**	SLAs
Company, division or location	**Figure 6**	Dublin
Country	**Figure 6**	Ireland
Related framework/regulation	**Figure 6**	COBIT 5 APO09

Source: Ian Cooke. Reprinted with permission.

Follow-up Procedures

Once the proposed actions are agreed upon, procedures for follow-up activities should be established.[16] This should include:

- An evaluation of management's response
- A verification of the response, if appropriate
- Follow-up work, if appropriate

Upon completion of the follow-up activities, the status of the audit recommendation item should change. For example, the recommendation status may change from "outstanding" to "partially implemented," "fully implemented" or, if verified, "closed."

The significance can also change. This could occur where application systems have changed, compensating controls have been implemented, or business objectives or priorities have changed in such a way as to effectively remove or significantly reduce the original risk.

Assuming the Risk of Not Taking Corrective Action

Management may decide to accept the risk of not correcting the reported condition because of cost, complexity of the corrective action or other considerations.[17] In such circumstances, the recommendation may be disagreed with or deferred until a later date.

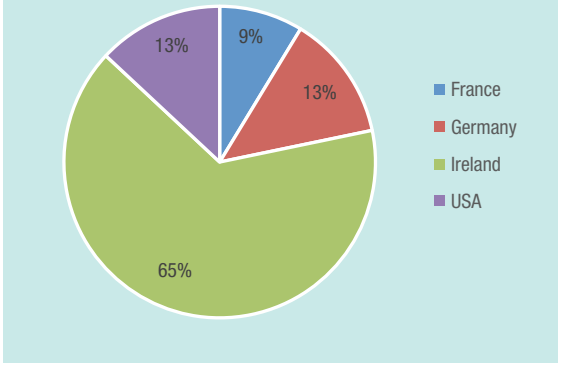
Reporting of Follow-up Activities

ISACA's documentation recommends that a report on the status of agreed-upon corrective actions arising from audit engagement reports, including agreed-upon recommendations not implemented,

should be presented to the appropriate level of management and to those charged with governance (e.g., the audit committee).[18]

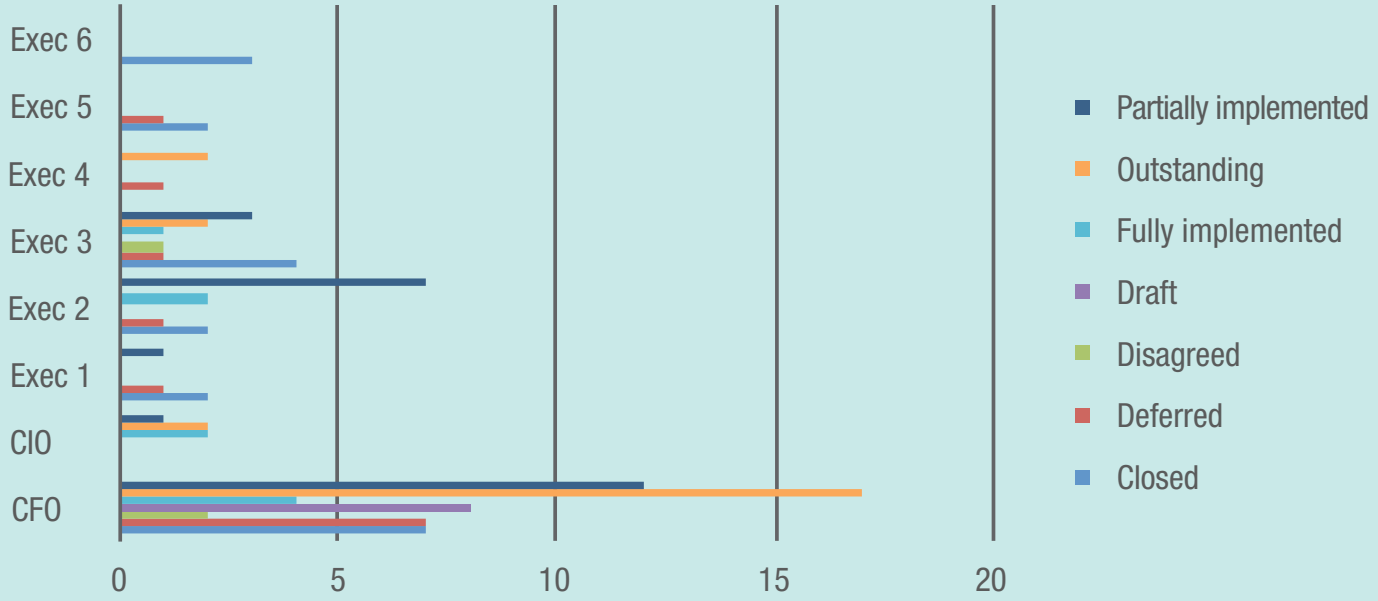
Reporting on the status of individual items is good practice. However, by collecting the information suggested earlier, together with the tracked statuses and related dates, more can be done. First, by using Excel pivot tables (or a similar tool) the data can be aggregated. This can then be used to show how entire sections, divisions, countries or owners are performing (**figures 8** and **9**).

Figure 8—Sample Summary—Outstanding by Country



Source: Ian Cooke. Reprinted with permission.

Figure 9—Sample Summary—Status by Owner



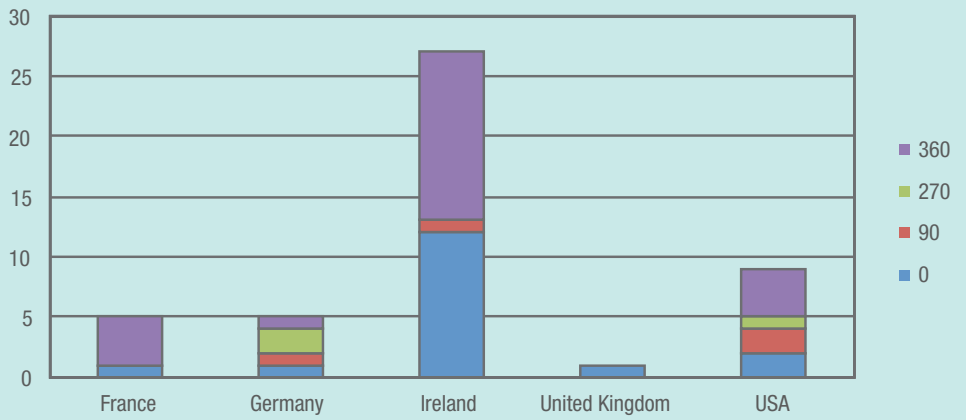
Source: Ian Cooke. Reprinted with permission.

Excel pivot tables can also be used to summarize the audit recommendations statuses into formats with which management will be familiar (**figure 10**).

Or, they can be used to demonstrate compliance to the enterprise's standards (**figures 11** and **12**).

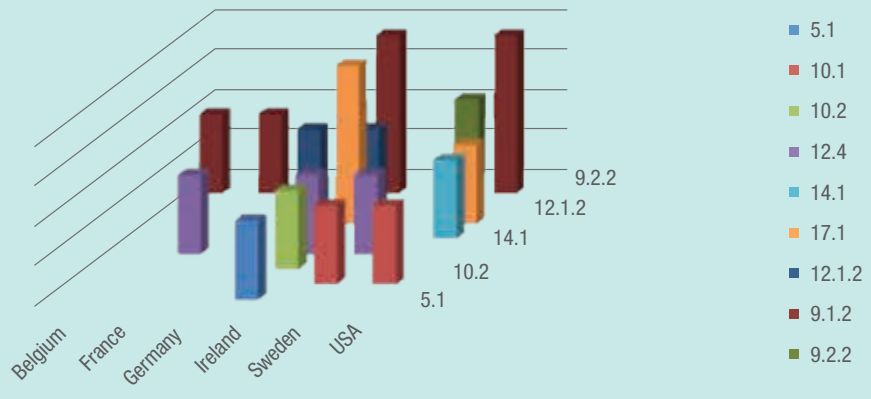
These examples indicate pain points and are very much lag indicators. However, a careful review of the allocated themes reveal that they can also be considered lead indicators. For example, if a new application is going to be implemented in Ireland, there are likely to be issues with authentication and authorization (**figure 13**).

Figure 10—Sample Summary Overdue Items by Number of Days



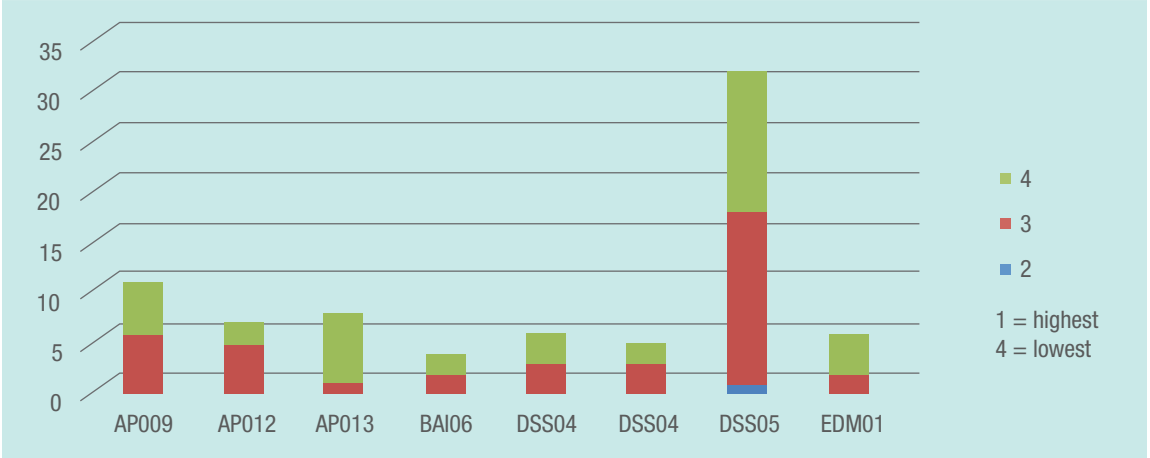
Source: Ian Cooke. Reprinted with permission.

Figure 11—Sample Summary Closed Items by International Organization for Standardization (ISO) Clause



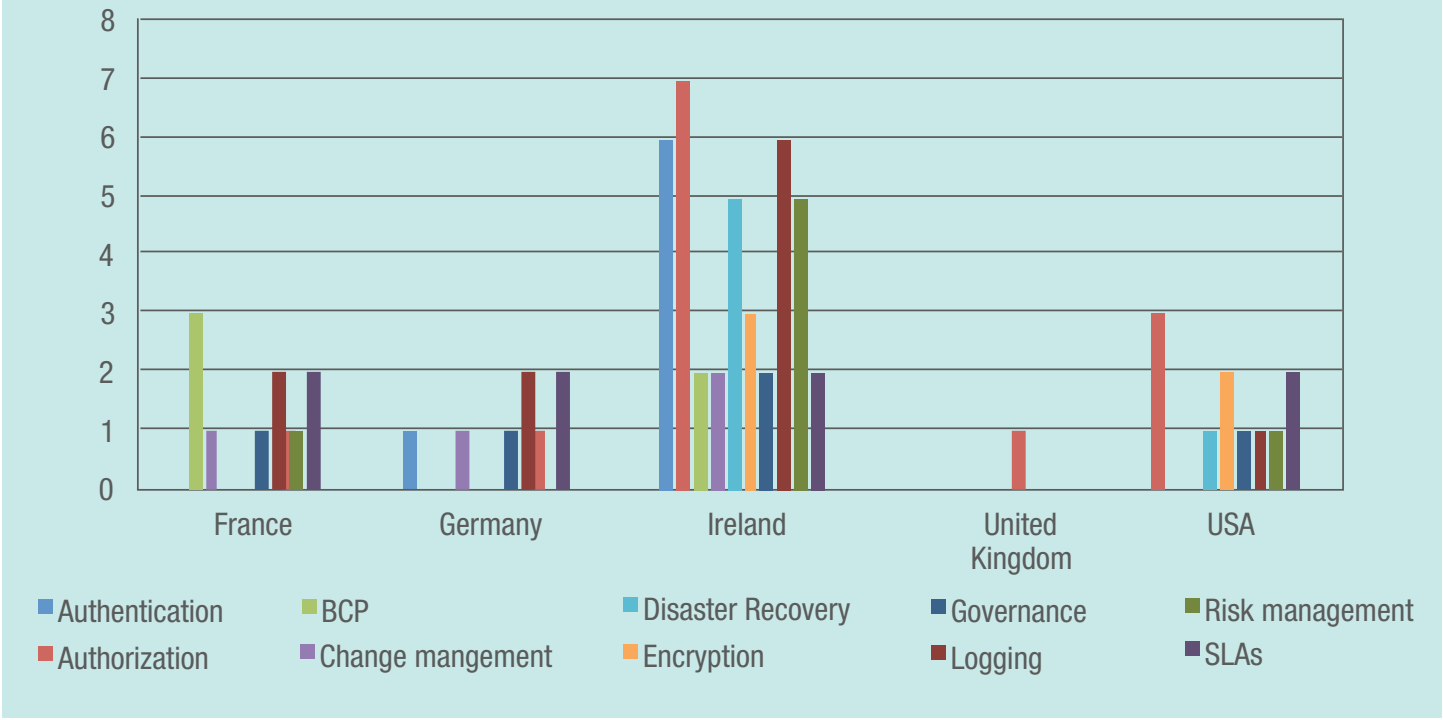
Source: Ian Cooke. Reprinted with permission.

Figure 12—Sample Summary—Significance by COBIT 5 Reference



Source: Ian Cooke. Reprinted with permission.

Figure 13—Sample Summary—Open Items by Theme



Source: Ian Cooke. Reprinted with permission.

Benefits of the Enhanced Audit Follow-up Process

Capturing the audit recommendation statuses in an assurance findings register means that, as per good practice, a report on the status of agreed-upon corrective actions can be presented to senior management and the audit committee. However, by capturing the suggested additional information, one can:

- Present summarized information by country/department/region/owner
- Present the information in a format with which executives are familiar
- Clearly show compliance to standards and regulation
- Use the information as a lead indicator for new initiatives

This gives a better perspective of the risk affecting different areas of the enterprise.

Endnotes

1 ISACA®, *COBIT® 5 for Assurance*, USA, 2013, p. 17, *www.isaca.org/COBIT/Pages/Assurance-product-page.aspx*
2 ISACA, *ITAF™: A Professional Practices Framework for IS Audit/ Assurance, 3rd Edition*, USA, 2014, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITAF-3rd-Edition.aspx*
3 ISACA, COBIT® 5, USA, 2012, p. 27, *www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx*
4 *Op cit*, COBIT 5, p. 27
5 *Op cit*, ITAF, p. 39
6 *Op cit*, COBIT 5, p. 27
7 *Op cit*, ITAF, p. 141
8 *Op cit*, COBIT 5, p. 27
9 *Ibid*.
10 *Ibid*.
11 *Op cit*, *COBIT® 5 for Assurance*, p. 45
12 ISACA, *COBIT® 5: Enabling Information*, USA, 2013, p. 37, figure 28, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product-page.aspx*
13 *Op cit*, COBIT 5, p. 27
14 *Ibid*.
15 *Op cit*, ITAF, p. 142
16 *Ibid*.
17 *Ibid*.
18 *Ibid*.

Advanced Data Analytics for IT Auditors

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 click on the Comments link to share your thoughts.

Data analytics is a must-have capability for the audit function[1] and widely expected to become a big part of its future.[2]

Data analytics is defined as, "the science of examining raw data with the purpose of drawing conclusions about that information..."[3] The definition continues, stating:

> *The science is generally divided into exploratory data analysis (EDA), where new features in the data are discovered, and confirmatory data analysis (CDA), where existing hypotheses are proven true or false... In information technology, the term has a special meaning in the context of IT audits, when the controls for an organization's information systems, operations and processes are examined. Data analysis is used to determine whether the systems in place effectively protect data, operate efficiently and succeed in accomplishing an organization's overall goals.*[4]

Spiros Alexiou, Ph.D., CISA
Is an IT auditor who has been with a large company for eight years. He has more than 20 years of experience in IT systems and data analytics and has written numerous sophisticated computer programs. He can be reached at *spiralexiou@gmail.com.*

Numerous disciplines use simple and advanced data analytics for:

- **Classification**—Identifying good customer/bad customer and fraud/no fraud
- **Clustering**—Identifying groups with similar behavior
- **Association**—Determining that everyone who bought item A also bought item B, and 80 percent of them also bought item C
- **Summarization**—Describing groups with certain characteristics (e.g., executives with average use of company card totals greater than **x** dollars)
- **Link analysis**—Determining connections (e.g., A called B, and B immediately called C, hence, A may be linked to C)
- **Deviation detection**—Identifying transactions significantly different from the average
- **Prediction/estimation**—Predicting trends or growth of a new business
- **Visualization**—Perhaps this is not data analytics proper, but aids in nonautomated human discovery (e.g., charts or medical imaging)

Two Categories of Data Analytics

Data analytics techniques generally belong to one of the following two categories:

- **Simple**—One knows what one is looking for. The first category typically has a well-defined rule or threshold and looks for violations (e.g., all transactions with monetary value larger than a certain threshold or all retired employees who continue to have access to IT systems). The first category of analytics usually employs queries to a database or spreadsheets. Audits use this category of analytics extensively. As data size increases, auditors often rely on aggregated data that IT prepares. Such data may be inadequate for reasons of flexibility and dependence on IT. Data do not need to be big to be useable or useful.

- **Advanced**—One does not know *a priori* what one is looking for (e.g., auditors are not checking whether thresholds are violated or even the threshold values). For example, auditors discover a new phenomenon that is not yet covered by known rules and thresholds. Auditors may be interested in trends or patterns, or they may be interested in discovering new things. The data are often telling a story and, in this category, auditors want to be able to read the story. An example is fraud—auditors may not know exactly if fraud exists and precisely what it consists of because new forms of fraud may appear. Auditors may even be interested in teaching a computer how to read data and make inferences, although the computer's performance should be supervised.

The first category of data analytics is analogous to learning to drive by learning the rules (e.g., how to start the engine, how to brake, how to turn the wheel, understanding speed limits), and the second category is similar to learning to drive by watching videos categorized as good and bad driving. The techniques in the second category are widely used in many fields and are often combined with methods from the first category or other methods from the second category. The main focus of this article is advanced data analytics.

The Complexity of Advanced Data Analytics

Advanced data analytics deals with complex cases that cannot be labeled with a simple rule such as "if the transaction value is larger than a given amount and no prior history of such a transaction by this user is found, classify it as suspicious." These simple rules typically involve thresholds, and crossing these thresholds is an indicator. Sophisticated fraud schemes often evade detection by the simple rules of the first category of data analytics techniques. Advanced data analytics techniques aim to detect these interesting cases. For example, although short duration calls may not be suspicious by themselves, a combination of such calls with other information can be a sign of abuse in telecommunications or private automatic branch exchange (PABX) systems. In general, although an undetected intrusion or fraudulent activity may not violate a single rule or threshold and, thus, evade the first category of analytics, the activity must, nevertheless, exhibit characteristics that are different from normal activity to be detected by advanced data analytics. Advanced data analytics can detect deviations from normal behavior even if normal behavior has not been defined in terms of rules or thresholds. However, to detect these cases, all relevant information, (i.e., fields) must be identified and included in the data, even though it may not be clear yet how the information must be correlated to identify deviations for a fraud case, for example.

The Case for Domain Expertise

Regardless of the data analytics category or method, domain expertise is vital to data analytics and is the prime reason why enterprises recruit new auditors who have domain expertise in a relevant field such as IT or finance.

> **"Regardless of the data analytics category or method, domain expertise is vital to data analytics."**

Domain expertise is required to identify the relevant fields in the data. Systems and data analytics tools return noise if they are provided with irrelevant data, and the cost of investigating false positives is typically substantial. For example, if an enterprise employs data analytics to identify possible fraud, money laundering or a possible attack, a data

scientist can understand data analytics methods and apply them well, but does not necessarily know the relevant fields and how they should be used. A domain expert understands the information that is relevant, or potentially relevant, to fraud, money laundering, an attack, intrusion, etc., but does not necessarily know the data analytics methods for using this information in complex cases.

Does One Need to Be a Data Scientist to Use Data Analytics Tools?

The short answer is no. Ideally, one should be able to instruct a system or tool to, "run method A on data set B, and provide the results." Numerous tools can help auditors do that. The "Top 10 Data Analysis Tools for Business"[5] provides a list of data analytics tools. Most of these tools provide the methods that are described later in this article. The main differences among these tools are ease of use, interfacing and pricing.

Users of data analytics tools must be able to:

- Understand what method A does
- Prepare data set B so that it is useable by method A
- Interpret the results

To be able to use these tools, some familiarization with data analytics jargon and terminology may be required because the methods and submethods often have technical names, such as sequential minimal optimization (SMO), a support vector machines (SVM) method and K-means (the most widely used clustering algorithm).

Data Preparation

Typically, a data set requires data preparation if it contains:

- More than one field (e.g., monetary value and number of transactions)
- A non-numeric categorical field (e.g., male/female)
- A nominal field, e.g., position in the company (administrator, director, data entry personnel)

Data preparation provides the relative importance of each field to programs or tools, e.g., the importance of a common user making 10 transactions vs. an administrator making 10 transactions. Another example is the number of bank transactions made vs. the total amount of the transactions. Are they equally important? Is the total amount more important? If so, how much more important? The data preparation task is akin to defining a common scale to measure different quantities and requires domain expertise. This task may be further complicated if the data set contains non-numeric data, such as yes/no fields that answer questions such as, "Is there a suspicious destination of money transfer?" The non-numeric data must not only be converted to a number, but also to a number that is scaled to assign its relative importance with respect to other fields.

Assigning relative importance numerically is necessary because many methods use the concept of distance, i.e., a measure of how close two events are to each other in their characteristics, e.g., field values for transactions. Each event consists of a number of fields, and each field value must be numeric (or converted to a number) and scaled to reflect its importance with respect to other fields. This is where domain expertise comes into play. No program is smart enough to determine relative importance, unless it is told how to do so.

Data Analytics Methods

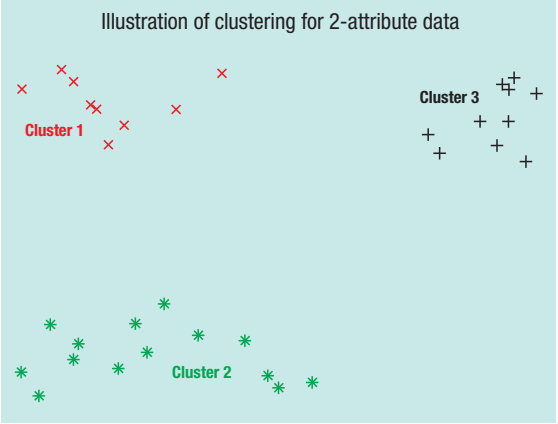
Although more methods are available, there are five data analytics methods that can enhance audits.

Clustering
Clustering organizes data into similar groups, for example:

- A group of managers that shows a similar behavior in outsourcing work that is quite distinct from all other managers
- A group of customers that exhibit a similar behavior, such as high volume transactions of small individual value
- IP packets with special characteristics

Clustering naturally identifies groups with characteristics that are similar within the group and dissimilar from members of other groups. **Figure 1** shows clustering for data with two attributes. Data belong to one of the three clusters shown (X, *, +).

Figure 1—Clustering for Data With Two Attributes



Source: Spiros Alexiou. Reprinted with permission.

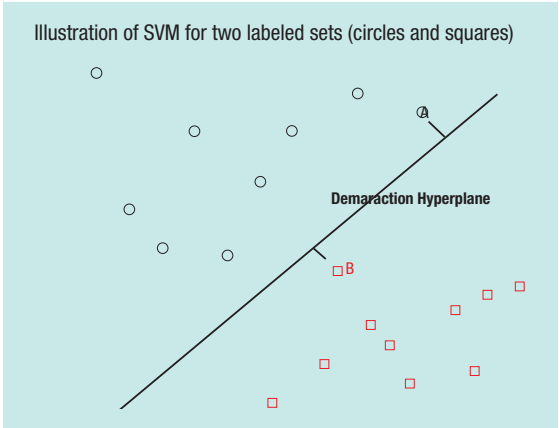
Human analysis and interpretation of the group characteristics, such as center of gravity of the cluster, average values and spread of the data attributes in each cluster, are performed subsequently with the goal of understanding each group. Clustering requires a well-defined distance to access similar behavior. Clustering does not identify strange or suspicious clusters, although it can identify events within a cluster that are distant from most others in the same cluster (outliers). Therefore, humans must interpret and understand the results. Clustering is a very good exploratory tool that makes almost no assumptions and has been used in diverse audits ranging from accounting to network traffic.[6, 7, 8] For example, clustering was applied to network traffic to identify two groups, namely, normal and abnormal network traffic flows.[9] Each member of these groups has characteristics, specifically, packets, bytes and different source-destination pairs, that are closer to the members of the group than to the members of the other group.

Support Vector Machines

The support vector machines (SVM) data analytics method is similar to clustering, because SVM defines, as accurately as possible, the borderline between different clusters, such as fraud/no fraud or solvent/nonsolvent. The feature that separates SVM from clustering is that SVM uses previously labeled data sets to teach the computer to draw the borderline, which, in mathematical terms, is the hyperplane. SVM defines this hyperplane/borderline so that it best divides the two labeled data sets. The division effectively maximizes the area, i.e., the sum of the distances of the closest point of each data set to the borderline, between the two data sets, as illustrated in **figure 2**. Thus a new event, or point, to the left of the established borderline is classified as the rest of the points to the left of the borderline (e.g., fraud/no fraud, positive opinion/negative opinion of a new information system).

Figure 2 shows SVM for two labeled data sets (circles and squares). The demarcation hyperplane best divides the two data sets, i.e. it maximizes the sum of the distances of the closest points A and B from the borderline/hyperplane. SVM is a robust method with a solid mathematical basis and is trainable with relatively few data sets. However, the results are not transparent to users. In addition, the method is quite sensitive to the labeling of borderline cases (points A and B in **figure 2**). An incorrect label in the learning/training data can cause erroneous results. Therefore, the SVM method is best to use when one seeks to determine a borderline and has a high degree of confidence in the labeling of the known cases, especially those that are close to the borderline. Example uses for the SVM method are solvency analysis, intrusion detection and verifying financial statements.[10, 11, 12]

Figure 2—SVM for Two Labeled Data Sets (Circles and Squares)



Source: Spiros Alexiou. Reprinted with permission.

Case-based Reasoning

The case-based reasoning (CBR) method attempts to mimic, on a high level, the reasoning of the human brain. A common problem-solving method that is used by doctors, mechanics and lawyers is to find a similar problem and review how it was handled. CBR uses this same process by saving the solutions to problems in a database. New cases reference the similar cases in the database (**figure 3**).

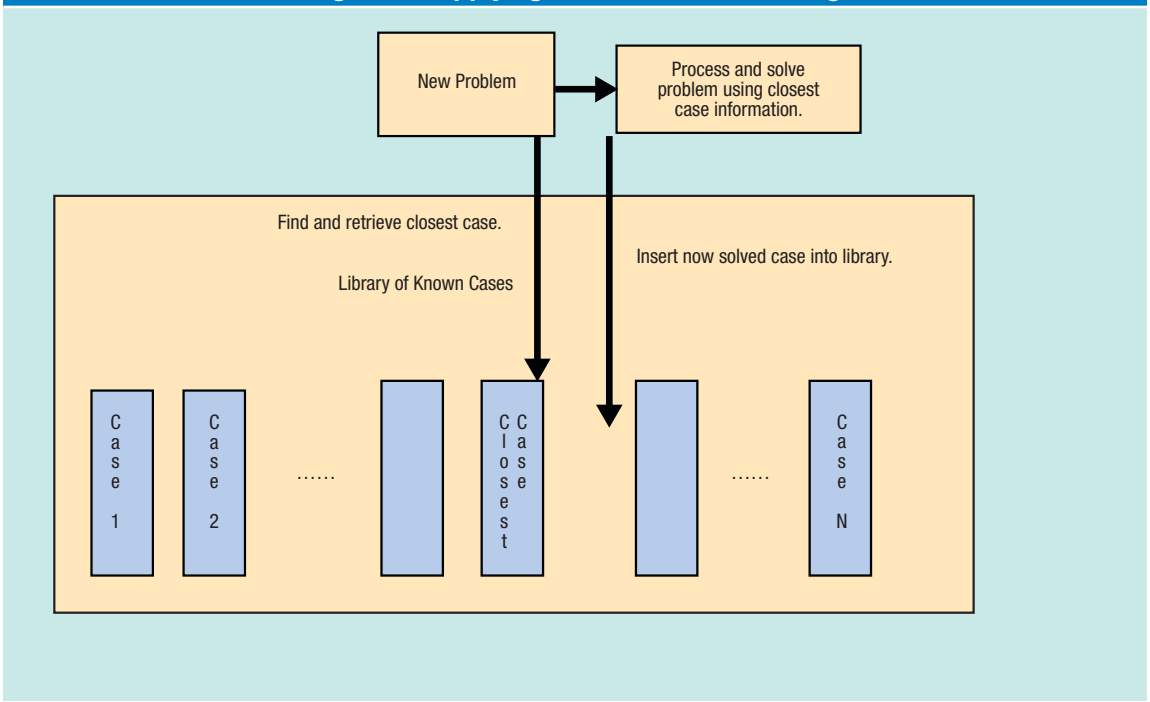
Rules for a new case are constructed based on proximity to the known cases in the database. One weakness of CBR is that a new case that is far from anything known thus far can be misidentified. In practice, the decision or classification is often based not only on the nearest known case, but also on a few nearest neighbors (k-NN), so that the effect of a possible error in a known case is alleviated. The CBR method requires a well-defined distance to access the closeness of two cases. An important advantage of the CBR method is its transparency—the result is based on its similarity to a known case X. Thus, CBR is very useful for classifying a new case based on experience thus far, assuming that previous experience with similar cases exists and their decisions can be explained.

CBR examples in practice range from identifying suspicious transactions to accounting and bank audits.[13, 14, 15, 16, 17] For example, by analyzing the frequency of occurrence of system calls, researchers were able to identify intrusions[18] and, by analyzing access logs, identified anomalous system misuse from inside users.[19]

Artificial Neural Networks

The artificial neural networks (ANN) data analytics method attempts to mimic, on a low-lying neural level, the human brain. Given a set of learning or training data (input), ANN creates a network that produces the known result (output). The ANN method expects that, if the network is given a new set of input data, the network will correctly predict the output. The artificial neural networks method can be viewed as a complex, multidimensional interpolation scheme that, by knowing the output or response to a number of different inputs, predicts the output to different inputs in the same range. The biggest drawback of this method is that it is not transparent to humans and does not provide a simple explanation of why it predicts the output. This drawback is important in many applications, including audits, because it is not acceptable to report

Figure 3—Applying Case-based Reasoning



Source: Spiros Alexiou. Reprinted with permission.

an issue, for example, fraud, which has details that are not understood. Nevertheless, ANN has been used extensively, including for audit purposes.[20] A list of ANN examples in audit, including detection of management fraud using publically available predictors of fraudulent financial statements[21, 22] is available. ANN can be valuable if used as an indicator of something that may be worth investigating.

Random Forest

The random forest data analytics method is a type of decision tree. Decision trees try to create rules from existing evaluated (labeled) cases. For example, one rule that can be deduced is that reporting of financial errors is reduced when an independent audit committee exists and it meets more than twice a year. However, decision trees are prone to overfitting by paying attention to all attributes in the data. For example, a decision tree may use information that is completely irrelevant to the final outcome to formulate a rule. The random forest is an improved variant that uses many different trees that each use a subset of all attributes. The random forest method is designed to alleviate overfitting and the sensitivity of decision trees to noise and uses averaging, which is an effective defense against noise. This method has some similarities to the Delphi method,[23] i.e., an iterative improvement of the opinions of a number of experts that should converge to a single answer. Perhaps a better analogy is a general election or referendum, where most of the voters are assumed to be reasonable on most issues, but each individual voter may have unreasonable views on a few issues. In the same way, the majority of trees in the forest are assumed to be good for most of the data and make different, random errors on some data. If the required answer is a number, then an average of the tree responses is taken as the forest response. If it is a yes/no type of answer, then a majority vote is used. Therefore, a random forest can give humanly understandable rules for classifying current and future cases that are based on already-labeled cases.

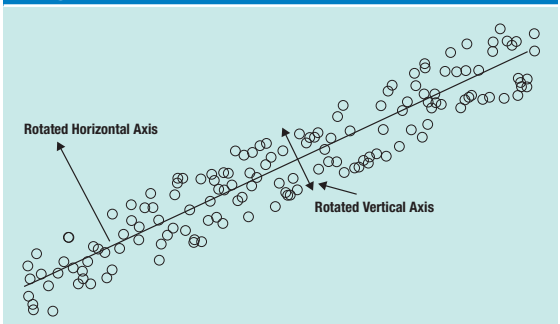
Tools based on random forests typically work off the shelf and give fair results with relatively few data records and many attributes. A recent example of applying random forests to detect financial fraud formed rules based on numerous indicators, such as debt to equity (DEQUTY), current asset ratio (CURAST), and gross profit and EBIT (TPEBIT).[24]

Reduction of Complexity: Principal Axes or Components

Understanding the results in the simplest terms possible is always important, because the results need to be explained to management. Typically, records consist of numerous fields that describe the detailed attributes of an event, e.g., a transaction or login attempt. Principal axes is a mathematical technique to reduce the number of relevant fields. For example, the data analytics methods may detect one type of fraud or another interesting behavior that is characterized by a high number of transactions and low monetary value, and the remaining fields or attributes are largely irrelevant. This example has one principal axis with most of the fraud along this axis. Another axis might describe a different type of fraud and contain a different combination of attributes. This axis is another principal axis.

Figure 4 illustrates the concept of principal component analysis: Data exhibit a much larger variation along the rotated horizontal axis than along the rotated vertical axis. As a result, comparatively little information is lost by ignoring the rotated vertical axis, hence reducing the complexity of the problem to one variable (the rotated horizontal axis) instead of two.

Figure 4—Principal Component Analysis



Source: Spiros Alexiou. Reprinted with permission.

Principal axes analysis aids human understanding, because the large majority of data of interest are along these axes and are easier to understand and visualize. A simple example is intrusions, where the entry and exit time individually might not be relevant, but their difference might be important. Therefore, a different set of axes might be much more informative if it reveals, for example, that intrusions have long durations.

Best of Both Worlds

Methods from both data analytics categories are often combined. Rule-based methods from the first category (one knows what one is looking for) are typically fast, simple and often conclusive. Second category (one does not know exactly what one is looking for) methods are typically more computationally intensive, more complex in data preparation and interpretation, and often indicative. Hence, auditors often apply rule-based methods first and then use second-category methods for cases that are harder to classify.

A significant number of analytics tools are available and many of them are free. These tools can be an important addition to the arsenal of audit tools.

It has been said that, "ANNs and CBR systems have proven they offer better audit effectiveness, better audit quality and reduce audit business risk at a low cost for public accounting firms. It's time these tools are used by auditors."[25] Although every audit is different and has its own requirements, it is likely that many audits could benefit from applying simple and advanced data analytics.

Applying both categories can improve abnormality detection at a low cost, because many of the tools are free and open source. For example, researchers combined their CBR classifier with signature verification to analyze the frequency of occurrence of system calls and identify intrusions.[26] Conventional tools can be used to effectively whitelist cases, therefore, speeding up the procedures. In addition, results from advanced methods can be integrated in rule- and threshold-based methods. For example, traffic flows with certain characteristics corresponding to the abnormal flow cluster will be labeled suspect.

There are data analytics techniques and tools that can significantly aid auditors in discovering knowledge hidden in data, confirming hypotheses and making the most of the available data. These resources are best combined with the auditor's (and possibly other parties') domain expertise and with more conventional tools. The tools are available and many of them free and easy to use once auditors know what they want to do with the data.

"These resources are best combined with the auditor's (and possibly other parties') domain expertise and with more conventional tools."

Endnotes

1 EYGM Limited, "Harnessing the Power of Data: How Internal Audit Can Embed Data Analytics and Drive More Value," EYG no. AU2688, October 2014, *www.ey.com/Publication/vwLUAssets/EY-internal-audit-harnessing-the-power-of-analytics/$FILE/EY-internal-audit-harnessing-the-power-of-analytics.pdf*

2 Izza, M.; "Data Analytics and the Future of the Audit Profession," ICAEW, 22 April 2016, *www.ion.icaew.com/MoorgatePlace/post/Data-analytics-and-the-future-of-the-audit-profession*

3 Rouse, M.; "Data Analytics (DA)," *TechTarget*, January 2008, *http://searchdatamanagement.techtarget.com/definition/data-analytics*

4 *Ibid*.
5 Jones, A.; "Top 10 Data Analysis Tools for Business," KDnuggets, June 2014, *www.kdnuggets.com/2014/06/top-10-data-analysis-tools-business.html*
6 Thiprungsri, S.; M. A. Vasarhelyi; "Cluster Analysis for Anomaly Detection in Accounting Data: An Audit Approach," *The International Journal of Digital Accounting Research*, vol. 11, 2011, p. 69-84, *www.uhu.es/ijdar/10.4192/1577-8517-v11_4.pdf*
7 Munz, G.; S. Li; G. Carle; "Traffic Anomaly Detection Using K-Means Clustering," 17 January 2016, *https://www.researchgate.net/publication/242158247_Trafc_Anomaly_Detection_Using_K-Means_Clustering*
8 Dhiman, R.; S. Vashisht; K. Sharma; "A Cluster Analysis and Decision Tree Hybrid Approach in Data Mining to Describing Tax Audit," *International Journal of Computers & Technology*, vol. 4, no. 1C, 2013, p. 114-119
9 *Op cit,* Munz
10 Auria, L.; R. A. Moro; "Support Vector Machines (SVM) as a Technique for Solvency Analysis," DIW Berlin, German Institute for Economic Research, August 2008, *www.diw-berlin.de/documents/publikationen/73/88369/dp811.pdf*
11 Abd Manaf, A.; A. Zeki; M. Zamani; S. Chuprat; E. El-Qawasmeh; *Informatics Engineering and Information Science, International Conference*, ICIEIS 2011, Proceedings, Springer, 2011
12 Doumpos, M.; C. Gaganis; F. Pasiouras; "Intelligent Systems in Accounting," *Finance and Management*, vol. 13, 2005, p. 197-215
13 Curet, O.; M. Jackson; "Issues for Auditors Designing Case-based Reasoning Systems," *The International Journal of Digital Accounting Research*, vol. 1, iss. 2, p. 111-123, *www.uhu.es/ijdar/10.4192/1577-8517-v1_6.pdf*
14 Liao, Y.; V. R. Vemuri; "Use of k-Nearest Neighbor Classifier for Intrusion Detection," *Computers and Security*, vol. 21, 2002, p. 439-448
15 Denna, E. L.; J. V. Hansen; R. D. Meservy; L. E. Wood; "Case-based Reasoning and Risk Assessment in Audit Judgment," *Intelligent Systems in Accounting, Finance and Management*, vol. 1, iss. 3, September 1992, p. 163-171
16 Ho Lee, G.; "Rule-based and Case-based Reasoning Approach for Internal Audit of Bank," *Knowledge-Based Systems*, vol. 21, iss. 2, March 2008, p. 140-147, *http://dl.acm.org/citation.cfm?id=1344916*
17 Singh, A.; S. Patel; "Applying Modified K-Nearest Neighbor to Detect Insider Threat in Collaborative Information Systems," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, iss. 6, June 2014, p. 14146-14151
18 *Op cit,* Liao
19 *Op cit,* Singh
20 Chao, H.; P. Foote; "Artificial Neural Networks and Case-based Reasoning Systems for Auditing," *Accounting Today*, 2 July 2012, *www.accountingtoday.com/news/artificial-neural-networks-case-based-reasoning-auditing-63178-1.html*
21 Koskivaara, E.; *Artificial Neural Networks in Auditing: State of the Art*, Turku Centre for Computer Science, February 2003, *http://citeseerx.ist.psu.edu/viewdoc/wnload?doi=10.1.1.67.459&rep=rep1&type=pdf*
22 Fanning, K. M.; K. O. Cogger; "Neural Network Detection of Management Fraud Using Published Financial Data," *Intelligent Systems in Accounting, Finance and Management*, vol. 7, 1998, p. 21-41
23 Rand Corporation, Delphi Method, Rand.org, *www.rand.org/topics/delphi-method.html*
24 Liu, C.; Y. Chan; A. Kazmi; S. Hasnain; H. Fu; "Financial Fraud Detection Model Based on Random Forest," *International Journal of Economics and Finance*, vol. 7, iss. 7, 25 June 2015, p. 178-188, *https://mpra.ub.uni-muenchen.de/65404/*
25 *Op cit,* Chao
26 *Op cit,* Liao

MEMBER GET A MEMBER 2016

Get Members. Get Rewarded.

REACH OUT AND HELP COLLEAGUES AND OTHER PROFESSIONALS BECOME ISACA® MEMBERS. **THEY GET THE BENEFITS OF ISACA MEMBERSHIP. YOU GET REWARDED.**

Recruit 2 – 3 new members *and receive an attachable tracking device. Easily locate your valuable items, includes multiple customization options: a US $25 value.*

Recruit 4 – 5 new members *and receive an indoor/outdoor home assistant that flies, 2.4 Ghz camera included. Flips upside down with 4.5 ch. 3D control and LED lights: a US $145 value.*

Recruit 6 – 7 new members *and receive an any-surface projector. Turn any surface into your very own display and entertainment center: a US $279 value.*

Recruit 8 – 9 new members *and receive hi-tech, smart luggage that you can control from your phone: a US $375 value.*

Recruit 10 or more new members *and receive a high-quality gaming system with WiFi capabilities and built-in Blu-ray player. Also includes a controller and 2 games: a US $550 value.*

THE MORE MEMBERS YOU RECRUIT, THE MORE VALUABLE THE REWARD.

When ISACA grows, members benefit. More recruits mean more connections, more opportunities to network—and now, more rewards you can use for work or fun!

Get recruiting today. It's easy. Learn more at *www.isaca.org/GetMembers*

INFLUENCE MORE

ISACA®

Trust in, and value from, information systems

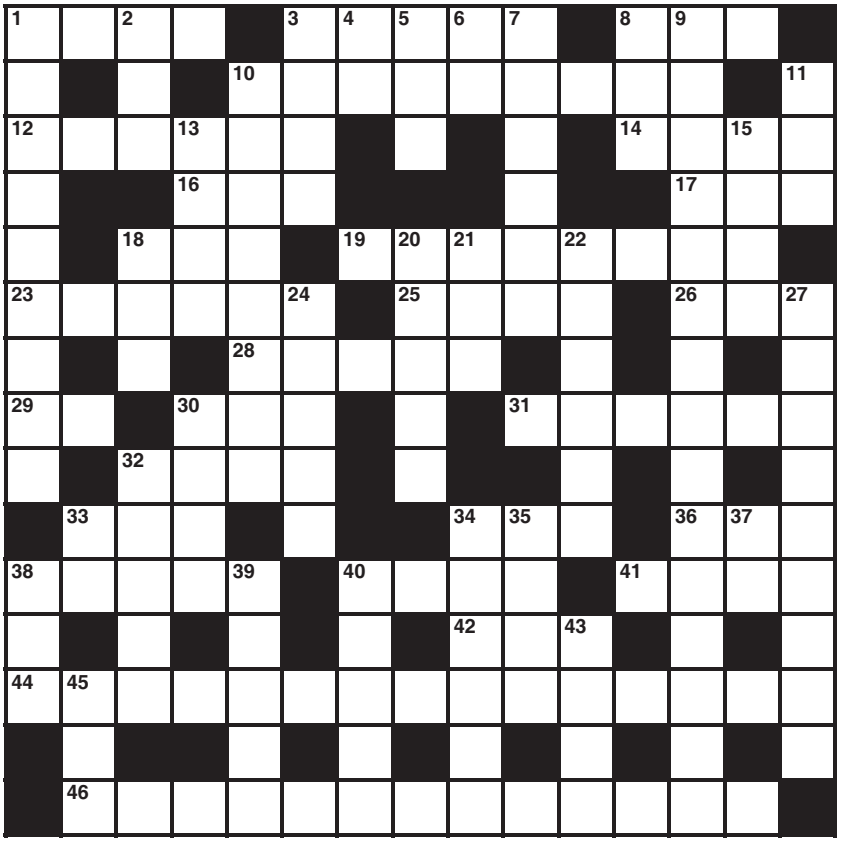
* Rules and restrictions apply and can be found at *www.isaca.org/rules*. Please be sure to read and understand these rules. If your friends or colleagues do not reference your ISACA member ID at the time they become ISACA members, you will not receive credit for recruiting them. Please remember to have them enter your ISACA member ID on the application form at the time they sign up.

crossword puzzle

by Myles Mellor
www.themecrosswords.com

ACROSS

1 Slang term for something undeniably important and paralyzingly dull
3 Standards
8 Measure of printing resolution, for short
10 Incentive
12 Author of the 2001 book, “Code,” and founder of Creative Commons
14 Important qualification for information security professionals
16 That, in Spanish
17 Abbr. on a book’s spine
18 Criticize harshly
19 Hard-to-decide predicaments
23 Writer of “Runaround,” where he introduced the Three Laws of Robotics, dealing with ethical choices for automatons
25 Programmer’s stock-in-trade
26 See 7 down
28 Ethical
29 Novelist, __ Carre
30 Understand, in a way
31 Fight back against
32 Faultless
33 Skill
34 “The God of Small Things” novelist Arundhati
36 ____ and don’ts
38 Important qualification to be able to relate security issues to risk
40 Apogee
41 Team on a national level that responds to cyber security incidents
42 Add up
44 Never do today what you can do tomorrow
46 They should be included with any text in a manual



DOWN

1 Easily influenced
2 Technology critical to Uber
3 Canceled, as a mission, 2 words
4 Work earning extra pay, abbr.
5 Boundary
6 Unit of potential
7 Idea or custom held to be above criticism, goes with 26 across
8 Medical school graduate
9 Term originated by Ann Cavoukian relating to taking into account privacy during the engineering process, 3 words
10 Inappropriate name
11 Family of syntax elements similar to a programming language, abbr.
13 Rich layer
15 “Could be better”
18 Slice of the ___
20 Domain naming system that the US government has controlled for many years and is giving up control in Oct 2016
21 Internet laughter letters
22 Part of RAM
24 Picks a candidate
27 Resist
30 Courage
32 Excellent, slangily
33 Symbol for atomic number 18
34 Itis used in some security scans
35 Of England’s oldest university
37 Alternatively
38 Maximum level
39 Greek island where scenes from “For Your Eyes Only” were filmed
40 Balance-sheet “plus”
43 It is hailed on the street
45 Investors’ expectations

Answers on page 58

quiz #169

Based on Volume 4, 2016—Mobiil Apps
Value—1 Hour of CISA/CISM Continuing Professional Education (CPE) Credit

TRUE OR FALSE

KHAN ARTICLE

1. Sixty-one percent of the US adult population currently owns a cell phone, and of that 61 percent, 31 percent are smartphones.
2. The basic risk segments can be divided into four main mobile app security categories, namely: mobile devices, mobile networks, mobile app web servers and mobile app databases.
3. By integrating mobile devices into the workplace, employees can maximize the service they provide to customers.
4. To prevent malicious extraction from mobile devices, it is highly recommended that the Data Encryption Standard (DES) is used.

SOOD ARTICLE

5. Using data science, it is possible to identify and extract critical information using techniques such as data mining, machine learning, statistics and natural language processing.
6. Traditional security solutions work perfectly with cloud applications; the protection they afford to on-premises systems translates seamlessly to the cloud.
7. A question to ask ourselves is whether data science can be used as a mechanism, among other things, to prevent and remediate data exposures.
8. Cloud applications are now being used for malicious activities including hosting and delivering malware and establishing communication channels for data exfiltration.
9. Correlation involves mapping large sets of data under specific security analytics buckets to understand the complete posture of an attack.
10. Additional security components are executed to analyze the generated anomaly for potential threats. An example of this is deep content inspection (DCI).

WLOSINSKI ARTICLE

11. Examples of malware capabilities include listening to actual phone calls as they happen.
12. One method of social engineering is “Dishing” where an attacker masquerades as a trustworthy entity.
13. Encryption is overkill and not needed as wireless networks simply cannot pass sensitive information to individuals and/or organizations.
14. The most common risk factors that apply to using mobile devices include computer viruses, worms or other personal computing device-specific malware, and theft of sensitive data.

ZONGO ARTICLE

15. The Australian Prudential and Regulatory Authority (APRA) raised a concern that cloud reporting by regulated entities mostly focused on the benefits, while failing to provide adequate visibility of associated risk.
16. Effective cloud risk management requires the board of directors to request pertinent information including cloud value proposition, i.e., data security, privacy laws, data location, business resilience, regulatory compliance.
17. Although cloud providers continue to invest heavily in security capabilities, concerns about data security and regulatory compliance remain key barriers to cloud adoption.

CPE quiz

Prepared by
Kamal Khan
CISA, CISSP, CITP, MBCS

Take the quiz online

CPE quiz #169

THE ANSWER FORM

Based on Volume 4, 2016

TRUE OR FALSE

KHAN ARTICLE

1. _____
2. _____
3. _____
4. _____

WLOSINSKI ARTICLE

11. _____
12. _____
13. _____
14. _____

SOOD ARTICLE

5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

ZONGO ARTICLE

15. _____
16. _____
17. _____

Name _____

PLEASE PRINT OR TYPE

Address _____

CISA, CGEIT, CISM or CRISC # _____

Answers: Crossword by Myles Mellor
See page 56 for the puzzle.

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, CGEIT, CISM or CRISC CPE credit.

standards guidelines tools and techniques

ISACA Member and Certification Holder Compliance

The specialized 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 mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

General
1001 Audit Charter
1002 Organizational 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

The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorization as the standards (also divided into three categories):

- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

Please note that the guidelines are effective 1 September 2014.

General
2001 Audit Charter
2002 Organizational 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

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 programs, 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*.

Prior to issuing any new standard or guideline, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director, Thought Leadership and Research 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*.

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 these products will assure a successful outcome. The guidance 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 judgment to the specific control circumstances presented by the particular systems or IS environment.

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

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors, employers or the editors of the *Journal. ISACA Journal* does not attest to the originality of authors' content.

ISSN 1944-1967

Subscription Rates:

US:
one year (6 issues) $75.00

All international orders:
one year (6 issues) $90.00.

Remittance must be made in US funds.

advertisers/ web sites

leaders and supporters

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

NEW!

CISA, CRISC, CISM and CGEIT Review Manuals Are Now Available as eBooks!

ISACA® Review Manuals in secure eBook format are compatible with any EPUB 3 reader such as Adobe Digital Editions or Bluefire Reader. These manuals will conveniently travel with you on your laptop, tablet or phone.

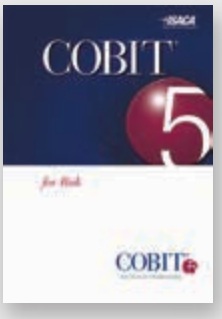
- Searchable content for greater ease-of-use
- Time-saving internal and external hyperlinks
- Interactive features within the table of contents
- Available for immediate download after purchase—with no waiting and no shipping cost anywhere in the world!

CISA® CRISC™ CISM® CGEIT®

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

FEATURED BOOKS

COBIT 5 for Risk by ISACA



by ISACA

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

WEB DOWNLOAD
Product Code: WCB5RK
Member / Nonmember:
$35.00 / $75.00

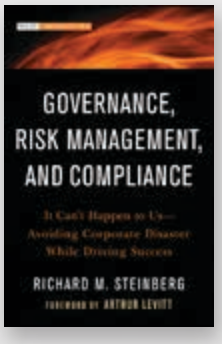
Effectively managing IT risk helps drive better business performance by linking information and technology risk to the achievement of strategic enterprise objectives.

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.

COBIT 5 for Risk provides:

- Stakeholders with a better understanding of the current state and risk impact throughout the enterprise
- Guidance on how to manage the risk to levels, including an extensive set of measures
- Guidance on how to set up the appropriate risk culture for the enterprise
- Quantitative risk assessments that enable stakeholders to consider the cost of mitigation and the required resources against the loss exposure
- Opportunities to integrate IT risk management with enterprise risk
- Improved communication and understanding amongst all internal and external stakeholders

Governance, Risk Management, and Compliance: It Can't Happen to us—Avoiding Corporate Disaster While Driving Success

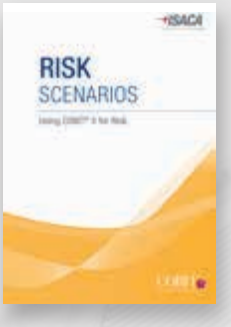


by Richard M. Steinberg

PRINT
English Product Code:
123WCRM
Member / Nonmember:
$33.00 / $43.00

Governance, Risk Management, and Compliance shows senior executives and board members how to ensure that their companies incorporate the necessary processes, organization, and technology to accomplish strategic goals. Examining how and why some major companies failed while others continue to grow and prosper, author and internationally recognized expert Richard Steinberg reveals how to cultivate a culture, leadership process and infrastructure toward achieving business objectives and related growth, profit, and return goals.

Risk Scenarios Using COBIT® 5 for Risk



by ISACA

PRINT
Product Code: CB5RS
Member / Nonmember:
$35.00 / $60.00

WEB DOWNLOAD
Product Code: WCB5RS
Member / Nonmember:
FREE / $60.00

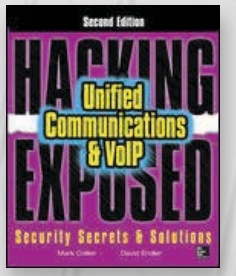
Risk scenarios are recognized as powerful tools that help risk professionals to ask the right questions and prepare for the unexpected. Scenario analysis has become an important component of enterprise risk management. *Risk Scenarios Using COBIT 5* for Risk gives guidance on the development of IT-related risk scenarios, as well as providing guidance on how to use *COBIT 5 for Risk* to solve for current business issues. The publication provides a high level overview of risk concepts, along with over 50 complete risk scenarios covering all 20 categories described in *COBIT 5 for Risk*. Special guidance is given on how the COBIT 5 enablers can help in risk management activities. The accompanying toolkit contains interactive risk scenario templates for each of the 20 categories.

2 EASY WAYS TO ORDER:

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

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

Hacking Exposed Unified Communications & VoIP Security Secrets & Solutions, 2nd Edition



by Mark Collier and David Endler

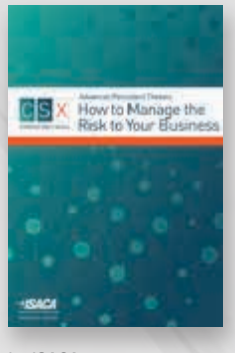
PRINT
Product Code: 36MHHE
Member / Nonmember:
$50.00 / $60.00

"*Hacking Exposed: Unified Communications & VoIP Security Secrets & Solutions,* includes more sophisticated attack vectors focused on UC and NGN. The authors describe in depth many new tools and techniques such as TDoS and UC interception. Using these techniques, you will learn how you can identify the security problems of VoIP/UC. This book is a masterpiece."

– Fatih Ozavci, Senior Security Consultant at Sense of Security, Author of viproy

Establish a holistic security stance by learning to view your unified communications infrastructure through the eyes of the nefarious cyber-criminal. *Hacking Exposed Unified Communications & VoIP, Second Edition* offers thoroughly expanded coverage of today's rampant threats alongside ready-to-deploy countermeasures. Find out how to block TDoS, toll fraud, voice SPAM, voice social engineering and phishing, eavesdropping, and man-in-the-middle exploits. This comprehensive guide features all-new chapters, case studies, and examples.

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



by ISACA

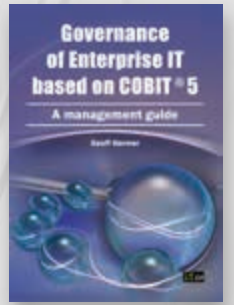
PRINT
Product Code: APT
Member / Nonmember:
$35.00 / $60.00

WEB DOWNLOAD
Product Code: WAPT
Member:
FREE

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.

This book is designed primarily for security managers, IT managers, IT auditors and students studying for computer science or information security qualifications. It is written in clear, nontechnical language so it will also be of value to business managers and government officials responsible for valuable intellectual assets or critical services that might be the target of an APT attack.

Governance of Enterprise IT based on COBIT 5



by Geoff Harmer

PRINT
Product Code: 22ITG
Member / Nonmember:
$35.00 / $45.00

UNDERSTAND THE PRINCIPLES AND PRACTICE OF COBIT 5 IMPLEMENTATION

Practical guidance on COBIT 5
Written for IT service managers, consultants and other practitioners in IT governance, risk management and compliance, this practical book discusses all the key concepts of COBIT®5, and explains how to direct the governance of enterprise IT (GEIT) using the COBIT®5 framework. Drawing on more than 30 years of experience in the IT sector, the author explains the main frameworks and standards supporting GEIT, discusses the ideas of enterprise and governance, and shows the path from corporate governance to the governance of enterprise IT.

The author covers the key elements of COBIT®5 implementation including:

- the 5 principles, the 7 enablers, the 37 processes and the goals cascade;
- the implementation of GEIT using COBIT®5 and an implementation lifecycle;
- the COBIT®5 Process Assessment Model (PAM) based on international standard ISO/IEC 15504.

Covers the COBIT®5 Foundation syllabus
For those studying for the COBIT®5 qualifications, Governance of Enterprise IT based on COBIT®5 also covers all the material needed for the COBIT®5 Foundation course, making it invaluable to anyone planning to take the exam.

Executive's Guide to IT Governance: Improving Systems

by Robert R. Moeller

PRINT
Product Code: 101WEG
Member / Nonmember:
$48.00 / $58.00

Create strong IT governance processes

In the current business climate where a tremendous amount of importance is being given to governance, risk, and compliance (GRC), the concept of IT governance is becoming an increasingly strong component. *Executive's Guide to IT Governance* explains IT governance, why it is important to general, financial, and IT managers, along with tips for creating a strong governance, risk, and compliance IT systems process.

Executive's Guide to IT Governance gives you the tools you need to improve systems processes through IT service management, COBIT, and ITIL

Big Data: A Revolution That Will Transform How We Live, Work, and Think

by Viktor Mayer-Schonberger and Kenneth Cukier

PRINT
Product Code: 1HMBD
Member / Nonmember:
$16.00 / $26.00

"No other book offers such an accessible and balanced tour of the many benefits and downsides of our continuing infatuation with data."
– Wall Street Journal

A revelatory exploration of emerging trends in "big data"— our newfound ability to gather and interpret vast amounts of information—and the revolutionary effects these society at large.

Social Engineering in IT Security: Tools, Tactics, and Techniques

by Sharon Conheady

PRINT
Product Code: 42MSE
Member / Nonmember:
$28.00 / $38.00

Cutting-edge social engineering testing techniques "Provides all of the core areas and nearly everything [you] need to know about the fundamentals of the topic."
– Slashdot

Conduct ethical social engineering tests to identify an organization's susceptibility to attack. Written by a global expert on the topic, *Social Engineering in IT Security* discusses the roots and rise of social engineering and presents a proven methodology for planning a test, performing reconnaissance, developing scenarios, implementing the test, and accurately reporting the results. Specific measures you can take to defend against weaknesses a social engineer may exploit are discussed in detail. This practical guide also addresses the impact of new and emerging technologies on future trends in social engineering.

- Explore the evolution of social engineering, from the classic con artist to the modern social engineer
- Understand the legal and ethical aspects of performing a social engineering test
- Find out why social engineering works from a victim's point of view
- Plan a social engineering test--perform a threat assessment, scope the test, set goals, implement project planning, and define the rules of engagement
- Gather information through research and reconnaissance
- Create a credible social engineering scenario
- Execute both on-site and remote social engineering tests
- Write an effective social engineering report
- Learn about various tools, including software, hardware, and on-site tools
- Defend your organization against social engineering attacks

2 EASY WAYS TO ORDER:

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

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

THE NEXUS
CYBER NEWS CONVERGED

CSX™
CYBERSECURITY NEXUS

CONNECT TO ALL THINGS CYBER WITH *THE NEXUS*

Learn what cyber experts and industry leaders are thinking, doing and saying about global cyber security. Subscribe today for ***The Nexus***—the cyber security-focused monthly newsletter from **ISACA®'s Cybersecurity Nexus™ (CSX).**

Delivered FREE to your email inbox, ***The Nexus*** connects you to:

- Timely updates on emerging threats and promising solutions
- Critical insights from global leaders and cyber security innovators
- Information on the newest CSX tools and resources that can better protect your enterprise and secure your career success

Subscribe now at: **isaca.org/CSXNexus**

THE CHIRON **METHODOLOGY**

Evaluating, developing, validating and sustaining the Information Operation Professional skills in domain and Role Based tradecraft.

Visit us online at training.chirontech.com

Cyber Protection Professional™ (CPP)™

- Identify and evaluate existing information systems
- Evaluates information assets and identify vulnerabilities beyond established baselines
- Create and apply risk assessment and mitigation strategies

Discovery and Counter-Infiltration Professional™ (DCIP)™

- Hunt for adversaries that persist inside the network
- Identify and mitigate threats not detected by traditional monitoring and diagnostic tools
- Develop real-time solutions to resolve incidents and prevent their recurrence

Cyber Threat Emulation Professional™ (CTEP)™

- Emulate the Tools, Techniques and Procedures utilized by adversaries to conduct penetration testing and offensive Information Operations
- Replicate cyber threat activities through penetration tests
- Identify weak points in networks so Active Defenders can mitigate and resolve each vulnerability

Cyber Development Professional™ (CDP)™

- Develop products that verify the integrity of existing services and systems
- Create solutions that facilitate configuration and administration
- Produce tools that facilitate situational awareness on hosts and in networks

CHIRON

PHONE: 410.672.1552 x 109 **FAX:** 410.672.3187 **ADDRESS:** 7021 Columbia Gateway Dr. Suite 250 Columbia, MD 21046