Volume 2, 2016

ISACA Journal

Project Management Methodologies and Associated Risk

Risk Management in Agile Projects

Essential Frameworks and Methodologies to Maximize the Value of IT

Auditing Agile—A Brave New World

ISACA®
Trust in, and value from, information systems

www.isaca.org


CSX™
CYBERSECURITY NEXUS
MOVE AHEAD IN YOUR CAREER.
LET CSX HELP GET YOU THERE.
It is more important than ever to make sure you have the right plan for your future, and that you know what you need to do to take your career to the next level. The new Cyber Security Career Roadmap from CSX is a free, interactive and customized tool that will help you figure out where you are, where you want to be, and what you need to do to get there. Take a free assessment and get a personalized plan you can refer to at any step of your career, and a clear path to success.
Get your free career assessment today at: www.isaca.org/csxjournal-career-roadmap
ISACA®

VOLUME 2, 2016

ISACA® Journal

Columns

Features

Plus

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

Online-exclusive Features

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

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

The Art of Data Visualization, Part 2
Karina Korpela, CISA, CISM, CISSP, PMP

Ataraxia and Premeditation as Elements of Judgment in the Risk Analysis Process
(Disponible también en español)
David Eduardo Acosta R., CISA, CISM, CRISC, BS 25999 LA, CCNA Security, CHFI Trainer, CISSP Instructor, OPST, PCI QSA

Auditing IS/IT Risk Management, Part 1
Ed Gelbstein, Ph.D.

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

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

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

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

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

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

HEALTH CARE SECURITY JOBS HAVE TRIPLED SINCE 2007*

*SOURCE: Labor Insight Jobs (Burning Glass Technologies)

ARE YOUR SKILLS UP TO MEETING THE CYBERSECURITY CHALLENGE?

Up-to-date security skills gained with Capella's Master's in Health Care Security can help you meet the needs of this important and fast-growing field.

Why choose Capella?

- You'll gain practical, hands-on experience working with industry-specific tools, helping you develop the cybersecurity expertise health care employers require.
- Our program aligns with the NSA Health Care Security focus area, which will earn you a digital badge to validate your mastery of health care security.
- Already have your CISSP®? You could be 40% of the way to your degree, saving you time and money.

MEET THE DEMAND. START TODAY. **Capella.edu/ISACA** or **1.866.933.5836**

Weary Willie's Guide to Cyberrisk Management

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.*

Clowning is almost dead as an art form.[1] But when I was a kid, there was one clown in particular known and loved by all: Emmett Kelly.[2] He played a sad-faced, down-and-outer called Weary Willie who tugged at our heartstrings while making us laugh. His most famous act concerned a spotlight. It would follow him wherever he went and he could not shake it. Willie came up with an idea: He would make it smaller and smaller, but then it would suddenly get larger and stickier. Finally he was able to make it small enough that he could hide it under a carpet.


Emmett Kelly

Looking at Emmett Kelly's *shtick* after all these years made me think about cybersecurity. Now, the mind works in curious ways, and mine more so than most. I am probably the only one who sees cybersecurity in a clown's act. What Weary Willie was telling me is that if we cannot eliminate a problem, we should make it small enough that it becomes manageable.

As long as terror, crime and general malice exist, there are going to be bad people doing bad things. We security professionals are not going to be able to solve all threats to information all the time. But it does not stop us from trying, sometimes one step ahead of the bad guys, sometimes two behind. It certainly seems that current events have us a few steps back. Like Willie, we are stuck with a problem that just seems to get bigger and that cannot be shed.

> "If we cannot eliminate a problem, we should make it small enough that it becomes manageable."

We need to make cyberrisk more manageable in our personal lives, in our businesses and in society at large. We security professionals cannot do it all ourselves. Unlike Willie, we need some help. Let us consider some of the members of the team who have to work together to contain the problem.

WEARY WILLIE'S TEAM

If we want to manage risk, we are in the domain of the risk manager, which, while a bit self-referential, is also a bit problematic. Some risk managers are senior executives who treat all potential sources of harm across an enterprise; others are little more than insurance buyers. A true manager of risk should consider all aspects of the threats cyberattacks pose to an organization and devise approaches to transfer and control the hazards, accepting the rest in an informed manner.

There is a vibrant market for cyberinsurance, although it has not reached anything near maturity. According to Statista, an industry statistics organization, 48 percent of worldwide companies carried insurance against data breaches in 2014, down from 54 percent the year before.[3] This may reflect growing wariness with the inclusions and exclusions available in commercial coverage. As for controlling the risk, there is little the risk manager can do except to point to IT to come up with solutions.

The chief information officer (CIO) is an obvious member of Willie's team. Some contend that dealing with the threat of cyberattacks empowers a CIO.[4] But in conversations I have had with CIOs in recent months, there is more of a sense of frustration. As the subject has received increased attention, especially at the board level,[5] cybersecurity is consuming a greater proportion of CIOs' time and attention. There is an attendant concern that other aspects of their jobs are suffering correspondingly. Improved service, new applications and cost reduction are usually the measures of CIOs' performance, and some are worried that these are being overlooked.

In most cases, information security falls under a CIO, but there are some who see this as a conflict of interest. In the battle for budget, cybersecurity seems to some CIOs to overwhelm everything else.[6] For most informed observers, the chief information security officer (CISO) is the leader in the fight against cyberattacks. In fact, one study indicates that the appointment of a CISO is a major factor in limiting the cost of data breaches.[7] Rather than a conflict of interest,

I see a partnership between a CISO and a CIO in managing cyberrisk. However, it is an unequal partnership, in that a CIO usually controls the budget and, therefore, the resources available to a CISO.

MANAGING CYBERRISK

These and other members of Willie's team share the responsibility for making cyberthreats manageable. What would manageable cyberrisk look like?

Trusted images of all software would be regularly updated and stored in such a manner that they would not be externally accessible. There would be a cadre of specialists analyzing system data from across an enterprise monitoring those systems for cyberattacks. These same specialists would drill routinely, validating the trusted images and in recovering software and data as quickly as possible.[8]

Most important, they would manage the business impact of cyberattacks. Widespread encryption would limit the risk of information theft. A cyberrecovery plan[9] would speed the return to normal operations following an attack that manipulated or destroyed systems and information.

Therein lies the axis around which cyberrisk management must spin. If the risk is to be made manageable, organizations must determine how much harm, financial and otherwise, they can tolerate from cybercriminals, governments and terrorists. Zero is not a meaningful answer. As with other threats, total elimination is neither affordable nor attainable. A risk manager can lead the effort to determine a reasonable level, which will require a CIO and a CISO to determine the cost of implementing the necessary solutions. (Of course, this is an iterative process. If the cost is too high, risk management must reconsider its definition of tolerability. There is nothing new or "cyber" about this process.)

Based on the products available in the marketplace to deal with cybersecurity, interest in prevention and detection far outstrips those for recovery. If the threat of cyberattacks is to become more manageable, recoverability will need to be more central to the overall program. That was not a part of Weary Willie's approach and this is where Willie and I part company. He swept it under the rug. I prefer to recognize the magnitude of the problem, accept it and manage it.

AUTHOR'S NOTE

I encourage you and all readers to provide feedback. Please visit my article online at *www.isaca.org/journal*, use the comments section and I will respond to you there. Let us keep the discussion going!

ENDNOTES

[1] Sager, M.; "The Life of a Clown," *Esquire*, June/July 2015, *www.esquire.com/news-politics/a35139/sparky-the-clown-interview-brian-wishnefsky/*

[2] This article will make more sense and be a lot more enjoyable if you take a look at *https://vimeo.com/7098350*.

[3] Statista, Statistics and Facts on Cyber Insurance, *www.statista.com/topics/2445/cyber-insurance/*

[4] Deloitte Australia, "Cyber Security, Empowering the CIO," 2014, *www2.deloitte.com/au/en/pages/risk/articles/cyber-security.html*

[5] ISACA®, *Cybersecurity: What the Board of Directors Needs to Ask*, USA, 2014, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx*. There is a great deal of attention being given to the role of a Board of Directors (BoD) in cybersecurity. I am of the somewhat contrarian point of view that a BoD should accept the reality of the risk, fund the solutions and get out of the specialists' way.

[6] Stanganelli, J.; "Cyber Security And The CIO: Changing The Conversation," *Information Week*, 2 June 2015, *www.informationweek.com/strategic-cio/cyber-security-and-the-cio-changing-the-conversation/a/d-id/1320660*

[7] Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, May 2013, p. 13, *www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF*

[8] I have previously called these specialists CyberCERTs in an article by that name. Ross, S.; "CyberCERT," *ISACA® Journal*, vol. 5, 2014, *www.isaca.org/archives*

[9] The US National Institute of Standards and Technology's (NIST) Cybersecurity Framework calls for such a plan, without defining what it is or what it would contain. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, USA, 2013, p. 34, *www.nist.gov/cyberframework/*. See also my previous article, Ross, S.; "Frameworkers of the World, Unite Part 2," *ISACA® Journal*, vol. 3, 2015, *www.isaca.org/archives*

George Quinlan, CISA

George Quinlan, CISA, has worked in IT infrastructure, operations, governance, security, risk and compliance for 25 years and currently works as a senior IT consultant for Equilibrium IT Solutions in Chicago, Illinois, USA. For the past 10 years, he has taught the CISA review courses for the ISACA Chicago Chapter, and now also teaches the CRISC review course.

Q: *How do you think the role of the IT security professional is changing or has changed? What would be your best piece of advice for IT security professionals as they plan their career path and look at the future of IT security?*

A: Ten to 15 years ago, IT security was an obscure IT role that few companies had or really needed. Now, IT security is becoming mainstream, highly in demand and sought after. The best advice I would give someone is to seek opportunities for training and acquiring new skills and knowledge and to leverage the resources of ISACA® to improve your professional self.

Q: *How do you see the roles of IT security, governance and compliance changing in the long term?*

A: I think these roles are going to become mainstream business functions, no longer optional or "nice to have," but critical to the ongoing business operations in many industries and organizations.

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

A: The biggest risk factors are the speed, complexity and ease with which an organization can become the victim of a cyberincident. Perhaps an even larger risk is the ignorance at the level of the chief executive officer (CEO) and board of directors (BoD). Many CEOs and BoDs still believe that IT has security and risk covered and are happily unaware of the real risk their organizations are facing. I do not think a business can fully protect itself, but must look at security through the lens of a risk-based approach and act accordingly.

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

A: I started in IT as a very technical, hands-on network engineer and worked my way up into IT management. In 2005, I was running IT operations for a credit card processing company and my boss asked me to take on security and Payment Card Industry (PCI) compliance. At that time, I discovered ISACA and the Certified Information Systems Auditor® (CISA®) certification, and it was the best certification I had ever sat for (I had approximately 15 active technical certifications at one time). The body of knowledge I have gained through ISACA and the CISA certification has made me better in every aspect of my job. I am far more knowledgeable, and I can also relate industry best practices and that knowledge to my job and my clients.

Q: *How did you make the transition from IT security to roles in sales and marketing? And what skills have helped you the most in these more recent roles?*

A: I think an effective IT salesperson knows the industry and the business inside and out. The skills I have obtained throughout my career help considerably. What I find interesting is that sales has a lot to do with psychology and human needs and emotions as much as it does technology.

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

A: IT incidents or major outages are very challenging, and this includes security incidents. I cannot really elaborate on specific details, but I will say that the key to effective response in a time of crisis is being prepared. I have been through a number of fairly serious and high pressure incidents, some were major. Being prepared is the key. This should include a response plan, a team that has practiced responding and more.

Unfortunately, all too often I see organizations focus solely on preventative controls (the latest firewalls or other security measures) and really miss the boat on detective and corrective controls. I am a part-time ski patroller with emergency medical services (EMS) training so I see a lot of injured patients on a regular basis and deal with a lot of stressful trauma situations. The two key things I have learned are:

1. Crisis situations are always stressful, confusing and never go by the book
2. Preparation and practice ahead of time is absolutely critical. It is your training and practice that gets you though these kinds of crises. For instance, I would not want someone having to read the cardiopulmonary resuscitation (CPR) manual when I am in cardiac arrest.

WHAT IS THE BIGGEST SECURITY CHALLENGE THAT WILL BE FACED IN 2016? HOW SHOULD IT BE ADDRESSED?
The frequency and impact of security breaches will continue to rise. Security practices need to become more mainstream.

WHAT ARE YOUR GOALS FOR 2016?
1. Obtain my Certified in Risk and Information Systems Control™ (CRISC™) certification
2. Work on my Certified Information Security Manager® (CISM®) certification next

WHAT IS YOUR FAVORITE BLOG?
Krebsonsecurity.com

WHAT IS ON YOUR DESK RIGHT NOW?
Lots of coffee cups!

WHAT IS YOUR BEST PIECE OF ADVICE FOR OTHER IT SECURITY PROFESSIONALS?
Work for a company/organization that has support from the top.

WHAT DO YOU DO WHEN YOU ARE NOT AT WORK?
In the summer, I race sailboats on Lake Michigan. In the winter, I ski and I am a member of the Ski Patrol (we rescue injured skiers). In between, I try to hit the gym.

Is There Such a Thing as a Bad IS Auditor?, Part 2

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.

In Part 1, we discussed the concepts of "good" and "bad" and their many gradations. All of the shades of badness examined (the well-connected, the faker, the lazy, the bureaucrat, the cookbook auditor, the geek and the sociopath), other than the sociopath, are fairly harmless. They are nuisances, definitely, but not individuals who can significantly damage the organization.

In this column, the profiles (other than the timid) represent an increasing level of danger to the organization. There are overlaps among the various profiles.

These negative profiles raise an ethical issue for "good" auditors: the role of organizational policy and whistleblowing. These are big topics, and the intent here is to sensitize the reader to them and raise the question, "Have you thought about this?"

THE ARGUMENTATIVE

The argumentative auditor believes that always being right is the appropriate behavior and will insist that his/her findings and observations could not possibly be wrong and/or revised. Audit meetings get "interesting" when the argumentative auditor is dealing with an argumentative auditee; things can readily escalate into open conflict. This is bad news and usually ends up with senior management/chief audit executive (CAE) to resolve.

THE "MUST FIND SOMETHING"

This is the knowledgeable, experienced, well-mannered and dedicated auditor who feels that his/her role must be justified all the time. Fundamentally different from the argumentative auditor, this auditor can add much value except when he/she engages in the mindless pursuit of perfection.

One such contracted auditor was proudly telling how his six-week audit resulted in 75 recommendations. The auditee was miffed because many were trivial items they already knew about and had even mentioned to the auditor. Senior management got the impression that the chief information officer (CIO) was not up to the job when, in fact, he is a talented and respected figure. The CAE shares the blame for not controlling the contracted auditor and reviewing the draft report.

In the end, the report was put aside and not acted upon, and this auditor is unlikely to get another engagement at this company.

THE SOCIOPATH OR "GOTCHA" AUDITOR

Auditors have power in the form of largely unrestricted access to systems, data, senior management, physical facilities, etc., and their reports give them considerable influence. Such power is valuable when used intelligently and only when appropriate. However, there are those who take an aggressive attitude toward the auditee. In one example, the leader of the audit team shouted at an auditee, "If this is the best you can do, I'm not impressed." Embarrassment (on the part of the auditor) followed, as did a complaint to the appropriate staff representatives and, through them, to the executive level.

THE CONFLICTED

Engaging auditors from a specialist company for a specific task can provide the client organization unique skills and experience. At the same time, the specialist company would probably like to build a long-term relationship with the client organization and may be willing to be flexible just to get a foot in the door.

Is the specialist company's offer of *pro bono* work or a project at a highly discounted daily rate a conflict of interest issue? It is when the end result is a contract spanning many years on the basis that a good working relationship has been built and the specialist company has gained a good insight into the business being audited.

Conflict of interest should be anathema in audit. It can take too many forms to discuss here, but examples include, "I could recommend an excellent consultant to help you with this," or, "Since we are friends, I'll leave this item out of the report." The real problem arises when the auditors believe that their biased advice is unbiased.

THE PROFESSIONAL NICE GUY

This type of auditor has a psychological need to be liked and will accommodate auditees' wishes such as avoiding making them look bad. These individuals fail to recognize the difference between being liked and being respected, the latter being a far greater professional asset. They can play political games—the main difference from the proper political player, described in the next section, is a lack of courage. The professional nice guy does not have the wherewithal to stab someone in the back to ensure their downfall.

ETHICAL DILEMMA

Every person lives by a set of values derived from culture and nurture. Betraying such values can become a source of deep unhappiness, and there may be times when the ethical dilemma of doing what an individual feels is the right thing to do and recognizing the consequences of doing so needs to be faced.

For example, in 2010 there was the internationally reported falling-out[1] between the undersecretary general (UG) for the Office of Internal Oversight Services of the United Nations (UN) and its secretary general (SG) related to the UG's end-of-assignment report.[2] This report represented an unprecedented personal attack in which the UG accused the SG of undermining her efforts to increase accountability in the organization. It took courage to be so openly controversial and it inevitably marked the end of a notable career.

Other senior auditors whose values collided with those of their executives have been punished by being forced out of their organizations.

THE POLITICAL PLAYER

It is difficult not to consider this type of auditor unethical. In bad situations, they will compromise their values to get on with their careers by being helpful to someone with political influence and conspiring to bury controversial findings and observations.

The most skilled of them are able to change jobs frequently, sometimes from a client company to a provider of audit services and back, thus creating potential conflicts of interest and doing whatever it takes to grow their career, influence and remuneration. They are dangerous because they have no compunction about destroying someone if it fits their agenda.

AUDITOR EVALUATION FORMS: DO THEY REALLY WORK?

Feedback is valuable when it is objective. The design of a form can influence responses, i.e., the questions asked and their wording may be such that they limit the possible answers (good, needs improvement) to reflect what the CAE wants to hear. Many forms do not provide a space for free and/or anonymous comments.

When auditees must provide a name, title, etc., they are likely to be careful in their replies. There is no long-term benefit in alienating an internal auditor likely to come back in the future.

At the other extreme, there are web sites where individuals can comment anonymously and with a wide range of expression on hotels, cruises, restaurants, etc. While the open nature of these sites is great to consult when seeking certain services, in the corporate world, this approach could be problematic if it conflicts with organizational culture.

There is no right or wrong answer to this issue. The anonymous nature of the feedback is unfair and can be used to be malicious and/or exact revenge.

CONCLUSION

Because nobody is perfect, it is possible that every auditor has some element of "badness." The issues are whether they are conscious of it and it impacts their work and relations with the auditees.

A previous column, "Auditor: About Yourself and How Others See You,"[3] intended to make readers think about their individual degree of "good" and "bad." A West African proverb is applicable in this context: "Not to know is bad. Not to wish to know is worse."

ENDNOTES

[1] Lynch, C.; "Departing UN Official Calls Ban's Leadership 'Deplorable' in 50-page Memo," *The Washington Post*, 20 July 2010, *www.washingtonpost.com/wp-dyn/content/article/2010/07/19/AR2010071904734.html*

[2] Ahlenius, Inga-Britt; "End of Assignment Report," 14 July 2010, *www.unelections.org/files/Terraviva-EndofAssignmentReport-14Jul10.pdf*

[3] Gelbstein, E.; "Auditor: About Yourself and How Others See You," *ISACA® Journal,* vol. 2, 2015, *www.isaca.org/Journal/archives*

Is Information Technology Responsible for Corporate Crises?

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.*

During the early 1990s, I was visiting with the president of a top-ranked graduate management institute in India. The institute was so popular among students entering college that it required every applicant to sit for an admissions test. The test typically included at least one essay. The institute's president told me that one year he asked the applicants to write an essay on the statement, "There is no right way to do a wrong thing." The essays submitted were too brief and incoherent. It took him much less time to read them, but he was disappointed in the outcome.

I believe this is almost always true of everyone, not just students. We know what the *mantra* is, but we do not know how it enters our general behavior. We understand the concept, but we cannot seem to apply it well enough to make it second nature in us. For example, on the reality TV show *Shark Tank*, one budding innovator showcased her product, a mirror called Skinny Mirror that made people look a few sizes slimmer than they actually are in reality.[1] The idea is to boost the mirror users' self-confidence at the cost of lying to them, perhaps in the hope that they will strive to improve after looking at what they could look like. But lying is lying, regardless of its form. As a result, the "sharks" unanimously rejected the product idea as repulsive. Thus, we might cross the line not because we do not know what or where the line is, but because we just cannot incorporate it into our daily duties well enough.

> "Despite all that technology brings to improve lives and the living environment, it just cannot seem to shield itself from creative deployment for the wrong ends."

MEANS-ENDS RELATIONSHIPS

Means do not justify ends. Something that is wrong is wrong, regardless of the path followed to get there. However, I am particularly puzzled by the fact that technology is often victimized to arrive at the wrong ends. The only difference across a timeline of decades is that, in the past, the impact was limited to the organization and its immediate stakeholders; now, the scalability of technology delivers the outcome in a massively pervasive fashion. Despite all that technology brings to improve lives and the living environment, it just cannot seem to shield itself from creative deployment for the wrong ends.

The underlying human element is the culprit, although at first sight it seems like technology is the defendant. Take, for example, the most recent crisis at Volkswagen (VW). While the details are sketchy at this stage, it appears that senior engineers at VW embedded a code in the company's emission software to manipulate emission results. The code became active when the emission levels were measured; at all other times, the emissions were in violation of the benchmark requirements. As a result, the company, which is the backbone of the German economy, is now in deep trouble. The VW incident has left many people wondering if they can trust any business to do the right thing. And yet, this is not the only case; these days, there are many incursions into moral misbehaviors and to be accomplished, several of them rely on technology.

To a degree, IT permits anonymity (along with the scale), which, in turn, may invoke indulgence to moral temptations. Ashley Madison is a graphic example of this. Empowered by IT, the entire business model rested upon the idea that if individuals wished to indulge, the site would both facilitate it and help them hide it. The eternal temptation is vividly described in the company's logo: "Life is short. Have an affair." The business model here is upside-down. I wonder if a chief executive can set the right tone when his company's business objectives are improper, if not illegal. The virtualization of an extramarital affair does not make it right. However, in providing the service, Ashley Madison's success lies in human nature, which may be inclined toward believing that

having worldly fun depends on indulging in temptations. And the company has succeeded in leveraging the magnetic force of temptations. The proof: Ashley Madison had, at the time of its public discovery, more than 42 million subscribers.

Some new apps focus on alleviating the pains of finding a parking spot in crowded metropolitan areas (see, for example, *Streetline.com*). Parking spaces are a public asset and cannot be held hostage or temporarily "owned" by a computer app that detects an open space. But cities are slow to react and do not have the proper code to regulate such practices. As a result, companies selling parking opportunities establish a foothold in such cities. One might argue that there is nothing wrong with this; no existing regulation was violated. However, in reality, the company selling the privileges appears to virtually own the parking spots, a public asset that presumably should not be tied up or allocated to some preferred individuals. Helping people find a parking spot in a crowded city block is a good thing. However, on a larger scale, it appears that IT is helping encroach upon the spirit of the public ownership and right of use.

Also in the transportation arena, Uber has taken on the fight in various countries to legitimize its business in the face of current, established regulations and licensing requirements. The battle being fought in France is particularly noteworthy, where Uber argues that the country's regulations are confounding its prosperity and must be changed. Uber's lawyer, Hugues Calvet, argues, "The current legal framework doesn't correspond at all to new digital models." The plaintiff's lawyer, Maxime de Guillenchmidt, claims, "Uber's argument is intellectually dishonest."[2] Uber's technology helps improve efficiency and makes life more comfortable, but should it act like a regulator of its own industry? Should it get to the ends first and then legitimize the means? Now that the "Uberization" of businesses and even industries is on the rise, the question of intellectual dishonesty may pervade much of the service economy.

TECHNOLOGY AS A MEANS

While innovative ways to deploy technology as a means to an end (wrong or right) are emerging, the traditional ways to do so still remain strong. For example, the ever-growing practice of social engineering has a long and painful history and yet is still problematic. Senior citizens are cheated out of their life's savings. Even concert tickets purchased online are snatched away by looters electronically. As an enabler, technology ends up carrying the blame, but the reality is that it only feeds the temptation, perhaps with greater vigor. Resisting temptation is not up to technology.

The "conversion" of traditional crime (not involving technology) into cybercrime is striking. An ordinary fraud takes the shape of online fraud (e.g., auction fraud, advance fee fraud, phishing), burglary and malicious damage converts to online abuse (hacking, denial of service, viruses), child sex offenses appear as online child grooming or child pornography web sites, money laundering dresses up as online payment systems (through eCurrency, for example), ordinary theft is now more polished (e.g., identity theft; movie, music and software piracy), and stalking goes underground (cyberstalking, cyberbullying).[3] What used to be is still what it is; only the variety, impact and remoteness enable myriad scenarios, all with the same underlying human frailty hiding behind technology.

There are many ways in which people can do the wrong thing; technology is just one lever they can use. In using technology in the corporate arena, it appears that the actor—executives or the organization—has little remorse. At times, it may be that the actor would not have done the wrong thing if technology was not present as a collaborator in the act. It is strange that IT seems to be an acceptable medium to craft otherwise unacceptable, or at least suspicious, schemes.

> "It is strange that IT seems to be an acceptable medium to craft otherwise unacceptable, or at least suspicious, schemes."

WHY TECHNOLOGY?

Why is IT such a source of comfort to businesses and individuals in doing the wrong thing? In a recent study on the use of digital signatures, it was found that people who sign on a piece of paper are more honest than those who sign using a digital signature; in fact, the dishonesty levels of the digital signers exceed the levels of those who do not sign the document at all.[4] This does not bode well in light of the fact that by 2017, the number of e-signature transactions will exceed 700 million.[5] According to the study on honesty of digital signers, the reason people exhibit higher levels of

dishonesty when they append a digital signature is a weak association between the signature as a commitment and their self-presence in appending the signature, i.e., how much of themselves was present in the signature they provided. The study's findings show that the higher the score on self-presence, the greater the likelihood of honesty with regard to the commitment conveyed by the signature.

In a discussion of a study about dishonesty in golf settings, Dan Ariely notes the idea of psychological remoteness from the actual act causing people to indulge in dishonesty.[6] The study's findings showed that dishonesty in golf is directly influenced by the psychological distance from the action. According to Ariely, cheating becomes much simpler when there are more steps between the individual and the dishonest act. For example, if there is a desire to improve the unfortunate location of the ball, it is easy to rationalize moving the ball with a club and harder to do so when moving the ball by kicking it; the hardest situation is when the ball is picked up by hand and moved to another spot.

> "Cheating becomes much simpler when there are more steps between the individual and the dishonest act."

While these examples do not involve IT, the idea of remoteness from the act appears to be relevant. Technology in the Internet world causes people to be away from actually experiencing the act firsthand and that may lead to an inclination to do the wrong thing.

Another factor that seems to play a rather strong role is loopholes in the law. Laws and regulations may determine the lower levels of thresholds in moral behavior, but they are, nevertheless, important in motivating people to do the right thing. Since laws often do not keep pace with advances in technology and IT-leveraged business models, there could be a gaping hole where the act may be morally wrong, but legally compliant. The weak power of the law in the face of leapfrogging technology causes businesses to act first and worry about the regulations later. The battle in the fantasy football industry is a vivid example of such crises: regulators argue that the act is, indeed, gambling, while the industry's rebuttal hinges on fantasy football involving conscious, decision-making acts by the subscriber (player).[7] It is likely that the same kind of ethical puzzles will arise when drone usage rises to a visible level in the economy and driverless cars become part of daily life.

ENDNOTES

[1] *Shark Tank*, 22 October 2015 episode, *http://abc.go.com/shows/shark-tank/video/PL5539712/VDKA0_qjquiu9x*

[2] Schechner, S.; "Uber Accuses French Government of Trampling on the Sharing Economy," *The Wall Street Journal*, 15 September 2015, *www.wsj.com/articles/uber-accuses-french-government-of-trampling-on-the-sharing-economy-1442318187*

[3] Australian Crime Commission, "Cyber and Technology Enabled Crime," July 2013, *https://www.crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/cyber-and-technology-enabled-crime*

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

[5] Anand, P.; "The Lies E-Signatures Tell," *The Wall Street Journal*, 14 October 2015, *www.wsj.com/articles/the-lies-e-signatures-tell-1444788405*

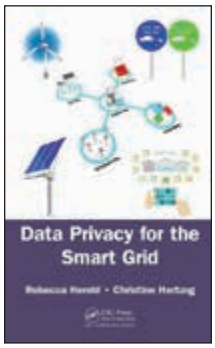
[6] Ariely, D.; *The Honest Truth About Dishonesty: How We Lie to Everyone—Especially Ourselves,* Harper Perennial, USA, 2013

[7] iPR Newswire, "New York Seeks End To Fantasy Gaming," 18 November 2015, *http://iprnewswire.com/new-york-seeks-end-to-fantasy-gaming/*

Data Privacy for the Smart Grid

Reviewed by A. Krista Kivisild, CISA, CA, CPA, who has had a diverse career in audit while working in government, private companies and public organizations. Kivisild has experience in IT audit, governance, compliance/regulatory auditing, value-for-money auditing and operational auditing. She has served as a volunteer instructor training not-for-profit boards on board governance concepts; has worked with the Alberta (Canada) Government Board Development Program; has served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter; and is a member of the ISACA Publications Subcommittee. Her areas of expertise are cybersecurity, governance and incident command system/supervisory control and data acquisition systems.

The smart grid is defined in *Data Privacy for the Smart Grid* as "the modernization of electric, natural gas and water grid infrastructure…the convergence of remote monitoring and control technologies with communications technologies, renewables generation, and analytics capabilities so that previously noncommunicative infrastructures like electricity grids can provide time-sensitive status updates and deliver situation awareness."[1] The majority of people live and work in buildings that use electricity, natural gas and water, and chances are these commodities are delivered via an infrastructure that is slowly becoming smart. The electrical grid is starting to collect information such as where there are power draws, who is pulling the resources, the times that more resources are pulled and perhaps even the types of machines that are pulling these resources. The smart grid facilitates bringing power to people, and the power of the information now captured is part of this transaction.



By Rebecca Herold and Christine Hertzog

While this grid is getting smart, it has been a long time coming. This book explains that there have not been any significant, industrywide technology migration initiatives until the smart grid, and the infrastructure is aging. This slow development shows how quickly the industry as a whole has moved in the past to embrace new capital/technology improvements, and this reveals some of the challenges preventing smart grid technology from being installed.

The smart grid is relevant to all those who are interested in data privacy. The more smart devices attached to the grid, the more information is collected on the consumer and about the consumer's behavior. The book explains that the detailed data collected by the smart grid could allow for forecasts about the number of individuals at a premise, when the location is occupied, sleep schedules and work schedules. The data privacy concerns raised by the authors are numerous and include being able to make assumptions about the health of the residents, which might be of interest to insurance companies, employers and media outlets (for public figures). Criminals could use the data captured from the smart grid to determine if targets are at home and what their routines are, resulting in criminals' ability to effectively target homes.

This book not only outlines the technology and the possible risk, it also walks readers through risk mitigation methods and how to address privacy. What the consumer needs to know and questions to ask potential service providers to ensure that privacy needs are met are also covered in this book. The authors of this book explain effective information security controls in a simple manner so that when controls are presented to consumers by a company, consumers can assess and evaluate which risk factors are covered by these controls and which may remain.

This book can be used to help informed energy consumers start asking and pushing utility suppliers and regulators to enforce upgrades to the grid now and create regulations upfront to better protect privacy. This book empowers the reader to ask better questions and get better service.

EDITOR'S NOTE

Data Privacy for the Smart Grid is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

ENDNOTES

[1] Herold, R.; C. Hertzog; *Data Privacy for the Smart Grid*, CRC Press, USA, 2015

Feature

Risk Management in Agile Projects

Alan Moran, Ph.D., CRISC, CITP, is an Agile thought leader and managing director of the Institute for Agile Management. His career spans both the private and public sectors, and his research interests lie in Agile management (e.g., risk, finance and governance) as well as the Agile enterprise. He is a frequently invited speaker at international conferences and is the author of *Agile Risk Management*, *Managing Agile: Strategy, Organisation, Implementation and People* (Springer Verlag), and *Valuing Agile: The Financial Management of Agile Projects*.

The inherent cadence and iterative nature of Agile practices make them well suited for the management of a wide range of risk commonly encountered in product development and related projects.[1] Indeed, the nature and pace of change in such undertakings present considerable challenges for traditional methods that presume well-defined and stable requirements, together with known risk, that can be captured and modelled using classic techniques. For example, the manner in which understanding of requirements evolves (e.g., facilitated workshops, Agile modelling), the explorative fashion in which designs are implemented (e.g., prototyping, architectural spikes) and the incremental delivery of solutions all help to tackle uncertainty and to promote desired outcomes. This is particularly true of highly innovative solutions where both the customer and the delivery team must collaboratively work together to iteratively define the scope and content of the final solution while tackling both upside and downside risk.

However, throughout Agile literature, there is also a pronounced tendency to focus exclusively on the downside of risk without considering opportunities that can be exploited. This is evident from the view, expressed in many methodologies, that risk should necessarily be considered as an exposure to potentially negative outcomes. Moreover, there is a prevailing view that merely being Agile suffices and that more explicit attention to the identification, assessment, treatment and monitoring of risk is, therefore, not warranted.

This notwithstanding, some methodologies, such as Agile Project Management (AgilePM),[2] which is based on the dynamic systems development method (DSDM), do incorporate an approach to risk management that is more consistent with risk community practices.[3] Furthermore, there is a growing appreciation within the Agile community of the link between risk (under in terms of uncertainty) and learning.[4]

In reality, risk can be subtle and complex, making them difficult for the uninitiated to identify and manage. Irrespective of the chosen Agile methodology, it is incumbent on Agile risk management to address the following concerns:

- Recognition of threats and opportunities within a project in order to balance the desire for reward against the risk incurred in its pursuit. This requires not only a thorough understanding of risk appetite and tolerance within a project, but also an appreciation of the risk inclinations of individual team members and the impact of social and cultural influences on risk management.
- Identification and prioritisation of appropriate risk response strategies (e.g., accept, mitigate, exploit) based on risk exposure and in a manner that is consistent with Agile practices (e.g., inclusion of risk-related tasks in a product backlog or use of a risk-modified Kanban board,[5] which is a planning tool in which activities are moved between lanes representing the phase of development in which they find themselves [e.g., Planned, In Progress, Done] and user story maps as described later in this article).
- Ability to judge whether or not risk is being managed in an effective and efficient manner through the monitoring of risk. This also includes awareness of the residual risk at the iteration level and how these impinge on the overall riskiness of the undertaking.

Thus, Agile risk management underpins project governance in whatever form this takes. In the Agile context, this translates into promoting the visibility of risk, ensuring collective ownership and accountability in relation to risk, and supporting informed decision making in an environment that is often founded on people-centric principles (e.g., collectivism, self-organisation and empowerment).

AN AGILE APPROACH TO RISK MANAGEMENT

Whilst Agile practitioners are often able to state what it is they are working on (e.g., user stories) and what quality criteria apply (e.g., definition of done), it is telling that they are seldom able to articulate the impact their work has on overall

project risk or how they are contributing towards its management.

The integration of established risk management techniques into Agile projects requires care if the value of team heterogeneity, efficient feedback loops and lean decision making are not to be eroded. Accordingly, it becomes necessary to adapt the risk management approach in a manner consistent with the preferences and principles enshrined in the Agile manifesto rather than to simply graft traditional risk practice on top of an Agile process. Indeed, experience indicates that this is possible using artefacts already commonly found in Agile projects (e.g., product backlog or Kanban board), as illustrated in **figure 1**.

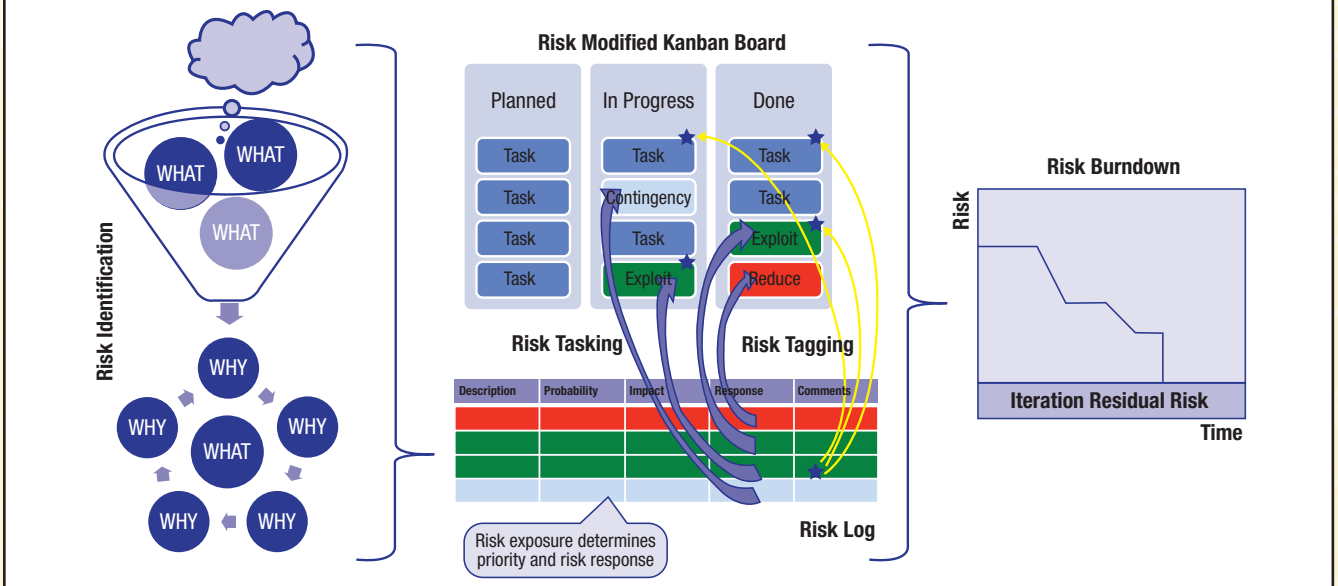
The natural cadence of Agile projects suggests that risk identification and assessment, along with the identification of risk measures, should be incorporated into iteration planning. In product-oriented methodologies (e.g., Scrum, XP), this corresponds to Sprint planning; whereas, in project-focused approaches (e.g., AgilePM), this ought to occur at the start of each Timebox (i.e., a structured and fixed time period that commences with initiation and planning activities that are followed by implementation work and concluded with a review). Thereafter, treatment and monitoring of risk can be embedded in the everyday practices at the iteration level.

One key difference between traditional and Agile project risk management is that ownership of risk is determined by project team members in a manner similar to the allocation of user stories (i.e., Agile requirements) and related tasks. This transforms the traditional role of the risk manager into one that has a more facilitative character that ensures attention to risk management. Such functions can easily be assumed by existing Agile roles (e.g., Scrum Master, DSDM Project Manager).

RISK IDENTIFICATION AND ASSESSMENT

Owing to the manner in which risk and effect are often confused, the identification of risk is harder than one would imagine.[6] Consider, for example, a project to migrate a web application from a physical to a virtual infrastructure in which the concern is raised about whether or not the application will be accessible after the migration. Whilst many may consider the nonavailability of the web application to be a project risk, it is, in fact, the effect of an unsuccessful migration. The real risk resides in the uncertainty that gave rise to the inaccessibility of the web application in the first place (e.g., doubts about whether the configuration of the virtual infrastructure is correct or if the web application is addressable via the domain name system [DNS]). This confusion between risk and effect is particularly pernicious owing to the manner in which it misdirects risk management activities.

Figure 1—Overview of Agile Risk Management Practices



Source: Alan Moran. Reprinted with permission.

Given the subtle issues surrounding the understanding of risk, one of the best techniques for Agile teams is based upon the what-why approach (**figure 1**). This entails a group brainstorming session to discover what might occur in a project followed by an analysis of why each event may occur. Whilst the former identifies effects, it is the latter that is concerned with risk. Indeed, it is not uncommon when discussing why an event might occur to hear explicit statements of uncertainty. For example, in the migration example cited previously, the inaccessibility of the web application (what) may be analysed further to reveal numerous risk (whys), such as the configuration of the virtual server or correctness of DNS entries, thereby enabling the identification of meaningful countermeasures. The advantage of this approach lies in its simplicity, especially for teams that may otherwise be unfamiliar with specialist risk management practices owing to the prevalence of more generalist skills. In addition, the diversity often found in Agile teams can be considered a strength in the search for possible risk, owing to the variety of business and technical perspectives. When conducting such sessions, however, do not focus on purely negative events (e.g., by asking what might go wrong), but rather keep the discussion open in order to admit possible opportunities that the project might exploit.

In keeping with traditional practices, risk should be recorded in a register. However, the visibility of this artefact must be maintained at all times and ownership of risk therein assumed by team members in much the same fashion as user stories or other Agile project tasks. This can be achieved by keeping the register in a place accessible to all team members and encouraging them to provide feedback as often and as early as possible (e.g., updates, omissions, corrections).

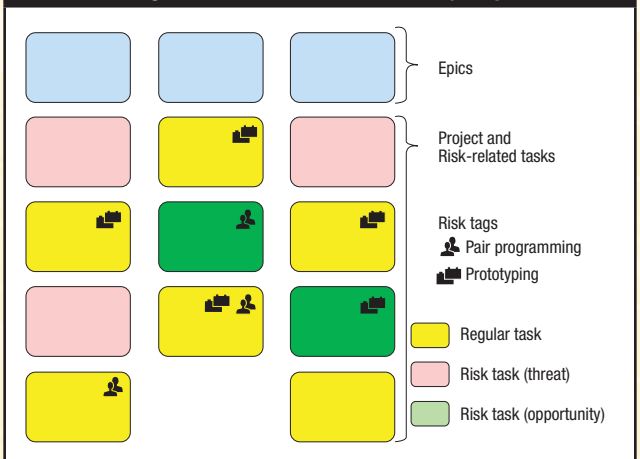
Risk assessment involves both the determination of risk exposure (where t-shirt sizing often suffices, e.g., using small, medium and large to denote magnitude) and the assignment of a risk score (to be used later during risk monitoring) that is based on the risk exposure band in which a risk falls. This score requires consideration of inherent risk and should accommodate not only what is involved in a requirement or task, but also how it is to done (e.g., use of risk-mitigating Agile techniques). Risk exposure is also central to risk prioritisation which, in turn, is an indication of the urgency with which learning must take place in order to tackle project risk.

RISK TREATMENT

Risk assessment provides the input required in order to determine risk responses (e.g., avoid, accept, exploit). Whilst some risk may be tackled by undertaking specific activities (referred to as "risk tasking" in Agile risk management), others require attention to the manner in which activities are undertaken (referred to as "risk tagging" in Agile risk management). For example, the presence of requirements risk when developing a product user interface may encourage the team to ensure that all such user stories are performed using pair programming, an Agile technique wherein two individuals work in tandem.[7] Thus, the team identifies all affected activities and tags them as a reminder of this decision (e.g., perhaps using a double head icon as a visual cue to use pair programming as illustrated in **figure 2**) when they later perform the activities during the iteration.

A risk-modified Kanban board encourages the colour coding of risk-related tasks (e.g., green for opportunity, red for threat) to support the visualisation of risk. Incidentally, such practices can also be extended to other Agile artefacts, including Agile story maps that describe the relationship between epics and their constitute user stories as illustrated in **figure 2**. This enables an excellent visualisation of the distribution of risk and even enables detection of where risk analysis may have been deficient (e.g., a collection of user stories with no apparent upside or downside risk).

Figure 2—Risk Modified User Story Map



Source: Alan Moran. Reprinted with permission.

RISK MONITORING

During risk assessment, the scores assigned to measure inherent risk can be used to construct a risk burndown chart that tracks overall risk management efforts. This device, which resembles the widely used story point burndown chart,

also makes clear to the team that there exists an iteration residual risk (comprised of the cumulative residual risk of user stories along with risk linked to transfer or sharing strategies) that cannot be entirely eliminated. Furthermore, it clearly exhibits the dynamics of risk management in a manner that might not otherwise have been clear (e.g., the fact that secondary risk may cause the chart to rise rather than fall). In a practice referred to as "risk walling," it is recommended to co-locate the risk burndown alongside other risk-related artefacts (e.g., risk register, risk-modified Kanban or user story map) in order to enhance transparency and actively solicit feedback from the team.

CONCLUSION

As Agile becomes ever more widely used, its stance on risk management, governance and related matters remains an impediment in some organisations. This is, however, beginning to change as answers to these challenges are being found and integrated into Agile methodologies and project practices. This provides not only oversight and accountability in relation to risk management, but also ensures that the benefits of Agile in terms of the value it delivers are not eroded.

ENDNOTES

[1] Moran, A.; *Agile Risk Management*, Springer Verlag, Germany, 2014

[2] DSDM Consortium, *The DSDM Agile Project Framework*, 2014, *www.dsdm.org/dig-deeper/news/dsdm-agile-project-framework-%E2%80%93-next-evolution-dsdm*

[3] *Op cit,* Moran

[4] Cockburn, A.; "How 'Learn Early, Learn Often' Takes Us Beyond Risk Reduction," *Humans and Technology*, February 2013, *http://alistair.cockburn.us/Disciplined+Learning*

[5] *Op cit,* Moran

[6] Hillson, D.; *Managing Risk in Projects*, Gower Publishing, UK, 2009

[7] Agile Alliance, *Guide to Agile Practices*, 2015, *http://guide.agilealliance.org/*

Auditing Agile—A Brave New World

Chong Ee, CISA, CGEIT, is a senior finance systems manager with Twilio, a cloud communications company based in San Francisco, California, USA. Ee is focused on optimizing the use and integration of financial cloud applications. Most recently, he implemented NetSuite and other Software as a Service solutions at Trulia to support the company's growth from startup through initial public offering and then as a public company. Before this, Ee spent 13 years in various compliance, audit and consultant capacities for Big Four audit firms, Fortune 500 companies and startups. Ee is a certified NetSuite ERP Consultant and NetSuite Administrator.

"We are running on Agile, so there is nothing to audit" is a refrain auditors hear all too often when attempting to audit clients who use Agile. For a profession rooted in plan-driven methodologies, from validating software development to documenting audit work papers, Agile presents a unique conundrum.[1]

THE CASE AGAINST DOCUMENTATION

Conceived by 17 self-professed "organizational anarchists" in a Utah ski resort in 2001, the first two values of the Agile manifesto listed in **figure 1** appear to clash with common audit constructs, as internal control design and validation are invariably predicated on process and procedural documentation. Furthermore, Scrum, a popular iterative Agile software development methodology, advocates for self-organizing, cross-functional teams, making audit challenging for auditors who are used to prescribed roles and responsibilities that have clearly demarcated segregation of duties (SoD) to mitigate the risk of wrongdoing or fraud.

Figure 1—Manifesto for Agile Software Development

We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- **Individuals and interactions** over processes and tools
- **Working software** over comprehensive documentation
- **Customer collaboration** over contract negotiation
- **Responding to change** over following a plan

That is, while there is value in the items on the right, we value the items on the left more.

Source: *agilemanifesto.org.* Reprinted with permission.

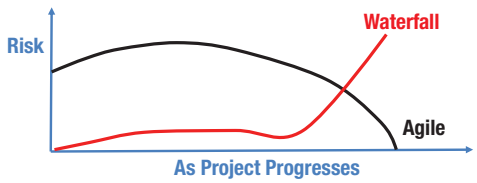
To understand the evolution of Agile and Scrum and identify related implications for audit, it helps to go back to the inception of the waterfall model, first proposed in 1970. Even though the waterfall model defines distinct phases for managing the development of large software systems, it nonetheless acknowledges the need for iteration.[2] Fast forward 30 years and this acknowledgment would have been ideal for proponents of Agile and Scrum, for whom each two-week sprint would culminate in the demonstration of working software. Beginning with a bare bones skeleton and inheriting more features with each successive sprint, the Scrum team seeks to "burn down" the requirements surfaced through the continual grooming of the product backlog.

The waterfall model advocates for significant documentation throughout the development life cycle. Some documentation does help to avoid any miscommunication on what has been agreed upon. Yet, it is the very maintenance of significant documentation during the requirements phase that would, in turn, give rise to more documentation, in the form of change requests seeking authorization for variances to plan. Fundamentally, the Agile manifesto does not so much devalue documentation; rather, it values working software more. Agile focuses on having good enough documentation to initiate and sustain an open dialog among cross-functional team members. The premise behind having good enough, rather than comprehensive, documentation is that, at the start of a project, all that needs to be known is not yet known. A plethora of unanticipated outcomes can arise; for instance, customers can, and often do, change their minds on features, even as the software is being coded (64 percent of features developed never or rarely get used).[3] Therefore, having excessive documentation at the start and using it as a benchmark for downstream activities can seem counterintuitive.

Despite a lesser amount of documentation, Agile can actually create greater transparency on uncertainties that may not be otherwise visible during a project's infancy. According to Jens Østergaard, founder of House of Scrum, the

risk associated with identified uncertainties tapers off with each successive sprint, whereas with waterfall, the initial, comprehensively documented set of specifications may give a false sense of security, only to be undermined when hidden complexities surface downstream when the project enters the testing and go-live phases (**figure 2**).[4] From an audit perspective, an auditor who looks for evidence too soon is likely to be reviewing material that is later overwritten as requirements become further clarified.

Figure 2—Risk Transparency in Waterfall vs. Agile



Source: Chong Ee. Reprinted with permission.

FROM STORYTELLING TO STORY-TESTING

This is not to discourage auditors from intervening early in the development of software. In fact, an unmined opportunity lies in user stories that are developed to characterize specifications in Agile. **Figure 3** depicts a template for user stories.

Figure 3—User Story Template

User Story Template	
As a	<role>
I want to	<action>
So that	<benefit>

Source: Chong Ee. Reprinted with permission.

One of the key ways Agile encourages responding to a change rather than following a plan (see the fourth value listed in **figure 1**) lies in the active update of remaining user requirements; in Agile, this is known as the grooming of the product backlog of user stories for each sprint. The user stories represent the voice of the customer, so the development team is wise to ensure that they are accommodated to the greatest degree possible.

How does the Scrum team know they have delivered on a user story? Behind every user story is a set of acceptance criteria that helps clarify the specific conditions that need to be met for a story to be delivered. Acceptance criteria identification can also break up bigger stories into smaller, more digestible pieces for developers to consider. User stories typically follow the independent, negotiable, valuable to users or customers, estimable, small and testable (INVEST) set of attributes.

Behavior-driven development (BDD) is a means for discovering and, consequently, testing against what the software ought to do. "A story's behaviour is simply its acceptance criteria—if the system fulfills all of the acceptance criteria, it is behaving correctly."[5] Automated testing tools allow the team to describe the acceptance criteria in terms of scenarios; scenarios become automated tests with the addition of step definitions using code. Scenarios take the form illustrated in **figure 4**.

Figure 4—Scenario Template

Given	<some initial context>
When	<an event occurs>
Then	<ensure some outcomes>

Source: Chong Ee. Reprinted with permission.

To illustrate, consider the example of developing a purchase requisition application for expenses over US $1,000 (**figure 5**).

Figure 5—User Story for Purchase Requisition

Purchase Requisition Submission	
As a	buyer
I want to	submit a purchase requisition for approval
So that	I can contract with the vendor for services.

Source: Chong Ee. Reprinted with permission.

How can it be confirmed that the Scrum team has delivered on this user story? A scenario to consider is shown in **figure 6**.

Scenarios force stakeholders to clarify just exactly what they need and can help to mitigate the risk of gold plating, which is the addition of features that do not add value. Thus, auditors can get involved early in the software development process not by looking for comprehensive documentation upfront, but rather by taking part in the user story development.

Figure 6—Positive Scenario in Submitting Purchase Requisition	
Scenario 1: Requisite Information Exists	
Given that	The fields “department,” “general ledger account,” “start and end dates” and “amount” are completed
And	The vendor selected is from the authorized list
And	The purchase approver defaults to the user’s supervisor
And	The purchase approver is an active user
And	The purchase approver has approval authority
And	The amount is greater than US $1,000
When	A user submits a purchase requisition
Then	The purchase requisition is routed to the purchase approver
And	An email is sent to the purchase approver to log into requisition application.
Source: Chong Ee. Reprinted with permission.	

Figure 7—Negative Scenarios in Submitting Purchase Requisitions	
Scenario 2: Missing Information	
Given that	The fields “department,” “general ledger account,” “start and end dates” and “amount” are missing
When	A user submits a purchase requisition
Then	An error message pops up to remind the user of mandatory fields to complete.
Scenario 3: Amount Under US $1,000	
Given that	The amount is under US $1,000
When	A user submits a purchase requisition
Then	An error message pops up to remind the user of the purchase requisition policy.
Scenario 4: No Approval Authority	
Given that	The purchase approver does not have approval authority
When	A user submits a purchase requisition
Then	An error message pops up to contact the application administrator.
Scenario 5: No Independent Approver	
Given that	The purchase approver is the same as the user
When	The user submits a purchase requisition
Then	The user is prevented from submitting the requisition.
Scenario 6: Duplicate Requisitions	
Given that	The amount and vendor selected are the same as an existing requisition submitted on the same date
When	A user submits a purchase requisition
Then	An error message pops up to warn the user of a possible duplicated requisition.
Source: Chong Ee. Reprinted with permission.	

Within each story, there is an opportunity to craft an abuse scenario where the nature of the proposed validation is negative, i.e., covering scenarios that do not follow the plan. **Figure 7** describes the expected application behavior for five abuse scenarios. **Figure 8** maps these scenarios against traditional internal control objectives.

Figure 8—Mapping Scenarios to Control Objectives			
Scenario	**Completeness**	**Accuracy**	**Validity**
2	X		
3			X
4			X
5			X
6			X
Source: Chong Ee. Reprinted with permission.			

It turns out that there are no controls addressing whether or not the proposed spending request is recorded correctly to the right general ledger (GL) account. Therein lies an opportunity for auditors to articulate other roles needed to ensure transaction integrity. By participating in the Scrum team during, rather than after, the sprint, auditors can add a story for finance personnel to provide a second layer of review, as outlined in **figure 9**.

Figure 9—Finance Review of Purchase Requisitions	
Purchase Requisition Finance Review	
As a	Finance user
I want to	Review an approved purchase requisition
So that	I can ensure that it has been recorded to the correct general ledger account.
Scenario 7: Correct Selection of GL Account	
Given that	The general ledger account has been correctly coded
When	The purchase approver approves the purchase requisition
Then	A finance user checks the “finance approved” checkbox.
Scenario 8: Incorrect Selection of GL Account	
Given that	The general ledger account has been incorrectly coded
When	The purchase approver approves a purchase requisition
Then	A finance user edits the general ledger account
And	An email is sent to the requisitioner describing the account update
And	The finance user checks the “finance approved” checkbox.
Source: Chong Ee. Reprinted with permission.	

Had the development approach been waterfall, auditors would have been satisfied obtaining sign offs of the initial requirement to have the enterprise buyers correctly code their proposed purchase to the right general ledger accounts, even though, in reality, this process is not executable. In addition to participating in user story development, auditors need to also adapt the manner in which they perform audits.

A specification should do something.[6] Thus, when auditing Agile, instead of expecting a three-ring binder of written specifications, a more appropriate approach may be for auditors to request the system log of executable specifications. The following questions can help the auditor gain insight on specifications:

- Where are the automated test results?
- What happens when they fail?
- What is the test coverage?
- How often are automated tests updated?

The good news is that Agile and Scrum artifacts are not vastly different from the traditional audit artifacts that auditors rely on to evidence a system of internal controls. User stories mirror user narratives, and acceptance criteria mirror application controls that ensure the accuracy, completeness and validity of the transactions processed. Auditors who consider a more complete picture of varied roles and scenarios (illustrated through user stories and acceptance criteria) make a valuable contribution to the Scrum team.

Auditors can also add value by challenging the prevailing mind-set that tests at the end of a project are the only way to produce the required quality. It is widely accepted that the later a bug is detected, the more costly it is to fix.[7] In the same manner, if acceptance criteria of stories are developed as a part of BDD, developers can employ test-driven development (TDD) to write tests before writing code. Studies on the adoption of TDD in three Agile teams at Microsoft and one at IBM reveal a 40 and 90 percent decrease, respectively, in the prerelease defect density of products.[8] Further, when combined with a continuous integration (CI) server that triggers testing every time new code changes are checked in, testing becomes part of, or a constant accompaniment to, coding, as opposed to a separate downstream test phase. Consequently, the earlier identification of unit and functionality errors reduces the cost to fix them later and frees up time for testers to add value through exploratory and end-to-end transaction testing.

ROLES THAT OVERLAP

The remaining Agile manifesto value addressed in this article emphasizes customer collaboration over contract negotiation (see the third value in **figure 1**). With its emphasis on distinct phases and handoffs, the waterfall model can be likened to a relay race,[9] while Scrum is derived from a restarting play where players huddle with their heads down to attempt to gain possession of the ball. When applied to software development, the Scrum approach focuses on having the distinct phases overlap through collaboration..

What implications does this have for audit? A key precept behind the emergence of design thinking as a means to solving problems is the emphasis on collaboration to attain sustainable product design. By playing a key role in the Scrum team by considering abuse scenarios in user stories, auditors engage actively in the collaboration.

Another useful adjustment auditors can make is to expand their scope of auditees. As mentioned earlier, the product owner, insofar as he/she drives the product backlog of user stories, is a key resource in making sure that compliance and security needs are met. Auditors can make a valuable contribution by ensuring broad representation of stakeholders on the Scrum team. The composition of the Scrum team plays a key role in aligning expectations for the project among all those involved.

However, just because the Scrum team is cross-functional does not mean all development, test/staging and production environments are accessible to anyone on the team. The audit objective behind SoD—restricting access by environment or configuration so that no one single individual has the ability to circumvent or hack the prevailing system of internal controls—is not mutually exclusive from the development objective of maintaining code integrity, which is making sure that valid code changes are not inadvertently overwritten or diluted by competing ones that have not been tested or do not integrate well with existing interfaces.

With the emphasis on customer collaboration over contract negotiation, it can be easy to be misled into thinking that Agile favors process over outcome. Interviews conducted with teams from three organizations, one using waterfall, another using Agile and a third using a hybrid of both, revealed that the waterfall organization saw a greater emphasis on product or outcome with preventive controls, whereas the Agile organization leaned toward process with detective and corrective controls.[10] With Agile's fundamental focus on outcome—working software—one can make a counterargument that in Scrum, control practices such as TDD, CI, and automated unit and acceptance testing are really focused on outcome, whereas the waterfall model, with its focus on formalized signoffs, is really borne out of an emphasis on process. **Figure 10** illustrates the different types of process- and outcome-based controls in Agile and Scrum.

Figure 10—Agile Outcome vs. Process Controls

Outcome Controls	Process Controls
Percent of test coverage	Product backlog
Number of failed builds	Progress in burndown chart
Number of failed unit tests	Findings from sprint retrospectives
Number of failed acceptance tests	Composition of Scrum team

Source: Chong Ee. Reprinted with permission.

As for whether Agile has more detective or corrective controls than waterfall, there are shades of gray when it comes to labeling a control as preventive or detective. Because the project is seen from production, the testing phase from the waterfall model is preventive, i.e., it reduces the likelihood of coding errors from arising in production by uncovering them in a test environment. From the perspective of development, however, testing is detective as it uncovers errors in coding from the development phase. Likewise, TDD in Scrum and Extreme Programming (XP), by forcing developers to fail the test before the code is written, detects the error even as it prevents it from arising ultimately in production. The same argument can extend to automated unit and acceptance testing; while they detect errors in development and staging environments, they really prevent them from arising in production. To characterize Agile controls as more detective than preventive is to miss an opportunity to dive deeper into what truly goes on.

CONTROL READINESS IS A FUNCTION

How control-ready an enterprise is depends not just on the practices adopted (whether that is waterfall or Agile in software development), but also on the environment, which is unique to each enterprise. Whether management employs a more top-down or bottom-up approach in controlling software development can make a difference in whether waterfall, Agile or a combination of both is ultimately embraced. In effect, auditors can audit the Agile team on how well it does Agile.

For far too long, auditors have been relying on validating the operating effectiveness of processes in the hope that a carefully controlled process will yield a positive outcome, e.g., verifying evidence of sign-offs. The problem with process controls is that while they may be necessary for fostering a positive outcome, they are by no means sufficient. Consider the user story of submitting purchase requisitions for approval outlined in **figure 9**.

When auditors sample invoices, they may find that all have been matched with approved requisitions. They are able to find a 100 percent two-way match with no exceptions. It would appear that all purchases made have been approved beforehand. Yet they cannot help but notice from the system audit timestamps that for a particular group of buyers, requisitions are almost always created shortly before invoices are applied—sometimes a matter of mere minutes. It turns out, for this group of buyers, because proposed spend is highly volatile and hard to predict upfront, requisitions are created only upon receipt of invoices, rather than before receipt of service.

These illustrative audit findings cast doubt upon requisition approval as a means to control spend precisely because it is not so much performed before services are rendered as it is after receipt of services—and often as a means of generating evidence for audit. Auditors must be proactive to ensure that audits remain effective safeguards against errors or fraud, not ritualized practices of audit for audit's sake.[11] Agile, with its emphasis on working software, focuses on outcome and, thus, provides auditors the opportunity to adapt their approach accordingly. A widely circulated observation among Agile and Scrum circles is that the Standish Group's study of software projects conducted between 2002 and 2010 revealed that Agile is three times more likely to succeed than waterfall.[12] Yet, auditors point out that the same Standish Group study reported that both Agile and waterfall projects shared a 50/50 chance of being challenged.

As lightweight frameworks, Agile and Scrum are not intended to be comprehensive. They do not address risk management, product strategy and other areas that comprise the slew of activities to enable and sustain product launch, continual enhancement and maintenance. When auditing Agile, it is important for auditors to realize that enterprises employing Scrum or Agile are not running on empty—there are indeed artifacts and ceremonies from a process perspective and metrics to track test coverage and automated test results from an outcome perspective. Perhaps, more important, auditors are best served by seeing that Agile, like its waterfall predecessor, is not a silver bullet to resolving the age-old struggle of bridging compliance and security with software.

ENDNOTES

[1] This article uses several Agile terms that are critical to understanding. A sprint is a set period of time during which specific work has to be completed and made ready for review. A burndown chart is a graphical representation of work left to do vs. time. A product backlog is a prioritized features list containing short descriptions of all functionality desired in the product.

[2] Royce, W.; *Managing the Development of Large Software Systems*, Technical Papers of Western Electronic Show and Convention (WesCon), 25–28 August 1970, Los Angeles, California, USA

[3] Johnson, J.; Standish Group Study reported at XP2002

[4] Ostergaard, J.; "Why Scrum Is So Hard," 20 August 2009, *http://www.slideshare.net/marakana99/jens-stergaard-on-why-scrum-is-so-hard-2416688*

[5] North, D.; "Introducing BDD," *Better Software*, March 2006, *http://dannorth.net/introducing-bdd/*

[6] *Ibid*.

[7] Beohm, B.; V. Basili; "Software Defect Reduction Top 10 List," *Computer*, vol. 34, iss. 1, January 2001, p. 135-137

[8] Nagappan, N.; E. Maximilien; T. Bhat; L. Williams; "Realizing Quality Improvement Through Test Driven Development: Results and Experiences of Four Industrial Teams," *Empirical Software Engineering*, vol. 13, iss. 3, June 2008

[9] Takeuchi, H.; I. Nonaka; "The New Product Development Game," *Harvard Business Review*, 64, no. 1, January-February 1986

[10] Cram, W. A.; M. K. Brohman; "Controlling Information Systems Development: A New Typology for an Evolving Field," *Information Systems Journal*, 23 (2), 2013, p. 137-154

[11] Power, M.; *The Audit Society: Rituals of Verification*, Oxford University Press, UK, 1997

[12] The CHAOS Manifesto, The Standish Group, 2012

Essential Frameworks and Methodologies to Maximize the Value of IT

Laurent Renard, CISA, CISM, CGEIT, CRISC, COBIT Foundation, DevOps, GRCP, ITIL Expert, Lean Six Sigma BB, MoP, MSP, P3O, PMI-ACP, PMI-PBA, PMP, PRINCE2, Resilia, Scrum PSM-PSPO, TOGAF, is a consultant and trainer at Global Knowledge who has previously held management responsibilities in numerous high-tech companies (Vivendi, Ascom and Digitas). In 2007, he published *The Guide to Clubs, Circles and Networks of Influence* and *Internet Strategy: MAO® and (r) Evolution* in 2008. He has taught marketing and strategy at EDHEC Business School (Lille, France) and currently teaches the Cloud Computing Executive Certificate at Ecole Centrale de Paris (France).

IT helps organizations achieve their goals and optimize their profitability by balancing risk at an acceptable level. Information systems professionals, including IT governance, security and audit professionals, wish to help organizations do so. For that, organizations need practical guidance, benchmarks and tools to select, deploy, and effectively and efficiently operate pertinent frameworks and methodologies.

This article presents the most essential frameworks and methodologies aimed at maximizing the value of IT, starting with IT governance (**figure 1**). IT governance leads to the design of IT architecture, which then enables portfolio management, which breaks down into program management and then into project management, and includes business analysis to provide the best products or services to operations. This article concludes with process optimization to continuously improve performance.

IT GOVERNANCE

IT governance is a subset discipline of corporate governance, defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals through maintaining risk at a level coherent with the risk appetite of the stakeholders.

COBIT

Just as corporate governance provides value to shareholders by optimizing a balance between financial return and risk, COBIT® provides a set of recommended best practices for governance and control processes of information systems and technology with the goal of aligning IT with business.[1] Because COBIT is business-oriented, using it to deliver value and govern and manage IT-related business risk is straightforward.

COBIT is positioned at a high level and has been aligned and harmonized with other, more detailed IT standards and good practices such as the Information Technology Infrastructure Library (ITIL); the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard ISO/IEC 27000; Capability Maturity Model Integration (CMMI); The Open Group Architecture Framework (TOGAF); Projects in Controlled Environment, version 2 (PRINCE2) and Project Management Professional (PMP). COBIT acts as an integrator of these different guidance materials, summarizing key objectives under one umbrella framework that links the good practice models with governance and business requirements (**figure 2**).

IT/BUSINESS ARCHITECTURE

IT architecture is the process of development of methodical IT specifications, models and guidelines using a variety of IT notations within a coherent IT architecture framework and following formal and informal IT solution, enterprise and infrastructure architecture processes.

The Open Group Architecture Framework

TOGAF is a framework for enterprise architecture that provides an approach for designing, planning, implementing and governing enterprise IT architecture. TOGAF is a high-level approach to design and is modeled at four levels: business, application, data and technology. TOGAF delivers value through the insurance of coherence and efficient evolution of all different architecture components.

PORTFOLIO MANAGEMENT

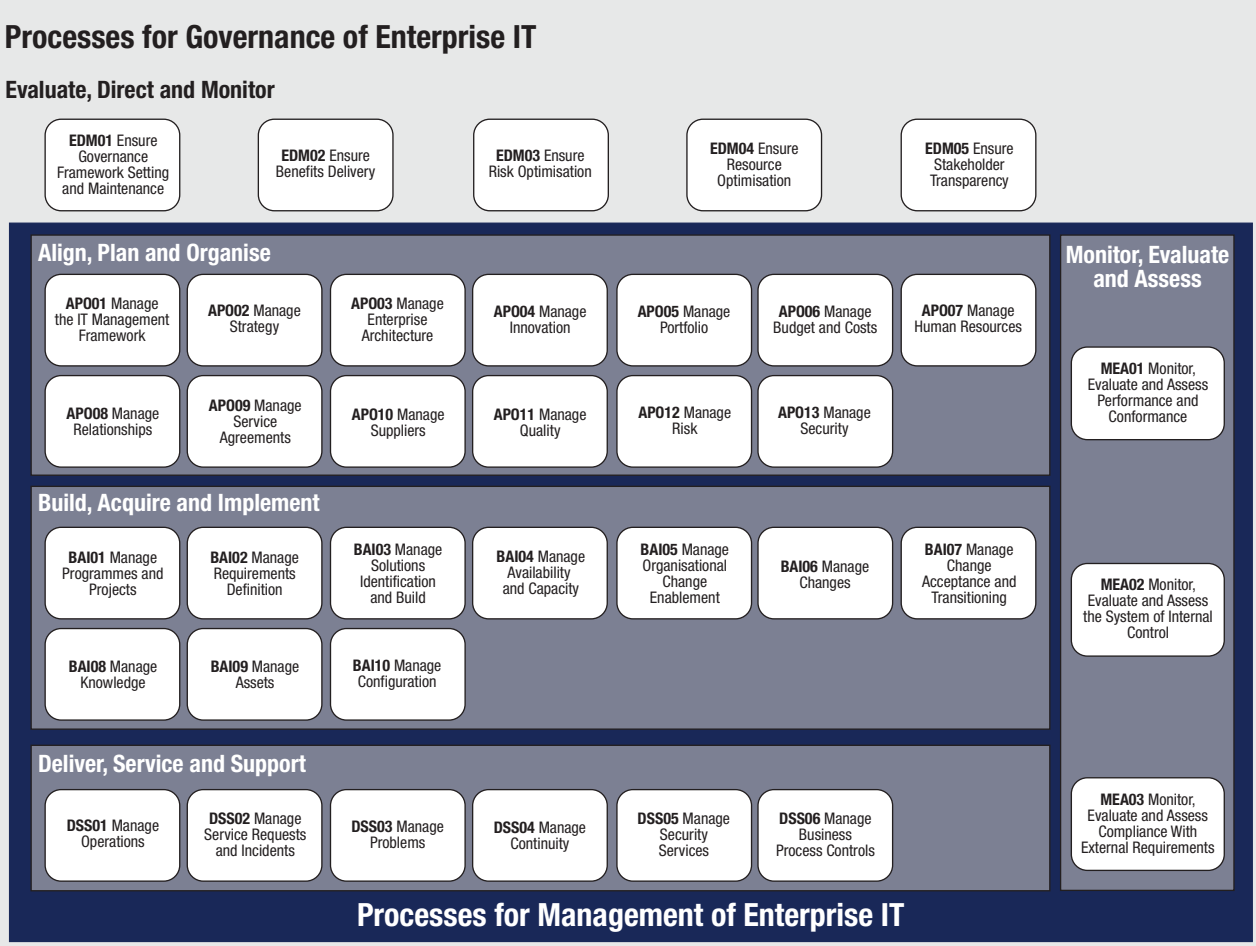
Portfolio management is the centralized management of the processes, methods and technologies to analyze and manage current or proposed programs or projects based on different key characteristics. The objectives of portfolio managers are to determine the optimal resource mix for delivery and to schedule activities to best achieve an organization's operational and financial goals, while honoring constraints imposed by customers; strategic objectives; or external, real-world factors. Portfolio management of projects can be seen as portfolio

Figure 1—Frameworks and Methodologies

Information Technology Life Cycle	Development				Operations
COBIT (IT governance)	Align, Plan and Organize; Build, Acquire and Implement				Deliver, Service and Support
	Monitor, Evaluate and Assess				
TOGAF (IT/enterprise architecture)	Architecture (vision, business, information system, technology), opportunities and solutions, migration planning, implementation governance, architecture change management				
PfMP (Portfolio management)	Programs/projects (identification and categorization, evaluation, selection, prioritization)		Portfolio (reporting and review, monitoring/control, risk management)		
MoP (Portfolio management)	Understand, categorize, prioritize, balance, plan		Management control, benefits management, financial management, risk management, stakeholder engagement, organizational governance, resource management		
PgMP (Program management)	Pre-program preparation	Program initiation	Program setup		Delivery of program benefits, program closure
MSP (Program management)	Identifying a program	Defining a program	Delivering the capability, managing the tranches		Realizing benefits, closing program
PMP (Predictive project management)	Initiating	Planning	Executing, monitoring/ controlling	Closing	
PRINCE2 (Iterative project management)	Starting project	Initiating project	Directing project, controlling a stage, managing stage boundaries, managing product delivery	Closing project	
Scrum (Adaptative project management)	Product vision	Road map	Product backlog, sprint planning, development, daily meeting, sprint review, sprint retrospective		
PMI-PBA (Business analysis)	Needs assessement	Business analysis planning	Requirements elicitation and analysis, traceability and monitoring	Solution evaluation	
CBAP (Business analysis)	Strategy analysis	Business analysis planning and monitoring	Elicitation and collaboration, requirement life cycle Management, requirement analysis and design	Solution evaluation	
ITIL (Classical IT life cycle)	Strategy	Design		Transition	Operations
				Improvement	
DevOps (Agile IT life cycle)	Flow->				<-Feedback
	Continuous experimentation and learning				
Lean Six Sigma (Processes optimization)					Define, measure, analyze, improve, control

Source: Laurent Renard. Reprinted with permission.

Figure 2—COBIT Processes for Governance of Enterprise IT



Source: ISACA®, COBIT® 5, USA, 2012

management of shares, which can be composed of different stocks that can possibly be competitors and/or have different life cycles, in order to balance performance.

Portfolio Management Professional Certification

A Portfolio Management Professional (PfMP) bridges the gap between strategy and implementation; maps the links among projects, programs, organizational project management and strategy; and describes the portfolio management processes along with the necessary communication, performance, risk and change management subsidiary plans. For fully integrated management of portfolios, programs and projects, it is recommended to use PfMP, Program Management Professional (PgMP) and PMP collaboratively because of the total compatibility of these three methodologies, all of which have been written by the Project Management Institute (PMI), the world's largest not-for-profit membership association for the project management profession.

Management of Portfolios

Management of Portfolios (MoP) approaches the management of change projects and programs from a strategic viewpoint. It provides an overview of all change activities, including what is in the portfolio, what it costs, what risk is present, what progress is being made, and what impact there is on business as usual and the organization's strategic objectives.

For integrated management of portfolios, programs and projects, people using the PRINCE2 methodology will find benefit in using MoP and Managing Successful Programs (MSP), which are produced by the same global accreditation body, Axelos.

PROGRAM MANAGEMENT

Program management is the process of managing a group of related projects in a coordinated manner to obtain benefits and control not available from managing them individually. Program management also emphasizes coordinating and prioritizing resources across projects, managing links between the projects, and the overall costs and risk of the program. A program can be differentiated from a project through the example of the iPhone program, which is composed of the iPhone (hardware) project, the iOS project, the iTunes Portal project and the different iApps projects.

Program Management Professional Certification

The Program Management Professional (PgMP) certification focuses on the strategic objectives, benefits and outcomes of projects and provides an integrated approach to resolve inconsistencies or disconnects across projects and organizational silos that cannot be necessarily resolved at the project level. A PgMP provides a holistic perspective to address the entire value creation life cycle, from the conception to the realization of benefits, and makes the connection between line managers who own the business and project managers who create the changes.

Managing Successful Programs

Managing Successful Programs (MSP) is based on three core concepts:[2]

- Transformational flow, which provides a route through the life cycle of a program from its conception to the delivery of the new capability, outcomes and benefits
- Governance, which allows an organization to put in place the right leadership, delivery team, organizational structures and controls, giving the best chance for success
- Principles, which are derived from positive and negative lessons learned from program experiences and are the common factors that underpin the success of any transformational change

PROJECT MANAGEMENT

Project management is the discipline of carefully planning, organizing, motivating and controlling resources to achieve specific goals and meet specific success criteria. A project is a temporary endeavor with a defined beginning and end, designed to produce a unique product, service or result to bring about beneficial change or added value. A project's main success criteria are scope, time and cost. Its primary constraints are quality, risk and resources. From the point of view of the sponsor, a project is defined by its profitability (Profitability P = Benefit/Cost with P>1, Cost of Capital (CC) and CC being composed of stockholders' Dividend Interest (DI) and bankers' Long-Term Debt Interest (LTDI), combined in the following formula: CC = xDI + yLTDI with x and y representing the respective share of long-term resources of the company).

There are three main typologies of projects: predictive, iterative and adaptive, each with a different methodology: PMP, PRINCE2 and Scrum, respectively.

Predictive Type: Project Management Professional

PMP is a project management certification based on the content of the *A Guide to the Project Management Body of Knowledge* (PMBOK Guide), which provides a foundation in a strong classical project management methodology and provides guidelines for managing individual projects; defines project management-related concepts; and describes the project management life cycle and its related processes, as well as the project life cycle. The PMP version 5 recognizes 47 processes that fall into five basic process groups and 10 knowledge areas that are typical of most projects. A project is called classical when the scope can be defined precisely upfront and most or all of the value is delivered at the end of the project (classical project example: a bridge). PMP is suited to all kinds of predictive projects, including IT projects.

Iterative Type: Projects in Controlled Environments, Version 2

PRINCE2 is an iterative, process-based method for effective project management based on seven principles, seven themes and seven processes.[3] The key features of PRINCE2 are focus on business justification, defined organization structure for the project management team, a product-based planning approach, emphasis on dividing the project into manageable and controllable stages, and flexibility that can be applied at

a level appropriate to the project. A project is called iterative when the scope can be defined upfront, but could be refined before each sequence, and some value can be created after each sequence (iterative project example: a new customer relationship management [CRM] module). PRINCE2 is suited mainly to IT iterative projects.

Adaptive Type: Scrum

Scrum[4] is an adaptive and incremental Agile software development framework that uses a flexible, holistic product development strategy in which a development team works as a unit to reach a common goal and enables teams to self-organize by encouraging physical colocation of all team members, as well as daily face-to-face communication among all team members and disciplines in the project.[5]

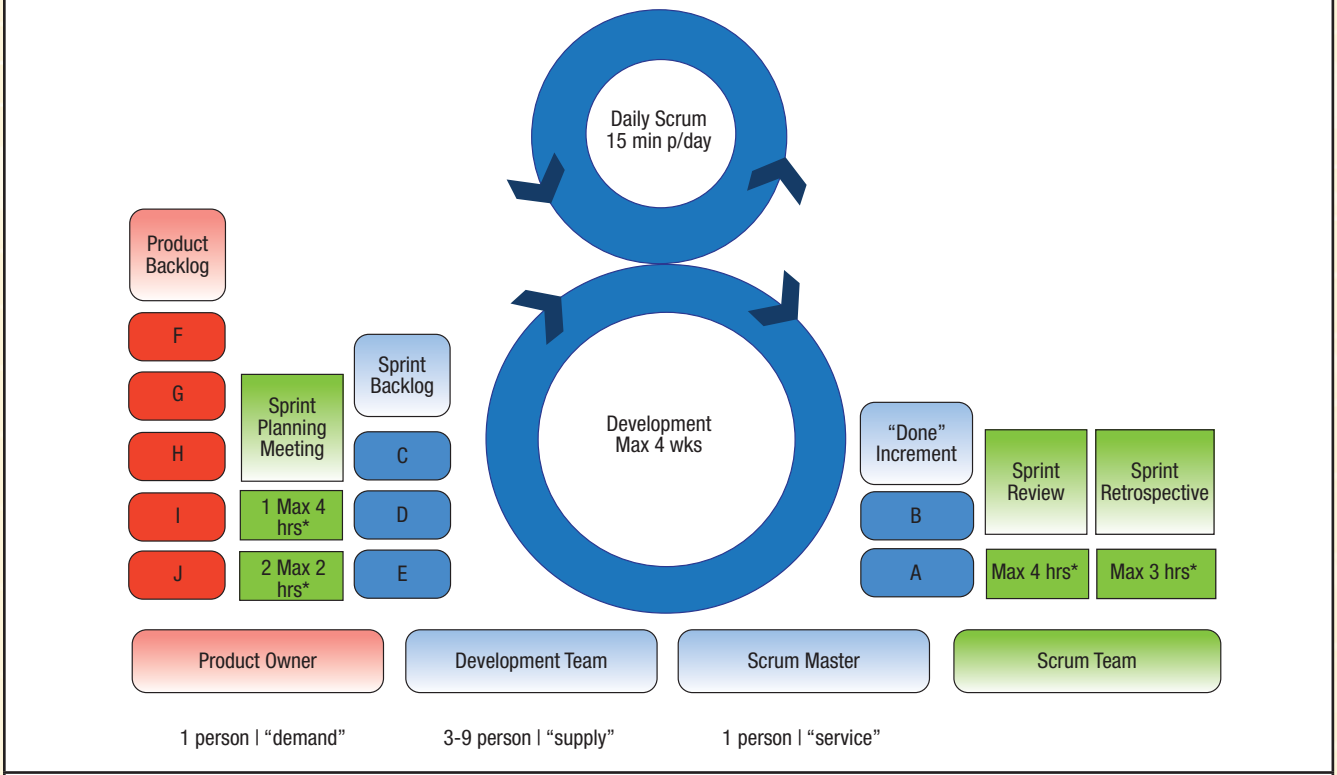
A key principle of Scrum is its recognition that during the production processes, customers can change their minds about what they want and need, mainly due to changing conditions in the environment.[6] As such, Scrum adopts an empirical approach, accepting that the problem cannot be fully understood or defined, focusing instead on maximizing the team's ability to deliver quickly and respond to emerging requirements (**figure 3**).

A project is called adaptive when the total scope cannot be precisely defined upfront and must be refined and updated before each sprint, and significant value can be created after each sprint (adaptive project example: Uber). Scrum is suited to adaptive projects, mainly web-innovative business projects that have a time-to-market effect (the first to launch an innovation makes sales that others will not make) and also, eventually, a first-takes-all effect (the first to launch an innovation can become the standard and then create a monopoly on the market).

BUSINESS ANALYSIS

Business analysis is the discipline of identifying business needs and determining solutions to business problems. As the project manager focuses on the project scope, the

Figure 3—SCRUM Framework



Source: Laurent Renard. Reprinted with permission.

business analyst focuses on the product scope—requirements analysis—and ensures that changes made to an organization are aligned to its strategic goals. These changes can include changes to strategies, structures, policies, business rules, processes and information systems. People being certified in project management (more so if applying for a PMP) or working in organizations having established project management practices will benefit from using the PMI-Professional Business Analysis (PBA) methodology, while business analysts working in pure business analysis organizations could, having fewer integration needs, opt for the Certified Business Analysis Professional (CBAP) certification, which is based on the Business Analysis Body of Knowledge (BABOK) guide.

Project Management Institute-Professional Business Analysis
PMI-PBA holders are experts in working with stakeholders to define an organization's requirements to shape the output of projects and ensure that they deliver the expected business benefit. PMI-PBA is oriented toward business analysts with, or wishing to get, project or program management experience, especially if they are working for a company that uses project management methodology based on the PMBOK (the reference model of the PMP certification).

Certified Business Analysis Professional
Certified Business Analysis Professionals (CBAP) master[7] the practice of enabling change in an organizational context by defining needs and recommending solutions that deliver value to stakeholders. CBAP is oriented toward business analysts planning to stay on the same path in their profession.

IT LIFE CYCLE MODEL

The IT life cycle model is a term used in systems engineering, information systems and software engineering to describe a set of processes for planning, creating, testing, deploying, operating and continuously improving an information system. The IT life cycle is about mastering the different phases, from requirements gathering of the customer through effective delivery of the expected value and its continuous optimization to stay competitive.

Information Technology Infrastructure Library
ITIL is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. ITIL describes IT processes, procedures and tasks that are not organization specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value and maintaining a minimum level of competency). ITIL is specifically suited for classical or iterative project management methodologies such as PMP or PRINCE2.

Development and Operations
Development and Operations (DevOps) is a set of practices for ITSM, more specifically Agile-oriented, that focuses on aligning IT services with the needs of business and emphasizes communication,[8] integration, automation and measurement of cooperation among software developers, quality assurance (QA) and IT operations. It aims to help an organization rapidly produce software products and services and improve operations performance.[9] The DevOps approach spans the entire delivery pipeline and includes improved deployment frequency, which can lead to faster time to market and lower failure rates of new releases. DevOps is specifically suited for adaptive project management frameworks such as Agile and, especially, Scrum.

PROCESS OPTIMIZATION

Process optimization is the discipline of adjusting a process so as to optimize some specified set of parameters without violating some constraint. The most common goals are minimizing cost and maximizing throughput and/or efficiency. This is one of the major quantitative tools in industrial decision making.

Lean Six Sigma
Lean Six Sigma is a methodology for process optimization that relies on a collaborative team effort to improve performance by systematically removing eight kinds of waste: defects, overproduction, waiting, nonutilized talent, transportation, inventory, motion and extra processing. Combining Lean manufacturing/Lean enterprise and Six Sigma, Lean Six Sigma is uniquely driven by a close understanding of customer needs; disciplined use of facts, data and statistical analysis; and diligent attention to managing, improving and reinventing business processes. Lean Six Sigma optimizes the global value delivered though all kinds of processes.

SELECT AND MASTER THE RIGHT TOOLS AND LEVERAGE SYNERGIES

When looking at a nail and a screw, one has to know the existence of the hammer and the screwdriver to choose the right tool. But in order to bring the best value, depending on the situation, one has to master both tools. If one has only

a hammer, everything looks like a nail, which is a reductive vision of the world. The more one masters the right tools, the bigger and the richer the world becomes.

AUTHOR'S NOTE

The author wishes to thank the Open Group, the Project Management Institute, Axelos, the Accrediting Professional Managers Globally, the Office of Government Commerce, Scrum (Ken Schwaber and Jeff Sutherland), the International Institute of Business Analysis, the DevOps Institute, Lean Six Sigma and Nathalie Massari.

ENDNOTES

[1] ISACA, COBIT 5, USA, 2012, *www.isaca.org/COBIT/Pages/FAQs.aspx*

[2] AMPG International, MSP Certification—Managing Successful Programmes, *www.apmg-international.com/msp.aspx*

[3] Projects in Controlled Environments, "What Is PRINCE2?," PRINCE2.com, *https://www.prince2.com/usa/what-is-prince2*

[4] Kumari, A.; "Scrum Adaptation in Clinical Data Management Practice," Scrum Alliance, 13 November 2014, *https://www.scrumalliance.org/community/articles/2014/november/scrum-adaptation-in-clinical-data-management-pract*

[5] Dice.com, More About Scrum, *https:// www.dice.com/skills/scrum.html*

[6] Project Management Institute, General Information About Business Analysis, PMI Professional in Business Analysis (PMI-PBA) FAQs, 2015, *www.pmi.org/~/media/PDF/Certifications/PMI-PBA_FAQs_v2.ashx*

[7] International Institute of Business Analysis, "What Is Business Analysis?," *www.iiba.org/Careers/What-is-Business-Analysis.aspx*

[8] Orlando, T.; "DevOps: Is There One Definition?," 3Pillar Global, *www.3pillarglobal.com/insights/devops-one-definition*

[9] Jasper Solutions, DevOps, *www.jaspersolutions.com/devops.html*

Optimizing Software Development With Lean Value Chain Analysis

Vimal Mani, CISA, CICA, Six Sigma Black Belt, is an associate vice president with Standard Chartered Bank and is based in Chennai, India. He is responsible for strategizing and building the information risk management practices of the bank's global human resources operations. Mani is a subject matter expert in enterprise information and IT governance practices and has assisted clients in addressing various information and technology risk. Mani also guides clients in a variety of business transformation and risk consulting engagements. He can be reached at *vimal.consultant@gmail.com.*

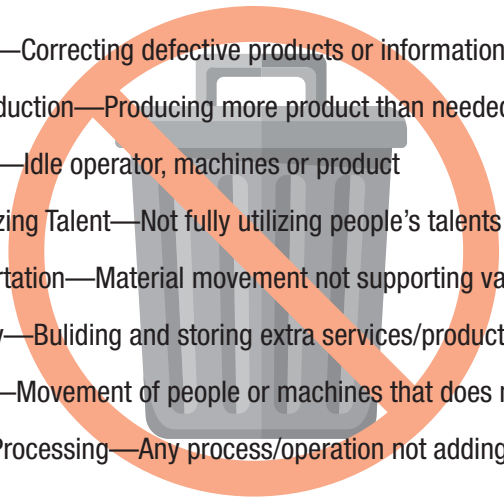
Lean is a philosophy of continuous, incremental improvement of business processes, products and services. Lean methodology helps in identifying the real value-adding activities involved in providing services to customers. Lean methodology is focused on shortening the time line between the customer request and the delivery of the service demanded by customers through the elimination of nonvalue-adding activities. However, to achieve this, an organization needs to understand customers' needs and wants and should identify key waste elements that will impact the delivery time line and quality of the services or products delivered to customers. Lean methodology defines waste as any activity that adds time and cost, but does not improve the services and products delivered to the customer.

Lean methodology does have a key technique called value analysis that helps identify value-adding activities present in a chain of activities. Value analysis in lean implementation involves assessing each process step through the eyes of the customer and determining whether the step is:

- **Value-adding activities (VA)**—These are activities that will directly achieve customer requirements and the ones for which the customer is willing to pay.
- **Nonvalue-adding activities (NVA)**—These are activities that will take time or resources, but do not directly achieve customer requirements, or the ones for which customers will not be willing to pay. Typical nonvalue-adding activities include reworking, inspection, movement and any of the eight wastes referred to in Lean methodology.
- **Value-enabling activities (VE)**—These are activities considered NVA from a customer perspective, but can satisfy a regulatory/compliance issue or other business requirement. These are also called "nonvalue added, but necessary," "business value add," or "nonvalue added, but required." For example, documentation required to satisfy regulatory compliance reporting is a value-enabling activity.

Figure 1 depicts considerations of Lean methods related to waste in a value chain.

Figure 1—Lean Methods Related to Waste in a Value Chain



- **D**efects—Correcting defective products or information
- **O**verproduction—Producing more product than needed
- **W**aiting—Idle operator, machines or product
- **N**ot Utilizing Talent—Not fully utilizing people's talents
- **T**ransportation—Material movement not supporting value-added steps
- **I**nventory—Buliding and storing extra services/products the customer has not ordered
- **M**otion—Movement of people or machines that does not add value
- **E**xcess Processing—Any process/operation not adding value to product

Source: Vimal Mani. Reprinted with permission.

The following are some Lean tools that are helpful in performing value chain analysis:

- **Voice of customers/customer satisfaction surveys**—The voice of customers helps in collecting customer experiences and expectations about services provided.
- **Data analysis**—This helps in analyzing the unstructured or structured data that are received in large volumes.
- **Kano model**—This model helps in defining customer requirements and translating them into specific processes that will deliver the desired products and services meeting customer requirements.
- **Quality function deployment (QFD)**—QFD helps in ensuring the quality of products and services.
- **Failure mode and effects analysis (FMEA)**—FMEA helps in identifying all possible failures in design of a process, product or service.
- **Critical to quality (CTQ)**—CTQ helps in identifying product and service quality attributes that are acceptable for customers.
- **Design of experiments (DoE)**—DoE helps in determining the relationship between factors affecting a process and the output of that process.
- **Kanban**—Kanban helps in visualizing work, reducing waste by limiting work in progress and maximizing customer value through a process known as value stream.

Each of the categories—VA, NVA and VE—have specific activities related to software development.

Value-adding activities related to software development include:

- Project planning
- Requirements analysis
- Requirements design
- Architecture and design
- Design reviews
- Coding
- Code reviews
- Testing
- Continuous integration
- Go live
- Knowledge transfer to clients

Nonvalue-adding activities related to software development include:

- Technical complexity that was not analyzed properly during requirements and project planning stages
- Presence of unwanted processes in the value chain
- Ineffective prioritization of requirements
- Incomplete/inadequate identification of tasks
- Wait time between the tasks
- Extra code and functionality developed for which customers will not be willing to pay
- Delays occurring in the project planning activities
- Ambiguous requirements analysis and definition
- Interruptions of ongoing tasks
- Too many parallel project activities
- Inadequate testing of developed software leading to redundant features
- Not using available team member knowledge and trying to reinvent things
- Overwhelming bureaucracy in the project environment
- Ineffective internal communication resulting in delayed project activities
- Lack of proper coordination between the product owner and development team
- Unassigned backlogs of work
- Lack of resources
- Teams working from different locations
- Lack of visibility of the information shared by more than one team
- Lack of technical skill sets among team members
- Late involvement of testers
- Inattention to the automation testing
- Partially completed/abandoned coding during the development process
- Extra- and low-value features developed, which may be rarely or never used by customers
- Waiting for completion of work from upstream and downstream teams
- Defects and lower-quality work that requires significant amount of revision
- Continuous switching or reallocation of work among team members
- Managerial overhead not producing tangible value for the project
- Delayed approvals resulting in delayed project deliverables
- Delays caused by waiting for project handoffs
- Time-consuming development of complex project dashboards/visual controls
- Daily meetings with no defined agenda

- Unstructured/unfocused quality assurance activities, such as project audits and reviews
- Missing acceptance criteria

Value-enabling activities related to software development include:

- Developing excessive amounts of project documentation
- Project compliance and regulatory reviews
- Management reviews
- Subject matter expert (SME) reviews

HOW LEAN VALUE CHAIN ANALYSIS HELPS

Value chain analysis helps software development teams gain a clear understanding of how long the planned software development activities will take to complete and how much NVA are present in the total planned activities. Value chain analysis also helps software development teams achieve dramatic reductions in time needed for software development and delivery to customers.

Implementing Lean value chain analysis helps IT services businesses identify waste and NVA present in software development and helps IT services delivery value chains by improving time to market, quality, cost, efficiency and effectiveness of overall IT operations. Waste is often intangible and difficult to identify in IT business processes. For example, delays are a significant category of waste/NVA in the IT services' business value chain (i.e., searching for specific information, NVA reviews, complex approval processes, slow response of applications, delays between coding and testing, aging of service tickets, delayed response time from the IT help desk). Productivity and time taken to deliver can be significantly improved by addressing the root causes of delays. Many global IT business organizations have experienced a 20 to 40 percent increase in IT productivity and reduced the delivery time of new applications and functionalities/features by 10 to 30 percent through the application of Lean techniques such as value chain analysis. As a result, IT service-oriented business organizations are able to achieve significant cost savings.

IMPROVED EXECUTION OF AGILE PROJECT MANAGEMENT PRACTICES

Lean methodology and techniques help optimize the end-to-end software development and delivery processes that are aimed at creating value for customers from the requirements stage to the go-live stage. Lean value chain analysis focuses on identifying NVA present in the IT delivery value chain that need to be removed. This involves adaptive software development processes, fast feedback cycles and significant involvement of the customer in the end-to-end process that forms the foundation of the Agile methodology. In short, it can be said that the Agile methods are Lean methods applied to the software development and delivery business. By marrying Lean and Agile principles with newly emerging techniques in markets such as development operations (DevOps)—a new technique emerging from the marriage of Agile development and collaboration among development teams and IT operation staff throughout the systems development life cycle (SDLC) stages—the value delivered to the customer can be significantly improved.

CONCLUSION

The idea behind the Lean methodology-driven software development is to eliminate as many NVA as possible from the software development value chain and deliver optimized value to customers in an optimized time period with optimized quality. Uncovering and reducing NVA or VE activities that do not add value to the software development value chain from the eyes of the customer are the keys to optimizing both the effectiveness and efficiency of a software development value chain.

Feature

Quick Fixes for Improving Cyberdefenses

Sanjiv Agarwala, CISA, CISM, CGEIT, BS 25999/ ISO 22301 LA, CISSP, ISO 27001:2013 LA, MBCI, is currently director and principal consultant at Oxygen Consulting Services Pvt. Ltd. Agarwala has more than 17 years of experience across multiple industry domains in various information security roles and has expertise in areas such as information security management systems, risk management, cybersecurity, systems audit, IT governance and business continuity management.

There is an increasing trend of companies moving to e-business models with connectivity using multiple channels such as the Internet, mobile devices, social media, and the cloud in an anytime, anywhere, always-on model. Businesses, small or large, are part of cyberspace and are continually connected directly and indirectly. While this has definitely improved business volume, it has also increasingly attracted the attention of cybercriminals.

Cyberattacks continue to rise at an alarming rate. Hacking tools are freely available on the Internet. Script kiddies are performing scans and attacks for fun and sometimes just to see if their efforts work. There is also an increase in organized and well-funded cybercriminal groups that continuously target organizations and exercise great patience to systematically exploit the weaknesses they discover. Improved connectivity has also allowed cybercriminals to expand their possible attack vector, so cyberrisk has become a key issue to be addressed by all organizations.

While most organizations already have good security practices in place, they need to spend quality time and resources for long-term cyberdefenses. This article provides quick fixes for closing cybersecurity loopholes and improving cyberdefenses as early as possible before cybercriminals can escalate the level of attacks on any organization.

RAISE CYBERSECURITY AWARENESS AT ALL LEVELS

People are the critical element in the journey toward improved security. Many cyberattacks are successful due to unaware and undisciplined end users. In many organizations that are already certified to ISO 27001 and other regulatory requirements, the board of directors (BoD) and end users may be curious about what is new in cybersecurity. If this curiosity is not addressed, the topic may not get serious attention. It is increasingly important for information security teams to create awareness of cybersecurity at all levels. Using examples of various data breaches such as the Target and Sony attacks[1] can quickly help demonstrate how cyberattacks can impact the organization.

REEXAMINE RISK MANAGEMENT EXERCISES

It is quite possible an organization already has a risk assessment process in place, but in the face of cyberthreats, it becomes important to reconsider the nature of these attacks and revisit the risk assessment exercise. Some of the popular risk management standards and frameworks that can be referred to for the risk assessment are ISACA®'s COBIT® 5,[2] ISO 31000:2009, Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management—Integrated Framework*, OCTAVE, the US National Institute of Standards and Technology (NIST) Risk Management Framework and many more. Many organizations may rate the threat and vulnerabilities as low, considering there are no known reported cyberattacks on the organization. Other organizations may have a false sense of security and confidence that, since they have security devices, tools and techniques, they are already cybersecure. It is time to reexamine whether these security devices can be bypassed by any means and realistically assess the risk to the environment. Risk management teams need to keep abreast of how cybercrimes are currently conducted and factor into similar use cases in their risk assessment exercise.

STRENGTHEN MECHANISMS FOR AUTHENTICATION AND AUTHORIZATION

Passwords, personal identification numbers (PINs), tokens and digital certificates are the most commonly used authentication mechanisms. While an organization may have an excellent password policy, it becomes important to evaluate whether it is implemented properly across the entire organization. Authentication management systems should not accept any weak authentication credentials. System and network administrators need to be extra careful, as they are responsible for highly privileged accounts.

Compromise of the authentication system itself and highly privileged accounts are high-risk areas that need to be reconsidered.

STRENGTHEN END-POINT PROTECTION MEASURES

Users with desktops, laptops, mobile handsets and personal digital assistants (PDAs) can be very lucrative targets for cyberattackers. Typically, organizations would deploy from basic antimalware to comprehensive end-point protection measures. Antimalware solutions should be able to detect and protect from various kinds of threat agents such as viruses, worms, Trojans, spyware, adware, keyloggers and other variants of malware. Organizations should ensure that there is adequate protection at points of entry through Internet and email access. End-point protection solutions should be capable of recognizing suspicious activity on end-user systems such as unusual ports and traffic patterns, file alteration, attacks on system files, and other activities that can be of interest to a cyberattacker.

CONDUCT REGULAR PENETRATION TESTING AND TAKE CORRECTIVE ACTION

For organizations that have not conducted penetration testing (internal and external), it may be time to consider this as one of the most effective ways to proactively identify technical security vulnerabilities in the system that could potentially be exploited by an attacker. Some organizations do perform penetration tests, but the question to ask is whether they have tracked confirmed vulnerabilities to risk mitigation measures and closure. If they have not, then these are the very vulnerabilities that may be exploited by cybercriminals and cause damage to the organization.

IMPROVE THE PATCH MANAGEMENT PROCESS

It is not uncommon to see vendors releasing multiple patches for operating systems (e.g., Windows variant, UNIX variant) and sometimes within a short time period. From an organizational perspective, it is perceived as a taxing process as it involves making sure that the patch not only addresses the known security issues, but also does not interfere with the business functionality. Many times, application vendors advise customers not to apply the latest patch because their software will not work with the new patch. And if this very system happens to be publicly exposed, the risk multiplies.

Cybercriminals are not only exploiting the known but uninstalled patches, but also zero-day vulnerabilities, for which vendors have not yet issued a patch. Considering these scenarios, it becomes important for the organization to focus on the necessary discipline for implementing the patch management process.

STRENGTHEN THE LOG MONITORING PROCESS

Most organizations have some level of log monitoring, and many of the automated tools show the top Internet Protocol (IP) addresses, top systems where attacks are concentrated, traffic patterns and many other details. Often, this is provided as a feature by the log monitoring system, but it is seldom used effectively. The reports may be generated, but not be reviewed adequately. Sometimes the reports are generated with greater vigor at the start of a new system deployment but monitoring tapers off over time. This is good news for cybercriminals because their activities may not be properly tracked and detected by the organization. Some attacks have become very sophisticated and organizations need to think of security event management-type solutions, but still these systems will not be useful unless the reports generated are fully analyzed and timely action is taken. Discipline in the log monitoring process is required for improved cyberdefense.

IMPROVE THE SECURITY INCIDENT RESPONSE PROCESS

Organizations may deploy the latest technologies, but in the war between cybercriminals and cyberdefense personnel, an effective security incident response process is a must. Cybercriminals will always attempt new techniques to bypass security, and technology may not always be the solution to detect a new cybercrime attack. Periodic test exercises (e.g.,

tabletop) and proper training of end users to help them recognize cyberincidents go a long way toward the prompt detection of such attacks. Cyberexperts should be involved to review all the incidents to ensure that cyberattacks do not go undetected and effective responses to cyberattacks are planned and undertaken. Sometimes a simple malware-related incident may turn out to be a targeted cyberattack.

CONSIDER THE DISASTER RECOVERY PROCESS FOR CYBERATTACKS

Most organizations have some type of disaster recovery process to tackle events such as environmental hazards, network failures, and hardware and application failures. However, organizations cannot afford to overlook the damage that can be rendered by the very specifically targeted attacks conducted by cybercriminals. Organizations need to include and plan for various cyberattacks, such as denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks, among the many hazards addressed in their disaster recovery process.

CONCLUSION

Cybersecurity threats are on the rise. Every organization is connected to one another, and any organization can become the victim of cyberattacks. A good strategy to strengthen the basic controls discussed in this article will go a long way toward improving the organization's cyberdefense.

Fundamental controls such as passwords; security awareness; antimalware and end-point protection; patch management; log monitoring; security incident management; and security at the operating system, application, database and network layer have become even more important.

Along with the strengthening of these controls, organizations have to start thinking like a smart hacker and proactively start protecting all the critical assets that may be of interest to an adversary. The offense informs the defense. Prioritization, metrics, continuous diagnostics, mitigation and automation are the five critical tenets of an effective cyberdefense as reflected in the SANS Critical Security Controls.[3]

Additional specific controls from ISO 27001:2013, COBIT® 5 and other relevant best practice guides can help further strengthen cyberdefenses as a long-term solution. Users have become mobile and more demanding; technology has made devices more compact with more features in an interconnected world; and, simultaneously, threats have evolved and attackers have become smarter. Cyberdefense can be more effective only when these transitions are understood and smart defense mechanisms implemented.

ENDNOTES

[1] McCandless, D.; T. Evans; "World's Biggest Data Breaches," *Information Is Beautiful*, infographic, 6 August 2015, *www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*

[2] ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

[3] SANS Institute, Critical Security Controls for Effective Cyber Defense, *www.sans.org/critical-security-controls/*

Application Security Risk
Assessment and Modeling

Shubhamangala B. R. is pursuing a Ph.D. with particular interests in application security, security requirements, compliance and risk. She is an associate professor in the Department of Computer Science and Engineering at Jain University (Bangalore, India). She has been previously published in the American Society for Quality *Software Quality Professional* journal and many of her papers are indexed in the Institute of Electrical and Electronics Engineers' Explore database. She can be reached at *brm1shubha@gmail.com*.

Snehanshu Saha, Ph.D., has taught computer science at PES Institute of Technology South Campus (Bangalore, India) since 2011 and heads the Center for Basic Initiatives in Mathematical Modeling. Saha has been working on the subvocalization of text using electroencephalography data and has published scholarly articles on the subject.

Breach incidents at organizations such as JPMorgan Chase, eBay, Home Depot, Sony Pictures Entertainment, the European Central Bank and the US Postal Service[1] beg the questions: Why are breaches continuing despite deploying cutting-edge solutions supported by compliance to thwart the attacks? Are applications more secure relative to current threats or less secure? How much more security is required? What is the current level of risk posed by application security? Can the security budget be decreased or should it be increased? If increased, to what extent is risk reduced? What is the applications' change in the risk level before and after the deployment of innovative security measures?

No definitive answer exists for these questions because there is no standard metric to know the exact status of application security. Unanswered questions have paved the way for attackers to continue exploiting applications. Therefore, a security metric that can quantify the risk posed by applications is essential to make decisions in security management and thwart attacks.

Currently, a generic risk assessment metric is used to assess application security risk (ASR). This does not encompass the basic factors of application security such as compliance, countermeasure efficiency and application priority. Obviously, the results are not commensurate with actual risk posed by application security. Real application security risk is perceived and not measured. Hence, organizations are not able to implement the required security controls. The business is unaware of its applications' susceptibility to attack. This is the main reason for continued attacks on applications despite deploying robust security measures. ASR measurement requires a specifically designed metric that involves all of the factors of application security. This article aims to define the standard for security in applications by designing a metric.

The entire process of metric design allows the business to find the optimum answer for the following questions:

- What path could an attacker take to get inside the application?
- What tools are required to defeat the existing security measure?
- What are the possible signs of an attack particular to each category of application?
- Can existing security measures detect the attack?

Answering these questions ensures that the organization has considered potential attacks and helps toward the implementation of required controls, if existing measures are inadequate.

EVALUATION OF THE EXISTING RISK METRIC

In general, risk is the probability of occurrence of an event that would have a negative effect on a goal.[2] Risk is a field. It is perception dependent. No clear definition for the concept of ASR exists. However, in this article, ASR is defined as a measure of an application's susceptibility to an attack and the impact of that attack. The following generic formula is currently used (with slight variations) to measure risk:

$$\text{Risk} = \text{Probability of Attack} \times \text{Impact of Attack}$$

Considering this equation, the impact of an attack is relatively easy and straightforward to assess. The term "probability of attack" indicates how likely it is that the attack occurs. The calculation of the probability of an attack has practical limitations.[3] The probability of simple situations (e.g., tossing a coin, picking a card, throwing a die) can be derived from probability principles. Evaluating the probability of real-time events (e.g., weather incidents, hurricanes, earthquakes) is possible based on historical records. But in the case of attacks, probability does not work because attackers do not work in any statistical pattern. For instance, consider the breach of retailer Home Depot in 2014. There is no previous history of breaches at Home Depot. What was the probability of a Home Depot breach before it happened, and what is the probability of a

Home Depot breach again in the future? Can probability predict that Home Depot will be breached again or never again? Even if probability provides an answer, will it match reality? It is clear that a risk formula has limited value in the field of application security. Additionally, this formula does not provide the risk measure present in applications as it focuses on likelihood of attack. Hence, organizations require a realistic application risk measurement that is independent of the probability of attack.

Application security is made up of four factors: vulnerability, countermeasure, breach impact and compliance.[4] Analyzing these key factors, four prime terms on which ASR depends emerge. The four key terms are breach cost (Bc), vulnerability density (Vd), countermeasure efficiency (Ce) and compliance index (CI). CI is the ratio of a number of compliance requirements met to a total number of compliance requirements in the application. Vd is the ratio of number of vulnerabilities to the size of software.[5] Ce is the measure of implementation efficiency of countermeasures. Bc is the assessment of likelihood of cost that would be incurred in case of attack. Based on application security key terms, a model for ASR has been designed. **Figure 1** represents this model.

Figure 1—Application Security Risk Model

Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.

For this model, Bc, Vd and CI are the inputs. The ASR metric is the output.

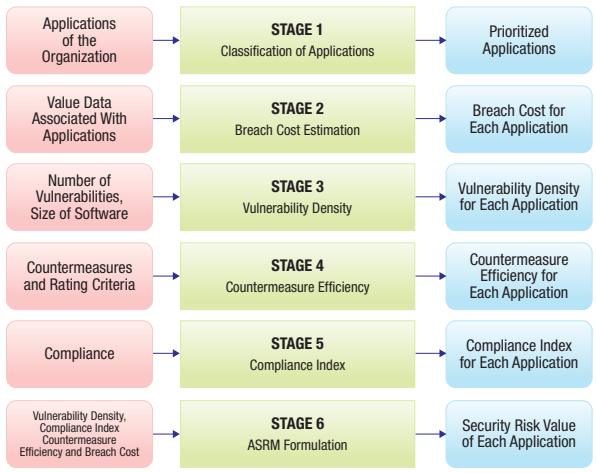
DESIGNING A METRIC TO FIND THE QUALITY OF APPLICATION SECURITY

Based on the application security risk model (ASRM), a metric to measure the risk of application security has been created. It is the ratio of the product of vulnerability density and breach cost to the product of countermeasure efficiency and compliance index. Bc and Vd are directly proportional to ASR. CI and Ce are indirectly proportional to ASR. The following is a mathematical representation of this formula:

$$\text{ASRM} = \frac{\text{Vd} \times \text{Bc}}{\text{Ce} \times \text{CI}}$$

The method of designing the ASRM includes six stages (**figure 2**).

Figure 2—ASRM



Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.

Stage 1: Classification of Applications

Organizations conduct business through applications. Organizations have dozens, hundreds or even thousands of applications. Every application has a unique role. Not all applications offer the same level of risk. Therefore, the classification of applications is important. This aids in determining the risk level offered by applications.

Classification strategy is organization-specific. Based on compliance stringency and the likely impact the application would cause in a breach, applications are classified into five groups, listed from highest level of risk to lowest level of risk: critical, important, strategic, internal function support and general function support applications. They are identified by notations A1, A2, A3, A4 and A5, respectively. Each group may contain one, a few or many applications:

- **Critical applications (A1)**—Critical applications are the highest-priority applications and high availability is expected. Downtime of these applications, even for a few seconds, could result in serious financial loss, legal loss, customer dissatisfaction and loss in productivity. Because these applications access high-sensitivity data, breaches to them can result in the total halt of organization service, high-risk data exposure, severe legal and financial loss, and complete loss of customer trust and brand value. Compliance stringency is very high for these applications. Enterprise applications, e-business applications and client-specific lines of business applications are prime categories of critical applications.
- **Important applications (A2)**—Important applications play a considerable role in organizational functioning. As the name suggests, these applications are important for the organization and their compliance stringency is high. Examples of important applications include the National Do Not Call Registry filter application in the US, simulators, data monitoring applications (stock and shares), content management systems and supply chain management applications. Availability of these applications during business hours is expected. Breaches due to these applications could result in a severe impact on an organization. Downtime of important applications results in considerable loss of revenue, customer dissatisfaction and moderate loss of productivity. The consequences in the case of a breach of an important application are significant disruption to the business function, loss of customer or business partner confidence, failure to deliver organizational services, substantial financial loss, and a compromise of confidential information.
- **Strategic applications (A3)**—The applications that support or shape the business objective are called strategic applications. These applications are developed in response to innovative corporate business initiatives. Strategic applications aim to lead the organization to outperform its competitors and lead the industry. If breached, these applications would have a damaging impact on the organization, including legal liability, significant expenditure to recover and a moderate disruption in functionality of services. An example of a strategic application is online banking through a cell phone, which provides customers with ease of operation. The data accessed by this type of application are confidential and compliance stringency is moderate.
- **Internal support applications (A4)**—Internal support applications cater to the internal functional needs of the organization and access organizations' internal data. Applications such as employee attendance monitoring, warehouse applications and customer relationship management (CRM) applications fall under the internal support application category. A breach to this category would cause significant damage resulting in moderate financial loss, mild disruptions in functionality, negative publicity and moderate expenditure to recover.
- **General support applications (A5)**—General support applications access public data and provide support to end-user functions. Examples include clinical health care support applications, job portals, social sites and front-end support applications. Security breaches of these applications result in minor impacts such as trivial financial loss, trivial effects on business function and minimal effort to recover.

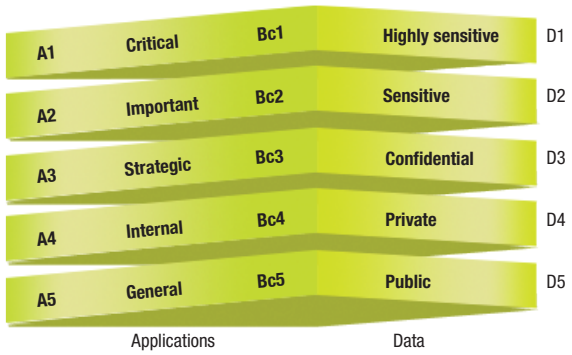
Stage 2: Quantification of Breach Cost

Breaches are very expensive to organizations. As a result of increases in frequency and sophistication of attacks, the cost of breaches is growing. The average cost of a breach to a company was US $3.5 million in 2014, 15 percent more than what it cost the previous year.[6] Bc includes tangible costs (e.g., legal cost, compliance cost, productivity loss cost) and intangible costs (e.g., loss of customer trust, loss of reputation). To assess a Bc (α), a rating system ranging from 0 to 1, where 1 denotes the maximum cost and 0

> "The cost of a data breach depends upon on two factors: application criticality and corresponding sensitivity of data the application accesses."

indicates the minimum cost, is used. The cost of a data breach depends upon on two factors: application criticality and corresponding sensitivity of data the application accesses. The cost of breaches that would occur due to each category of application starting from A1 to A5 is assessed and notated as Bc1, Bc2, Bc3, Bc4 and Bc5, respectively. The total Bc (α) of the organization is the sum of the individual Bc's. **Figure 3** represents the concept of applications' association with type of data (D1 through D5) and Bc.

Figure 3—Concept of Application Classification



Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.

To understand the Bc estimation, a sample Bc rating allotment for each category of data is shown in the last column of **figure 4**. As seen in **figure 4**'s table, adding individual Bc's, the total cost of a breach obtained is 1. A sample Bc rating of 0.4, 0.25, 0.2, 0.1 and 0.05 is allotted for applications from A1 to A5, respectively.

Figure 4 represents the concept of application categorization and Bc.

Figure 4—Sample Application Classification and Quantification of Breach Cost

Application Category	Breach Impact	Data Category	Breach Cost
Critical (A1)	Critical	Highly sensitive	Bc1 = 0.4
Important (A2)	Serious	Sensitive	Bc2 = 0.25
Strategic (A3)	Damaging	Confidential	Bc3 = 0.2
Internal support (A4)	Significant	Private	Bc4 = 0.1
General support (A5)	Minor	Public	Bc5 = 0.05

Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.

Stage 3: Application Vulnerability Density

Vulnerabilities are the security holes that are specific to an application.[7] Vulnerabilities do not cause any damage to the functioning of the application, but they allow attackers to exploit the application. Vulnerability exploitation may have a cascading effect, leading to a breach. Software size is considered in kilo lines of code (KLOC) or function points (Fp). Mathematically, it is represented as:

$$\text{Vulnerability Density (Vd)} = \frac{\text{Number of Vulnerabilities (Vu)}}{\text{Size of Software}}$$

This article considers the size of software in function points. The Vd for each application category is found by taking the average of individual Vd's for all applications in that application category.

To calculate the organizationwide Vd, an average of the Vd's for categories A1 through A5 is taken.

Stage 4: Countermeasure Efficiency

Vulnerabilities are the basic reason for security attacks. They pose the greatest risk to application security. A specific countermeasure can be more effective against a particular vulnerability and less effective against another. The other key issues with the countermeasures are that they may be obsolete, faulty, ineffective or inappropriate.[8] Hence, the evaluation of countermeasures against the discovered vulnerabilities is necessary to determine the risk level present in applications. The framework for countermeasure evaluation has five steps:

1. Consider the application category, application name and its vulnerabilities. There may be one or many vulnerabilities.
2. Discover the existing countermeasures against vulnerability. Their efficiency in mitigating the vulnerability is assessed using a rating scale ranging from 0 to 5. **Figure 5** provides the rating assessment criteria.
3. Sum the Ce ratings. This sum is called the total score.

Figure 5—Countermeasure Rating	
Rating (0-5)	**Assessment**
5	Excellent
4	Effective
3	Adequate
2	Inefficient
1	Poor
0	No existence of countermeasure
Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.	

4. Calculate the Ce factor (Cf) for each application. This is calculated by dividing the total score by the product of five times the number of vulnerabilities. The corresponding Cf is denoted by notations Cf_1, Cf_2, ...Cf_i, respectively. In the next step, Ce for application category A1 denoted by notation C1 is calculated by taking the average of Cf_1 to Cf_i.
5. Follow the same pattern of steps to determine the Ce for the remaining layers.

Stage 5: Compliance Index

Compliance means conforming to a rule, such as a specification, policy, standard or law.[9] In the field of security, compliance refers to an organization's conformity with accepted policies, regulatory requirements imposed by industry or government bodies, standard regulations, guidelines, customer expectations, and industry best practices. Each of these policies and regulations has a set of requirements, called compliance requirements.[10] Noncompliance results in disastrous effects, including government fines, canceled accounts, productivity loss, business disruption, revenue loss, fines, fees, penalties and other legal settlement costs. Noncompliance costs organizations, on average, 2.65 times more than meeting compliance rules.[11] Because of this cost, knowing the degree to which the application is compliant is vital.

CI can measure whether applications are compliant. If they are compliant, this index can measure the extent to which they have implemented the compliance requirements. CI is the measure of efficient implementation of compliance requirements divided by the total number of compliance requirements.

Mathematically, it is represented as:

$$CI = \frac{\text{Implementation efficiency of compliance requirements } (CR_e)}{\text{Total number of compliance requirements } (CR_t)}$$

The process of compliance index calculation includes four steps.

Step 1: Extract and Prioritize (CR)

Implementation efficiency of compliance requirements (CR) is measured by finding the depth of implementation of CR using a weighted rating methodology. Not all CR have the same priority. External CR, such as government regulation, laws and industry policies, have higher priority than, for example, internal CR, such as best practices, customer requirements or organization standards. The priority of CR depends upon the magnitude of damage that would be caused due to noncompliance. Consider the factors of legal importance with regard to CR, penalty, damage potential, depression in business value and customer distrust that would result from noncompliance. CR are divided into three categories: mandatory CR (C1), adequate CR (C2) and optional CR (C3). Mandatory CR are of the highest priority and these requirements are expected to be implemented unfailingly. Nonimplementation of these requirements causes severe legal and organizationwide consequences. C2 are of medium priority. Their implementation is subject to application type, application domain and customer expectation. C3 are of low priority and their implementation depends on customer requirements and the application deployment platform.

The total CR are represented as a set of requirements ranging from R_1 to R_n:

$$CR = \{R_1, R_2, \ldots\ldots\ldots\ldots R_n\}$$

These requirements are divided into three groups:

- C1: {set of mandatory requirements}
- C2: {set of adequate requirements}
- C3: {set of optional requirements}, → CR={C1+C2+C3}

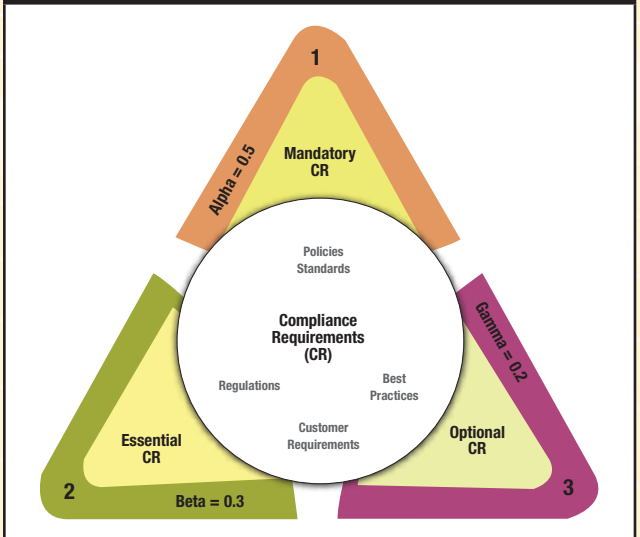
To understand the concept of CR classification, consider the payment gateway (A1) application of the A1 category. The A1 application contains 36 CR. It includes 20 C1 requirements, 12 C2 requirements and four C3 group requirements. The classification of CR is illustrated in **figure 6**.

Figure 6—Illustration of CR Classification					
Application Category	**Application A_x**	**CRA1 {R1, R2…Rc}**	**C1 {R1…Ra}**	**C2 {Ra+1…Rb}**	**C3 {Rb+1…Rc}**
A1	Payment gateway (A1)	36	20	12	4
*CRA1=Total number of CR for the application A1					
Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.					

Step 2: Assign Weights to CR

As the priority of CR varies, weights are assigned to the three categories of CR—C1, C2 and C3—based on the priority and factors such as application deployment, platform, size and number of users. Weights denoted by the terms *alpha* (α), *beta* (β) and *gamma* (ϒ) are assigned to each category of compliance—C1, C2 and C3, respectively. For the purpose of better understanding this concept, weights have been assigned here—0.5 for *alpha* (α), 0.3 for *beta* (β) and 0.2 for *gamma* (ϒ). These weights are subject to variations. Practically, it is dependent on organization and application demography. The concept of classification and assignment of weights to CR is represented in **figure 7**.

Figure 7—CR Prioritization



Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.

Step 3: Assess Implementation Efficiency of CR

Once the requirements are classified into C1, C2 and C3 groups, the implementation efficiency of CR is evaluated.

The rating methodology is a scale of 0 to 5. Initially, every requirement is assessed for implementation efficiency. In the case of nonimplementation of CR, a rating of 0 is assigned. If a requirement is implemented, the efficiency of the implementation is assessed and ratings are assigned in the range of 1 to 5. Assessment criteria for CR is given in **figure 8**.

Figure 8—Rating Methodology

Rating (0-5)	Implementation Assessment	Explanation
5	Excellent	Well exceeds objective
4	Effective	Exceeds objective
3	Adequate	Meets objective
2	Inefficient	Needs improvement
1	Poor	Reconsider implementation
0	Not implemented	Requirement implementation missing

Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.

Figure 9 illustrates the rating methodology of CR for C3 of payment gateway, part of the critical group application. It contains four requirements under C3. Each requirement is assessed for implementation efficiency using the ranking table. Ratings in the range of 0 to 5 are assigned for each requirement. The total score is calculated by adding the individual scores of applications. The implementation efficiency (IF_{CX}) is calculated by the formula:

$$\frac{\text{Total score}}{5 \times \text{Number of requirements}}$$

The same procedure is followed for all of the CR.

In **figure 9**, the implementation efficiency for C3 for the application A1 is 0.7. Following a similar pattern, implementation efficiency is calculated for all of the requirements.

Step 4: Calculate Compliance Index

Once the implementation efficiency for C1, C2 and C3 is obtained, these values are multiplied by correlating the weight factor *alpha* (0.5), *beta* (0.3) and *gamma* (0.2). CI is the sum of these values. The process is illustrated in **figure 10**.

In the first section, **figure 10** provides the formulas to find CI. In the second section, it provides a sample calculation of CI for AC1 category application. Following the same procedure, the CI for each category of applications is calculated. The CI for the entire organization is calculated by taking the average of individual category compliance indices. The formula is:

$$CI_{ORG} = \frac{(CI_{AC1} + CI_{AC2} + CI_{AC3} + CI_{AC4} + CI_{AC5})}{5}$$

CI values for all five application categories are provided in **figure 11**.

Figure 9—Illustration of Rating Procedure for CR

Application: Payment gateway (A1) in the AC1 category NCRq = 04 = {R1, R2, R3, R4}						
CRq $\{R_1,R_2 \ldots R_4\}$	R1	R2	R3	R4	Total score (T_{sX})	IF_{CX}
Rating	R_{a1}	R_{a2}	R_{a3}	R_{a4}	$T_{s1} = R_{a1} + R_{a2} + R_{a3} + R_{a4}$	$IF_{C3} = \frac{T_{s1}}{5 \times NCRq}$
Sample rating for C3 in A1						
Rating	5	3	2	4	$T_{s1} = 5 + 3 + 2 + 4 = 14$	$IF_{C3} = \frac{14}{5 \times 4} = \frac{14}{20} = 0.7$
NCRq = Number of CR in C3 of A1 CRq = CR in C3 of A1 IFCX = Implementation efficiency factor						
Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.						

Figure 10—Illustration of Calculation of Compliance Index

AC	A ID	C_{TR}	Compliance Requirement Implementation Efficiency			Weighted IM Efficiency			CI for Each Application	CI for Each Category
			IF_{C1}	iF_{C2}	IF_{C3}	α x IF_{C1}	$\beta \times IF_{C1}$	$\Upsilon \times IF_{C1}$		
AC1	A_1	C_{TR1}	V_{11}	V_{12}	V_{13}	$V_{11} \times 0.5 = V_{14}$	$V_{12} \times 0.3 = V_{15}$	$V_{13} \times 0.2 = V_{16}$	$CIA_1 = V_{14} + V_{15} + V_{16}$	$CI_{AC1} = \left(\frac{CIA_1 + CIA_2 + CIA_3 + CIA_4}{4}\right)$
	A_2	C_{TR2}	V_{21}	V_{22}	V_{23}	$V_{21} \times 0.5 = V_{24}$	$V_{22} \times 0.3 = V_{25}$	$V_{23} \times 0.2 = V_{26}$	$CIA_2 = V_{24} + V_{25} + V_{26}$	
	A_3	C_{TR3}	V_{31}	V_{32}	V_{33}	$V_{31} \times 0.5 = V_{34}$	$V_{32} \times 0.3 = V_{35}$	$V_{33} \times 0.2 = V_{36}$	$CIA_3 = V_{34} + V_{35} + V_{36}$	
	A_4	C_{TR4}	V_{41}	V_{42}	V_{43}	$V_{41} \times 0.5 = V_{44}$	$V_{42} \times 0.3 = V_{45}$	$V_{43} \times 0.2 = V_{46}$	$CIA_3 = V_{44} + V_{45} + V_{46}$	
	Illustration of Compliance Index for A1 Category									
A1	A_1	36	0.9	0.85	0.7	0.45	0.255	0.14	0.845	$CI_{AC1} = 0.85$
	A_2	42	0.9	0.84	0.76	0.45	0.252	0.152	0.854	
	A_3	40	0.9	0.85	0.73	0.45	0.255	0.146	0.851	
	A_4	46	0.92	0.82	0.71	0.46	0.246	0.142	0.848	
Vx = Value obtained IM = Implementation										
Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.										

Figure 11—ASR for Each Application Category									
Application Category	Bc	Vu	Fp	Vd	Vd*Bc	Ce	Compliance Index	ASRM = Vd*Bc/ Ce*CI	ASRM %
A1	0.4	8.00	12.00	0.67	0.27	0.85	0.85	0.369089	36.908
A2	0.25	12.00	20.00	0.60	0.15	0.83	0.75	0.240964	24.096
A3	0.2	20.00	25.00	0.80	0.16	0.71	0.55	0.409731	40.973
A4	0.1	32.00	40.00	0.80	0.08	0.65	0.51	0.241327	24.132
A5	0.05	40.00	35.00	1.14	0.06	0.60	0.42	0.226757	22.675
Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.									

Stage 6: ARSM Formulation

Combining equations for Vd, Bc, CI and Ce, the ASRM can be written as:

$$ASRM = \frac{Vd \times Bc}{CI \times Ce}$$

$$\rightarrow ASRM = \frac{\left(\frac{Bc1 \times Vd1 + Bc2 \times Vd2 + Bc3 \times Vd3 + Bc4 \times Vd4 + Bc5 \times Vd5}{5}\right)}{\left(\frac{CI_{AC1} + CI_{AC2} + CI_{AC3} + CI_{AC4} + CI_{AC5}}{5}\right) \times \frac{(C1+C2+C3+C4+C5)}{5}}$$

Substituting the corresponding values for threat resistance and CI from previous figures, the value of the ASR for the whole organization can be computed. **Figure 11** represents the value of the ASR for each application category.

The highest ASR value is 40.97 percent for strategic applications. However, the risk posed by critical and important applications are of vital concern. The lowest value of ASR is 22.65 percent for the A5 group of applications.

ASR THRESHOLD HEURISTICS

The use of the ASRM allows for the determination of the risk level present in applications. Not all risk can be resolved immediately due to budget and resource constraints. Developing the right strategy for the prioritization of risk helps avoid security attacks on applications. A heuristics-based risk threshold methodology can be used to develop an ASR mitigation strategy. Heuristics are the rule-of-thumb techniques to solve the problem.[12] Using two factors—the application criticality and risk value obtained by application of the ASRM—organizations' specific risk threshold levels can be determined. Heuristics are used to design the threshold levels. ASR heuristics are formed in combination with business objectives, strategic goals and mission priorities. The process of developing a risk threshold heuristic is illustrated in **figure 12**.

For critical applications, a risk value less than 10 percent is accepted. Any risk above this range calls for mitigation action. Similarly, organization-specific risk threshold heuristics can be formed for each category of applications to achieve better application security.

Figure 12—ASR Threshold Heuristics			
Heuristics (H)	ASRM Value	Risk Category	Mitigation
H1	> 20%	High	Immediate
H2	15-20%	Moderate	As soon as possible
H3	10-15%	Low	Organization's discretion
H4	<10%	Accepted	None required
Source: Shubhamangala B. R. and S. Saha. Reprinted with permission.			

RESULTS AND DISCUSSIONS

The ASRM has wider applications in organizations subject to application complexity, application domain, market demands and customer expectations. A few usages of the ASRM include:

1. The ASRM is applicable to all types of applications. The quantification of risk through a metric provides a platform to know the real risk of application security.
2. The ASRM provides a realistic measure of application security risk. This formula avoids using the probability of attack and instead looks at the components of application security risk.
3. Application classification provides an intelligent avenue to prioritize the risk mitigation process.
4. The security investment to mitigate risk is justifiable using the ASRM. The ASRM and application classification provides an opportunity to choose cost-effective solutions based on risk mitigation techniques.
5. Vulnerability identification provides awareness on the nature and strength of vulnerabilities present in all of the applications of an organization. This identification may lead to the discovery of a deficiency in development that is causing vulnerabilities. With the integration of this information, the organization can determine the

possible kinds of security attacks on the organization. The security team can investigate whether an attack on these vulnerabilities can create a domino effect that extends beyond the individual applications. This investigation information is useful in the selection of appropriate countermeasures to nullify high-potential vulnerabilities.

6. The entire process of determining ASR allows the organization to identify, remediate and transform only the most significant risk and not those risk factors that have an acceptable level of protection. The act of directing the organization to focus only on lacking systems rather than on all applications results in benefits such as cost savings, time savings, efficient management of applications and better achievement of security resiliency.

CONCLUSION

Application security is a critical risk factor for organizations, as 99 percent of tested applications are vulnerable to attacks.[13, 14] Attacks continue because no standard metric is in practice to measure the risk posed by poor application security. The ASRM provides an accurate assessment of risk for individual applications, each category of applications and the organization as a whole.

Risk assessment has key deliverables, namely identification of potential vulnerabilities that are threats to an organization's mission, compliance attainment and countermeasure effectiveness. Depending on the risk value of applications, a business continuity plan or disaster recovery plan can be created in realistic terms. These two plans are key to driving the organization toward its advancement in the market.

Risk assessment is a continuous process. However, the frequency at which risk assessments should be completed, and for which applications, remain unanswered questions. The prioritization of applications provides a way to establish a frequency of risk assessment. For example, critical category applications can be assessed every six months, important category applications assessed every year and so on. This saves time and provides a systematic way to create a risk assessment schedule, allowing for the intelligent protection of applications against threats. An ASR assessment metric provides a road map for the implementation, evaluation and improvement of information security practices. The risk and vulnerabilities to the organizations keep changing with time. The ASR determination process places the organization in a position to address any new risk and/or vulnerabilities that arise so that application security can be achieved, keeping in mind practical limitations.

ENDNOTES

1 Magel, N.; "The Shape of Cyberthreats to Come: Rodney Joffe Speaks on 2015," Neustar Blog, January 2015, *www.neustar.biz/blog/authors/nikitas-magel*

2 Better, M.; F. Glover; G. Kochenberger; H. Wang; "Simulation Optimization: Applications in Risk Management," *International Journal of Information Technology & Decision Making*, 7(04), 2008, p. 571-587

3 Ingoldsby, T. R.; C. McLellan; *Creating Secure Systems Through Attack Tree Modeling*, Amenaza Technologies Limited, 2003, p. 550, 1000

4 Tipton, H. F.; M. Krause; *Information Security Management Handbook*, CRC Press, USA, 2003

5 Alhazmi, O. H.; Y. K. Malaiya; I. Ray; "Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems," *Computers & Security*, 26(3), 2007, p. 219-228

6 Ponemon Institute, *2014 Cost of Data Breach: Global Analysis*, 2014, *www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis*

7 Godbole, N.; *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, John Wiley & Sons, USA, 2008

8 Niedrite, Laila; R. Strazdina; B. Wangler; Workshops on Business Informatics Research, Springer Science & Business Media, Riga, Latvia, 2012

9 Vaishampayan, Vivek; *PMI-ACP Exam Prep Study Guide*, iUniverse, 2014

10 Sadiq, S.; G. Governatori; K. Namiri; "Modeling Control Objectives for Business Process Compliance," *Business Process Management*, Springer Berlin Heidelberg, 2007, p. 149-164

11 Hammond, L. B.; Summer Conference, The Texas Higher Education Human Resources Association (THEHRA), West Alabama, USA, 2014, *http://txhehra.org/2014/Hammond-HR-Ringmaster.pdf*

12 Smith, C.; D. J. Brooks; *Security Science: The Theory and Practice of Security*, Butterworth-Heinemann, UK, 2012

13 Walker, D.; "Nearly All Apps Vulnerable to Exploit," *SC Magazine*, 8 March 2013, *www.scmagazine.com/nearly-all-apps-vulnerable-to-exploit/article/283635/*

14 Cenzic, Inc., "The Latest Trends Report from Cenzic Reveals 99 Percent of Tested Applications Are Vulnerable to Attacks," PR Newswire, 6 March 2013, *www.prnewswire.com/new-release/the-latest-trends-report-from-cenzic-reveals-99-percent-of-tested-applications-are-vulnerble-to-attacks-195532431.html*

Feature

A Nontraditional Approach to Prioritizing and Justifying Cybersecurity Investments

Robert Putrus, CISM, CFE, CMC, PE, PMP, is an IT professional with 25 years of experience in senior management roles, program management, compliance services, information systems and management of professional service organizations. He is experienced in the deployment of various cybersecurity frameworks and standards. Putrus has written numerous articles and white papers in professional journals, some of which have been translated into several languages. He is quoted in publications, articles and books, including those used in masters of business administration programs in the US. He can be reached at *robertputrus@cox.net.*

Investments in cybersecurity tend to be fairly significant, so organizations continually seek ways to determine whether the investments were appropriate based on return. However, companies are challenged to apply and fit the traditional discounted cash flow methods to calculate a return on investment (ROI) and justify cybersecurity initiatives. Cybersecurity initiatives are even harder to justify than traditional IT initiatives using traditional accounting methods. Some state that cybersecurity initiatives are not investments resulting in profit; instead, they address loss prevention and mitigation of threats to the company's assets. In part, this is accurate. However, in today's world, with the severity of impact resulting from cybersecurity breach incidents, the argument should be supplemented to state that cybersecurity is on the same necessity level as any required infrastructure such as accounting, operations and IT functions to enable companies to do business.

Discounted cash flow methods are unable to quantify the intangible benefits that cybersecurity brings forward to companies. The focus of this article is to propose a nontraditional method to prioritize cybersecurity initiatives and develop a foundation for the return on (cyber)security investment (ROSI) with a method to quantify the intangible returns.

THE CHALLENGE

The perceptions and views of non-IT management toward cybersecurity are among the contributing factors posing the challenge to justify the expense of such initiatives. Examples of such views and perceptions are:

- **Security is not an investment.** Cybersecurity is a risk prevention and mitigation investment. There is no technical guarantee to immunize companies from cyberattacks due to human errors and from those with malicious intent. Traditionally, the view of business management toward IT is that it is an expense and this view has been extended to cybersecurity initiatives.
- **Cybersecurity is an IT discipline.** Cybersecurity is highly technical in content, and technical staffs generally have difficulty explaining to management, in layman's terms, what the proposed initiatives are and how they might protect the core values of the company. Often, management equates cybersecurity with the IT function and responsibility for IT security is exclusive to the IT team. This is a fundamental flaw. Cybersecurity is everyone's responsibility. The IT function must integrate cybersecurity into each of its initiatives. However, all business functions, IT and non-IT, must integrate cybersecurity into their initiatives as well.
- **A communication gap exists.** The communication gap between IT and the business community is a contributing factor in the underestimation and lack of appreciation of each other and the value and sensitivity of the duties and responsibilities of each. Often, the business community lacks a clear understanding of how IT applications, technologies and services may contribute to the company's business objectives in quantifiable and tangible ways. On the other hand, the IT community fails to link technology solutions to the primary interests of the business to increase revenue, expand market share, enhance customer satisfaction and allocate resources. This symptom arises when IT operates in a vacuum and in the absence of IT governance.

THE BIG PICTURE OF ROI

The lack of appreciation and understanding between the business and cybersecurity communities is a two-way street. Cybersecurity staff must be able to understand and accommodate the sensitivity of the business function needs. As a matter of fact, cybersecurity staff members need to reach out to the business community and engage it in the cybersecurity justification of its initiatives. It is worth mentioning that the IT and cybersecurity communities often lack the necessary

understanding of accounting disciplines to enable them to establish a quantifiable basis to advance cybersecurity initiatives and justification.

Is a security investment a business decision or a technology decision? Maybe before this question is answered, it is important to state that cybersecurity investments, in general, are viewed as technology decisions, when they are not. Cybersecurity investments should be looked at as business decisions supporting, protecting and sustaining the company's objectives and competitiveness. The perception of cybersecurity initiatives has to overcome three hurdles:

1. The view that cybersecurity expenses are part of the IT budget and have to be approved through the overall IT budget
2. Consideration of cybersecurity initiatives as equal to other IT initiatives and requiring approval by the company's business management team using the same company internal procedure and guidelines used for IT
3. The inability to quantify the intangibles. A substantial part of the realized benefits from cybersecurity initiatives is intangible. When performing an ROI analysis, it is critical to identify and quantify the intangible risk factors and benefits.

CYBERSECURITY INVESTMENT DECISION MODEL: RATIONALE AND APPROACH

What companies require for cybersecurity investment justification is a creative process to bridge the gap between business and cybersecurity communities, supported by a methodology to quantify the intangible benefits and risk.

The proposed investment justification process is based on examining recommended cybersecurity initiatives and quantifying the impact that such initiatives may have on the established company business objectives.

> "Cybersecurity investments should be looked at as business decisions supporting, protecting and sustaining the company's objectives and competitiveness."

The developed methodology and approach described is based on the analytic hierarchy process (AHP) technique (see sidebar).[1] Through this method, the company will be able to build a cybersecurity decision model (CSDM) that reflects company business objectives, critical success factors (CSFs), business challenges, business enablers and proposed cybersecurity initiatives. Through AHP,

THE ANALYTICAL HIERARCHY PROCESS (AHP): PAIRWISE COMPARISON AND ESTABLISHING PRIORITIES

AHP starts by refining a complex problem into smaller elements. It then organizes the elements into sets of homogeneous clusters, which are subdivided into more detailed sets until the lower levels of the hierarchy are established. This structure represents the total view of the model (e.g., enterprise) being studied.

AHP helps its users deal with complex problems (e.g., cybersecurity initiatives justifications) by representing the enterprise in hierarchical form and identifying the major elements within each level, depending on the level of detail required. The number and type of elements within each level in the hierarchy depend on the enterprise's business environment.

AHP compares any two elements in a given layer and measures the degree of impact on any element in the layer above it. The pairwise comparisons are repeated with every element in each level, starting from the top level and continuing downward to the lowest level of the decision model hierarchy.

AHP helps establish priorities by asking the workshop participants to state the degree of impact of the pairwise comparisons of the element sets in each level in the hierarchy structure with respect to each of the elements in the next higher level.

HOW TO CALCULATE THE PRIORITIES (PAIRWISE COMPARISON)

AHP uses a scale of 1 through 9 in the pairwise comparison to determine the dominance of each element with respect to the elements in the next higher level of every matrix.

CALCULATING RELATIVE WEIGHTS

The criterion weight for this matrix is calculated using a commonly used approximation procedure by taking the geometric mean (average) of the entries in each row.

organizations are able to quantify and compare the degree of impact of the proposed cybersecurity initiatives on any of the company-stated objectives and on any attribute in the CSDM.

Determining the portfolio investment and value of cybersecurity initiatives is highly correlated to company's willingness to articulate the following:

- The risk of potential cost of individual security incidents that the company is willing to bear
- The level of risk that the company is willing to accept when running its business
- The company's recognition that cybersecurity investment ought to be mapped to the company's business objectives, critical success factors and challenges

PLANNING, DESIGNING AND DEVELOPING THE NONTRADITIONAL METHOD IN JUSTIFYING CYBERSECURITY INITIATIVES

The key steps to implementing the process of the nontraditional ROSI are described in f**igure 1**.

Facilitate Management Workshop

Step 2 in **figure 1** is an example of a CSDM that is based on the nontraditional investment decision methodology for ROSI using the AHP technique. The CSDM is constructed through a series of steps in a workshop session using the AHP technique guided by the facilitator. The workshop participant team consists of representatives of company management from key operating departments. The rules of the workshop to construct the CSDM and perform the prioritization (AHP pairwise comparison) are collaboration and consensus building among the workshop participants.

Agree On Collaboration Approach

This is part of the norming process to build consensus and agreement among the management team through a workshop session. The rules of engagement of the workshop and method used should be clearly described by the facilitator and the expected roles and responsibilities accepted by the workshop participants.

Through collaborative efforts, the company expects management to buy in to the business justification of the

Figure 1—Key Steps to Plan and Implement the Process of Nontraditional ROSI

Steps	Description of the Steps	Commitment by the Company
1	Identify cross-functional team members who should participate in the cybersecurity workshop. Note: No advance preparation is required from the team members.	Cross-functional team: Senior management with experience representing departments such as cybersecurity, IT, accounting, operations, human resources (HR) and legal
2	The facilitator presents a walk-through case study of the nontraditional ROSI process and the rules of the AHP technique to the team (workshop participants). This will familiarize and prepare the team for the main workshop and obtain initial acceptance of the methodology.	4-6 hours (time commitment by the selected team)
3	Conduct workshop in a location other than company premises (recommended). The workshop participants will perform the following: • Build the CSDM by identifying and agreeing on the hierarchical layers of CSDM. Company objectives, CSFs, challenges, enablers and proposed cybersecurity initiatives. • Prioritize all elements in each hierarchical layer using the AHP technique.	8-12 hours
4	Facilitator prepares the final report and presentation.	Facilitator time
5	Team members present findings to company stakeholders.	2 hours

Source: Robert Putrus. Reprinted with permission.

cybersecurity investments and rationalize the strategic decisions they are making due to the enterprisewide nature of such decisions.

If the organization decides to implement any of the cybersecurity initiatives, which means it is committed to undertake the investment in funds, resources, schedules, risk tolerance, etc., the organization is required to develop a business case to substantiate the impact of its decision on the entire company through building consensus among management teams and seeking the support of the organization.

Develop the Company CSDM

The investment justification methodology proposed in this article applies to situations in which company competitiveness is examined, critical success factors are defined, and risk and challenges are identified. The objective of the CSDM is to frame the cybersecurity initiatives with justifications in alignment with company business objectives and governance.

The workshop participants will develop the hierarchical decision model, perform impact analysis and identify the portfolio of cybersecurity initiatives to examine, prioritize and implement. AHP is the technique used to facilitate and determine the degree of impacts and priorities of the proposed initiatives.

The beauty of AHP is that the managers of the enterprise can build their own and specific decision models with specific elements and priorities as they see fit for their company at that time.

Figure 2 is an example of a CSDM developed in a workshop setting where participants represent the major departments of the company.

The example illustrated in **figure 2** consists of six hierarchical layers. The number of layers is determined and agreed upon by the workshop participants. The definition of these layers, and all of the elements within each layer, are left to reader interpretation for the sake of simplicity in this article.

The example CSDM layers depicted in this case are:

1. **Goal**—Reducing the severity and likelihood of loss and fraud
2. **Business objectives**—This layer represents the cornerstone of the company establishment. These are the primary business objectives of the company.
3. **Critical success factors**—These are the business processes that are essential to achieve the company's business objectives. These processes have strategic and operational characteristics to achieve the enterprise strategy. The approach in identifying the CSFs is subjective in nature, but the collaborative approach of the workshop participants implies the objectivity needed. It is expected that the workshop participants will spend ample time brainstorming, identifying and agreeing on the processes that are of most importance in achieving the company's business objectives. Finally, the participants will agree on the selected essential CSFs.

Figure 2—Example of Cybersecurity Decision Model for Best Company Inc.

Prioritized Cybersecurity Investment					
(A Method of Return on Security Investment [ROSI])					
The Goal: Reducing the Severity and Likelihood of Loss and Fraud					
Objectives	Support corporate strategy	Secure future business	Reduce security incident costs	Support competitive performance	
Critical Success Factors	Maintain and enhance company image and reputation	Provide competitive advantage	Improve customer relationship	Enhance confidence	
Business Challenges	Loss of reputation	Economic loss	Lack of security costing the business	Lack of security costing productivity	Support strategic investment in it
Business Enablers	Increase risk avoidance	Reduction in compliance and audit costs	Reduction in severity, likelihood and loss cost	Reduction in risk exposure	Reduction in risk mitigation efforts
Proposed Investment Initiatives	Continuous monitoring, threat detection and fraud	Antivirus software	Enterprise security compliance	Behavioral mapping	End-user training/ policies and procedures

Source: Robert Putrus. Reprinted with permission.

4. **Business challenges**—This layer identifies the challenges facing the company. Simultaneously, these are the factors hindering the company from realizing the CSFs and, in turn, preventing the company from achieving its business objectives.
5. **Business enablers**—These enablers are the opportunities the company would like to create in order to contain, mitigate and manage the risk posed by the business challenges.
6. **Proposed investment initiatives**—These initiatives represent a cybersecurity program or projects that enable the attainment of the business enablers. These initiatives could be technical or nontechnical in nature.

At various times, enterprises will have their own model architecture where the number and type of stated layers and their attributes are unique to the strategy of the company as defined by the workshop participants.

In summary, the fundamentals articulated in this ROSI methodology and the development of CSDM are the following:

- Establish the link between cybersecurity initiatives and the enterprise objectives to ensure the buy-in and support of company management.
- Ensure the alignment of the senior management team with cybersecurity. This will elevate the cybersecurity initiatives to be an integral part of company governance.
- Demonstrate that cybersecurity initiatives are protecting the enterprise from the risk of economic, reputation and productivity loss. It is essential to the company's survival.

HOW TO INTERPRET IMPACT VALUES

The AHP technique highlights the degree of influence or the impact the proposed cybersecurity initiatives may have on a given attribute within the hierarchy. **Figure 3** illustrates that the examined investment option, continuous monitoring, threat detection and fraud, have the highest impact on the company goal of reducing severity and likelihood of loss and fraud.

Figures 4, 5 and **6** illustrate the established priorities of the examined and proposed investment initiatives.

Further details of the relative impacts and proprieties are found in **figure 3**.

It is important to mention that the proposed cybersecurity portfolio represents the best picture of the proposed investment to achieve the 100 percent impact for the established goal. If any of the proposed investments have not been undertaken, the company is at risk and the quantified risk is represented by the impact number. It is a company management decision to determine what risk exists and which risk it is willing to accept in the absence of any of the proposed cybersecurity investment initiatives.

The depicted impact (priority) percentages are examples only and are used for illustration of the ROSI methodology and its analysis. Companies will build their own CSDM based on their priorities and the strategy of their business.

CALCULATING THE FINANCIAL IMPACT AND RETURN ON INVESTMENT OF CYBERSECURITY INITIATIVES

After completing the prioritization of the elements of the CSDM, the methodology can be extended to the financial calculation of the cost and savings or cost avoidance of the proposed cybersecurity initiatives.

As demonstrated earlier in the prioritization of the cybersecurity initiatives, continuous monitoring, threat detection and fraud has the highest impact on the stated enterprise goal in the CSDM. The impact of cost and savings of such initiatives on all stated enterprise business objectives in the CSDM will be examined in the following exercise, which details the business objective to reduce security incident costs to illustrate the logic of costs and savings in implementing the continuous monitoring, threat detection and fraud cybersecurity initiative. From here, one must repeat and finish the exercise and apply it to the rest of the enterprise business objectives stated in **figure 7**.

ACHIEVEMENT OF BENEFIT THROUGH THE USE OF THE NONTRADITIONAL JUSTIFICATION OF ROSI

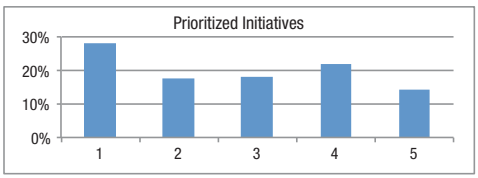
Several benefits and byproducts are expected through the use and performance of the ROSI nontraditional justification methodology, including:

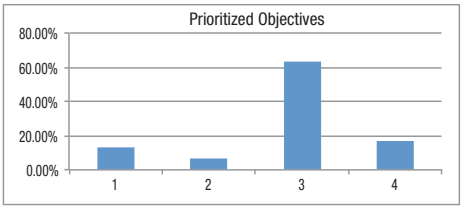
- Establishing a clear and dynamic link among company goals, objectives, risk factors and cybersecurity initiatives
- Elevating cybersecurity planning and implementation to the corporate governance level with easier interpretation for nontechnical and technical personnel
- Providing a communication platform for management team alignment and support
- Developing a company business model that is well understood by the management team and other company entities
- Identifying and prioritizing the interrelated elements where management is able to establish better planning, rationalization and deployment of initiatives

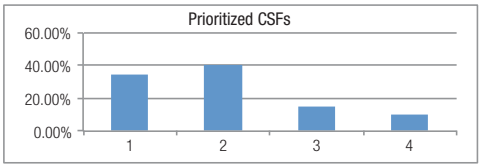
Figure 3—Prioritized Cybersecurity Initiatives

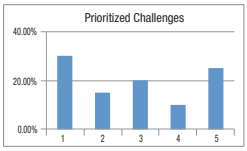
Prioritized Cybersecurity Investment (A Method of Return on Security Investment [ROSI])

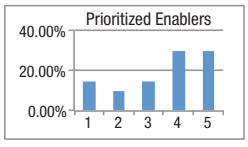
Example of a Cybersecurity Decision Model		The Goal: Reducing Severity and Likelihood of Loss and Fraud					
Continuous monitoring, threat detection and fraud	1	28%					
Antivirus software	2	18%					
Enterprise security compliance	3	18%					
Behavioral mapping	4	22%					
End-user training/policies and procedures	5	14%					
OBJECTIVES **(Prioritized to the Goal)**	Support corporate strategy 13.00%	Secure future business 7.00%	Reduce security incident costs 63.00%	Support competitive performance 17.00%			
Continuous monitoring, threat detection and fraud	30%	25%	30%	20%			
Antivirus	15%	10%	20%	15%			
Enterprise security compliance	10%	25%	20%	15%			
Behavioral mapping	25%	25%	20%	25%			
End-user training/policies and procedures	20%	15%	10%	25%			
CRITICAL SUCCESS FACTORS **[Prioritized to the Goal]**	Maintain and enhance company image and reputation 35.00%	Provide competitive advantage 40.00%	Improve customer relationship 15.00%	Enhance confidence 10.00%			
BUSINESS CHALLENGES **[Prioritized to the Goal]**	Loss of reputation 30.00%	Economic loss 15.00%	Lack of security costing the business 20.00%	Lack of security costing productivity 10.00%	Support strategic investment in it 25.00%		
BUSINESS ENABLERS **[Prioritized to the Goal]**	Increase risk avoidance 15.00%	Reduction in compliance and audit costs 10.00%	Reduction in severity, likelihood and loss cost 15.00%	Reduction in risk exposure 30.00%	Reduction in risk mitigation efforts 30.00%		
PROPOSED INVESTMENT INITIATIVES	Continuous monitoring, threat detection and fraud	Antivirus software	Enterprise security compliance	Behavioral mapping	End-user training/ policies and procedures		

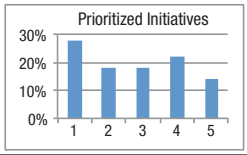












Source: Robert Putrus. Reprinted with permission.

Figure 4—Impact of Cybersecurity Initiatives on the Company Goal

GOAL: Reducing Severity and Likelihood of Loss and Fraud		
Proposed Cybersecurity Initiatives	**Initiative Number**	**Priority in %**
Continuous monitoring, threat detection and fraud	1	28%
Antivirus software	2	18%
Enterprise security compliance	3	18%
Behavioral mapping	4	22%
End-user training, policies and procedures	5	14%

Source: Robert Putrus. Reprinted with permission.

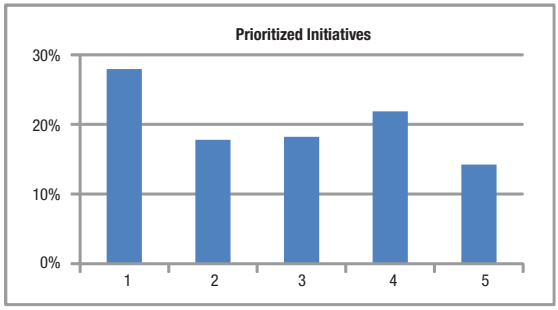


Figure 5—Impact Priority of the Objectives on the Company Goal

GOAL: Reducing Severity and Likelihood of Loss and Fraud		
OBJECTIVES	**Initiative Number**	**Priority in %**
Support Corporate Strategy	1	13%
Secure Future Business	2	7%
Reduce Security Incident Costs	3	63%
Support Competitive Performance	4	17%

Source: Robert Putrus. Reprinted with permission.

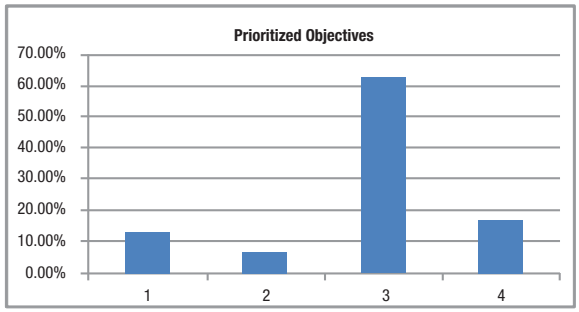
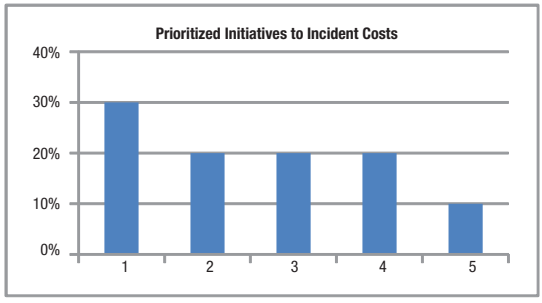


Figure 6—Impact of Cybersecurity Initiatives on the Company Objective

Objective: Reduce Security Incident Costs		
Proposed Cybersecurity Initiatives	**Initiative Number**	**Priority in %**
Continuous monitoring, threat detection and fraud	1	30%
Antivirus software	2	20%
Enterprise security compliance	3	20%
Behavioral mapping	4	20%
End-user training, policies and procedures	5	10%

Source: Robert Putrus. Reprinted with permission.



- Quantifying the impact the proposed initiative might have on each of the company objectives and on the bottom line, the company goal
- Seeking the support of the management team for future departmental initiatives and operational decisions

CONCLUSION

The credibility, accuracy and overall success of a nontraditional ROSI methodology depends greatly on management participation in and support of such initiatives, the experience and discretion of company management participating in the workshop, the acceptance of reaching

Figure 7—Financial Impact and Return on Investment of Cybersecurity Initiatives		
Calculating the Savings/Cost Avoidance From Implementing the Continuous Monitoring, Threat Detection and Fraud Cybersecurity Initiative		
Description	**Assumption**	**Impact**
Investment Cost 1: Continuous Monitoring, Threat Detection and Fraud	-$200,000	
A. Business Objective 1: Reduce Security Incident Costs		63%
Cost of single cybersecurity incident	-$150,000	
Total cost based on number of cybersecurity incidents per year	6	-$900,000
Target reduction in cybersecurity incidents	-30%	
Net impact based on target reduction	[Note: 0.63*(-30%)]	-19%
Savings: Potential savings/cost avoidance based on net impact/year		**$171,000**
B. Business Objective 2: Support Competitive Performance	[Note: Repeat the Exercise for "B"]	17%
Savings: Potential savings/cost avoidance based on net impact/year		**"B"**
C. Business Objective 3: Support Corporate Strategy	[Note: Repeat the Exercise for "C"]	13%
Savings: Potential savings/cost avoidance based on net impact/year		**"C"**
D. Business Objective 4: Secure Future Business	[Note: Repeat the Exercise for "D"]	7%
Savings: Potential Savings/Cost Avoidance Based on Net Impact/Year		**"D"**
TOTAL ANNUAL SAVINGS/Cost Avoidance	**$171,000 + "B" + "C" + "D"**	
Source: Robert Putrus. Reprinted with permission.		

decisions via collaborative efforts in a management workshop forum, and the broad acceptance of the nontraditional ROSI approach. Detailed information is not required to carry out the analysis and conclusion of the ROSI process and justification of cybersecurity initiatives. The approach is a process that can assist company management in performing business analysis and justification based on company objectives and business processes and easily link cybersecurity to enterprise governance. Management can make great use of this process by determining investment opportunity contributions, payback and priority for each one of the business objectives. The outcome of this methodology serves as a guide for investment and allocation of resources such as investment capital and HR. In addition, this proposed methodology helps ensure that management has communicated and developed a consistent understanding of rationale and support to approve and implement cybersecurity initiatives.

REFERENCES

[1] Putrus, R. S.; "The ROI of SOX: Sox Compliance Investments Can Boost Your Bottom Line," *California CPA*, 1 May 2006

[2] Putrus, R. S.; "Outsourcing Analysis and Justification Using AHP," *Information Strategy: The Executive*, vol. 9, no. 1, Fall 1992, p. 31-36

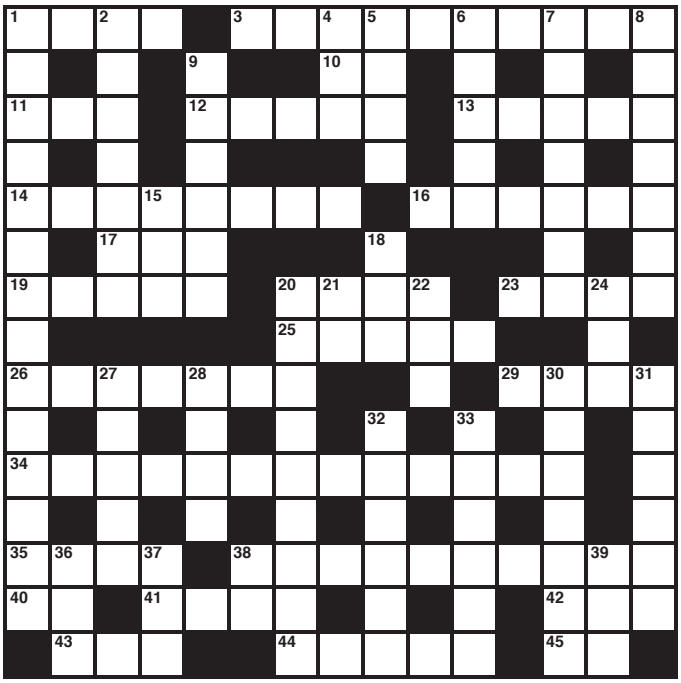
[3] Putrus, R. S.; "Accounting for Intangibles in Integrated Manufacturing," *Information Strategy: The Executive*, vol. 6, no. 4, Summer 1990, p. 25-30

ENDNOTES

[1] Saaty, T. L.; *Decision Making for Leaders*, Wadsworth, USA, 1982. Saaty, T. L.; *The Analytic Hierarchy Process*, McGraw-Hill, USA, 1980

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. Leader in the fight against cyberattacks, abbr.
3. One of the most effective ways to limit the risk of information theft
10. Stored energy, for short
11. A/C capacity meas.
12. Alternative to traditional development methodology
13. They do not justify ends
14. Retrieval of lost data
16. Most important senior executives
17. GPS direction, abbr.
19. Snooped (around)
20. Cab company attempting to change national legislative frameworks to suit their own business model
23. Check copy
25. Popular iterative Agile software development methodology
26. Not knowing about
29. An unusual word for comprehend or get
34. Type of IT auditor who tends to promote conflicts
35. ISACA® certification vital for cybersecurity professionals
38. Claim that cannot be backed up, 2 words
40. Edward, familiarly
41. Look (over)
42. Financial auditor's designation
43. German multinational software enterprise company
44. Model proportion
45. Tantalum symbol

DOWN

1. One form of risk management in relation to data breaches
2. Is the origin point for
4. Army rank, for short
5. Spin
6. Tries to get data out of, for example
7. Behind the eight ball, 3 words
8. Embryonic
9. Set aside
15. Together
18. In accordance with
20. Unique identifiers, 2 words
21. Referring to a period a long time ago, abbr.
22. ___ command
24. Words at the altar
27. Auspices
28. Intentions
30. Simulate, as an event
31. Reviewer of *Data Privacy for the Smart Grid*, A. ____ Kivisild
32. Often repeated word, as in a business philosophy or system of ethics
33. Responsible for
36. Hacker's targets
37. Apple or Android offering
38. Word showing hesitation
39. Luxury resort amenity

(Answers on page 58)

HelpSource Q&A

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

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

Ganapathi Subramaniam is an accomplished professional with 25 years of industry experience, Subramaniam's passion and profession have always been information security. He lives and works in India. As a conference speaker and columnist, he has addressed numerous gatherings of chief information officers and chief information security officers worldwide.

Q My company uses a cloud-based email service provider for corporate email. The same vendor also provides storage space for all the employees to store data. Please let me know the controls that ought to be in place from a security point of view. For obvious reasons, I am not naming the vendor. My company deals with a great deal of sensitive information that we have a legal obligation to protect.

A While there are many advantages of using a cloud service provider (CSP) for handling emails, they come with a few shortcomings. Your company must be cognizant of both these advantages and shortcomings. In most instances, the email service provider is a shared infrastructure environment. Your organization may not get a dedicated infrastructure environment. This shared tenancy arrangement means that access controls must be quite strong. Here are some indicative steps to ensure that the controls are in place to protect your organization's information:

- Integrate the mail authentication credentials with your active directory (assuming that you are using a Windows-based network). Having separate credentials will require users to remember a different password and username for accessing the mail system, an outcome you will wish to avoid.
- Allow access to mail only with at least a two factor-based authentication. For example, they may get a one-time password (OTP) on their mobile device, which will help to ensure that no third party is able to impersonate and access. I am aware of a particular cloud-based email system that sends alerts of suspicious login attempts to the administrators.
- Consider restricting specific users from sending email outside of your company if there is no business need for them to do so. They must be able to send email within the company domain only. While this cannot be made a universal control, this must be implemented for users based on your business needs.
- Consider restricting users from sending emails with attachments.
- For individuals accessing their corporate email using their smartphones, have a mobile device management (MDM) system in place. You need an MDM platform that can work on all types of mobile device operating systems—Windows, Apple and so on. Your tool must have the capability to wipe the data—only your company's data and not any personal data—from the phone of the individual leaving the organization. One of the big challenges is implementing "containers," in which corporate data cannot be comingled and stored alongside personal data.
- Update sender policy framework (SPF) records on your domain name system (DNS) to ensure that only authorized servers are allowed to send emails representing your company's domain. An SPF record is a type of DNS record that identifies the various email servers that are authorized to send email using your company's domain. The key aim of SPF records is to prevent spammers from sending messages forged from addresses belonging to your company.
- Impose device-level restrictions for users handling confidential or sensitive information. This means that only authorized devices can actually connect to your email system irrespective of whether they are connected to your office network or their home network. Some form of media access control (MAC) ID restrictions must be in place to ensure that only company-provided desktops/laptops are used to connect.
- Consider imposing time restrictions in terms of access. If some employees do not need around-the-clock access, then impose time restrictions.
- Ensure ability to implement IP address-based restrictions. This means that certain users must be able to access the email system from your office network only and not from any other location.

Do you have something to say about this article?

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

Go directly to the article:

• Ensure ability to implement information rights management (IRM). IRM controls help to ensure that emails do not get forwarded or copied, rather, they self-delete or disappear after a certain length of time. This will ensure that emails do not get forwarded further to unauthorized recipients.

Many cloud-based email service providers offer simplified versions of their solutions and offer those at lesser prices. In many cases, they dial back security controls. Security controls that ought to be present by default are then made add-on features.

Above all, your company must take a holistic approach to implementing controls aimed at preventing potential data leakages. There is no point in imposing controls on one particular system and keeping all the other holes permanently open.

Enjoying this article?

- Read *Controls and Assurance in the Cloud: Using COBIT 5*.

  www.isaca.org/controls-and-assurance-in-the-cloud

- Learn more about, discuss and collaborate on cloud computing and mobile computing in the Knowledge Center.

  www.isaca.org/knowledgecenter

CPE Quiz

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

Take the quiz online:

QUIZ #165

Based on Volume 6, 2015—The Internet of Things

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

TRUE OR FALSE

HEROLD ARTICLE

1. While the technologies are new, the information security concepts that should be applied are not new; data security concepts that have been used for five to six decades or more can be applied within these gadgets, as can the comparably newer privacy control concepts.
2. Privacy should be viewed as not just a differentiator or something to be done if legally required, but a standard requirement for any new technology or service involving personal data.
3. Location-based controls, which seem to have fallen out of favor as a viable security control in the past couple of decades, could also be used in a limited way to provide security to smart devices.
4. Make sure change controls, access controls and other long-time information security practices are implemented not only within the IoT devices, but also in the rules for using IoT devices for business and within business environments.
5. Encrypt only the wireless data transmissions, but not the data in storage.

ROTMAN ARTICLE

6. IoT raises multiple data privacy and security concerns when new data sources combine with legacy sources to reveal new insights about individuals through predictive analytics that may be inconsistent with the original purposes for collection and use.
7. Although IoT represents a state of change and advancement, a common set of principles can serve as the foundation for companies seeking to understand and manage privacy and security in the development and implementation phases of new connected devices.
8. Combining large data sets can offer powerful knowledge and analysis, but data usage may be inconsistent with the primary purposes of collection.
9. The appropriate or desired state is determined by the organization, with acknowledgement that the highest level of maturity (optimized) may not be suitable for all or even many situations.

IVANOVS AND DERUMA ARTICLE

10. Cybersecurity is a long-term trend in which information assurance, risk approach by design and privacy by default indicate the evolution of information security and give broader understanding of cyberspace.
11. In this case, soft skills for risk managers; auditors; process, information and system owners, including information security managers, are needed to resolve problems more creatively to assure the confidentiality, integrity, availability and accountability of an organization's information assets.
12. A better understanding of cyberecosystem elements, their relationships and main performance drivers makes it possible to plan and develop effective cybersecurity readiness, only with the adequate resources and capabilities of big enterprises.
13. Organizations need to go further; they need to reengineer the behavior, attitudes and knowledge of all stakeholders, including those outside the organization (e.g., customers, suppliers).

MUKHUNDHAN ARTICLE

14. A Poneman Institute study revealed that only 14 percent of companies surveyed said that their executive management does not take part in the incident response process, and "as a consequence of this involvement and awareness, incident managers may not find it difficult to prioritize incident handling and to obtain the resources from business leadership to invest in the skills and technologies necessary to deal with future security incidents," which are expected to increase significantly.
15. The incident manager should be prepared up front with the communication grid, i.e., what information should be communicated to which business stakeholders and during which life cycle stage of the incident.
16. An inappropriate financial gain is not considered a financial impact that requires investigation, analysis and eventually corrective action.
17. The IT manager, depending upon the evolving state of the incident and its containment or eradication success rate, would, in turn, be expected to constantly reassess the impact and respond accordingly.
18. On the other hand, if the network damage is spreading fast and is outpacing the incident response team, the business managers may have to consider other options, such as activating a disaster recovery site, transferring work to a different location or shifting to a manual option.

ISACA® Journal
CPE Quiz
Based on Volume 6, 2015—The Internet of Things

Quiz #165 Answer Form

(Please print or type)

Name _____

_____

Address_____

_____

_____

CISA, CISM, CGEIT or CRISC #_____

Quiz #165

True or False

HEROLD ARTICLE

1._____

2._____

3._____

4._____

5._____

ROTMAN ARTICLE

6._____

7._____

8._____

9._____

IVANOVS AND DERUMA ARTICLE

10._____

11._____

12._____

13._____

MUKHUNDHAN ARTICLE

14._____

15._____

16._____

17._____

18._____

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

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

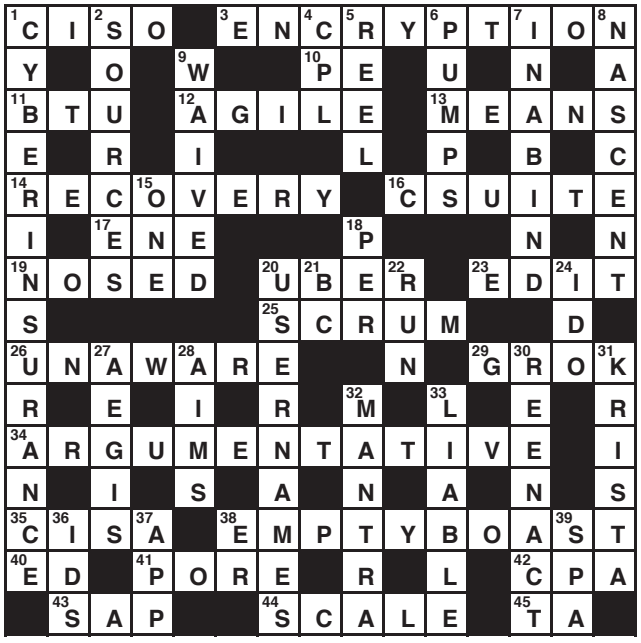
Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

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

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

Answers—Crossword by Myles Mellor

See page 54 for the puzzle.



ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

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

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

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

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

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

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The 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.

IS Audit and Assurance Standards

The titles of issued standards documents are listed as follows:

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

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

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

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

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

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

Reporting
2401 Reporting
2402 Follow-up Activities

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 of Privacy and Assurance Practices via email (*standards@isaca.org*); fax (+1.847.253.1443) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

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

Advertisers/Web Sites

Leaders and Supporters

ISACA® Journal, formerly *Information Systems Control Journal*, is published by 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*.

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

ISSN 1944-1967

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

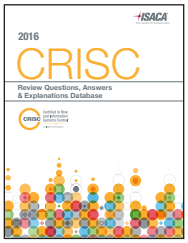
www.isaca.org/bookstore

UPDATED EXAM PREP MATERIALS

BETTER PREPARE FOR THE CRISC™ EXAM WITH ISACA'S CRISC™ CERTIFICATION EXAM PREPARATION MATERIALS

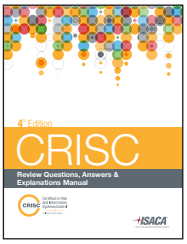
CRISC Review Manual, 6th Edition is an easy-to-navigate reference guide with a format designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The manual has been enhanced and represents the most current, comprehensive, peer-reviewed IT-related business risk management resource.

Member: US $85 | Non-member: US $115 | Product Code: CRR6ED



CRISC Review Questions, Answers & Explanations Database—12-Month Subscription is a comprehensive 500-question pool of items that contains the questions from the *CRISC™ Review Questions, Answers & Explanations Manual, 4th Edition.* The database is available via the web, allowing CRISC candidates to log in at home, at work or anywhere they have Internet connectivity.

Member: US $185 | Non-member: US $225 | Product Code: XMXCR14-12M



CRISC Review Questions, Answers & Explanations Manual, 4th Edition is designed to familiarize candidates with the question types and topics featured in the CRISC exam. These questions are not actual exam items, but are intended to provide CRISC candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam.

Member: US $60 | Non-member: US $80 | Product Code: CRQ4ED

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

Risk Resources

COBIT® 5 for Risk

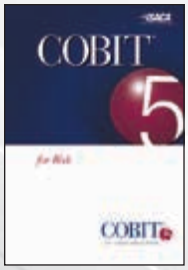
by ISACA

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
- Guidance on 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



Print
Member: US $35.00
Non-member: US $80.00
Product Code: CB5RK

eBook
Member: US $35.00
Non-member: US $75.00
eBook Product Code: WCB5RK

Available in Spanish and Hebrew

Effective Project Management: Traditional, Agile, Extreme, 6th Edition

by Robert K. Wysocki

Many projects fail to deliver on time and within budget, and often-poor project management is to blame. If you're a project manager, the newest edition of this expert and top-selling book will help you avoid the pitfalls and manage projects successfully. Covering the major project management techniques including Traditional (Linear and Incremental), Agile (Iterative and Adaptive), and Extreme, this book lays out a comprehensive overview of all of the best-of-breed project management approaches and tools today.

Print
Member: US $60.00
Non-member: US $70.00
Product Code: 50WPM6

IBM I Security Administration and Compliance

by Carol Woodbury

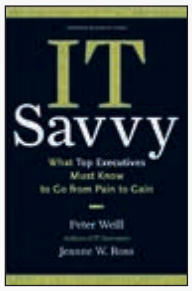
Explaining the importance of developing a security policy and detailing how to implement and maintain such a system, this guide reviews IBM i security and the way it functions within IBM i systems. Written in a clear, jargon-free style, this book covers topics such as system security levels, user profiles, service tools, encryption, auditing, compliance, and incident response. The author's methodology for implementing security is described in great detail, focusing on compliance with stated policies and procedures within an organization. Useful for security and system administrators, security officers, compliance officers, and auditors, the resources available in this book help protect systems from unauthorized activities and unplanned events.

Print
Member: US $50.00
Non-member: US $60.00
Product Code: 4MCSA

IT Savvy: What Top Executives Must Know to Go from Pain to Gain

by Peter Weill and Jeanne W. Ross

Digitization of business interactions and processes is advancing full bore. But in many organizations, returns from IT investments are flatlining, even as technology spending has skyrocketed. These challenges call for new levels of IT savvy: the ability of all managers-IT or non-IT-to transform their company's technology assets into operational efficiencies that boost margins. Companies with IT-savvy managers are 20 percent more profitable than their competitors. In "IT Savvy," Peter Weill and Jeanne Ross—two of the world's foremost authorities on using IT in business—explain how non-IT executives can acquire this savvy. Concise and practical, the book describes the practices, competencies, and leadership skills non-IT managers need to succeed in the digital economy.

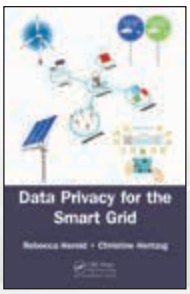


Print
Member: US $23.00
Non-member: US $33.00
Product Code: 5HBS

Data Privacy for the Smart Grid

by Rebecca Herold and Christine Hertzog

Many Smart Grid books include "privacy" in their title, but only touch on privacy, with most of the discussion focusing on cybersecurity. Filling this knowledge gap, *Data Privacy for the Smart Grid* provides a clear description of the Smart Grid ecosystem, presents practical guidance about its privacy risks, and details the actions required to protect data generated by Smart Grid technologies. It addresses privacy in electric, natural gas, and water grids and supplies two different perspectives of the topic—one from a Smart Grid expert and another from a privacy and information security expert.



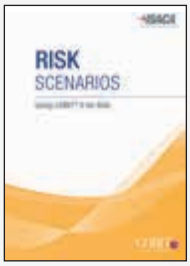
Print
Member: US $70.00
Non-member: US $80.00
Product Code: 64CRC

*Book Review included in this edition of the *Journal*.

Risk Scenarios: Using COBIT® 5 for Risk

by ISACA

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.



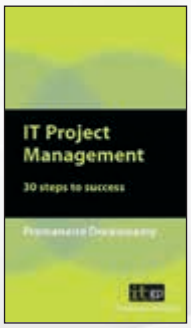
Print
Member: US $35.00
Non-member: US $60.00
Product Code: CB5RS

eBook
Free member download
Non-member: US $60.00
Product Code: WCB5RS

IT Project Management:30 Steps to Success

by Premanand Doraiswamy

Few businesses could function effectively without their IT systems. At the same time, they depend on IT for more than their day-to-day operations. Companies must constantly innovate in order to remain competitive and keep up with ever-changing customer requirements; IT projects deliver these innovations. The IT project manager is the person responsible for implementing the project and realizing the objectives it was designed to achieve



Print
Member: US $15.00
Non-member: US $25.00
Product Code: 12ITPM

Risk Resources

NEW!

A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS)

by ISACA

This book explains the security requirements, processes and technologies that are required to implement the Payment Card Industry Data Security Standard (PCI DSS) which is a compliance requirement for all enterprises that process, store, transmit or access cardholder information for any of the major payment brands, such as American Express®, Discover®, JCB, MasterCard® and VISA® brands.

The guide provides a comprehensive overview of the PCI DSS and explains how to implement its demanding security requirements. The guide also contains a wealth of background information about payment cards and the nature of payment card fraud. The content in this guide goes beyond explaining the requirements by providing the following valued information:

- Concise summaries of the most current PCI DSS requirements Version 3.1 (just released in 2015)
- Consolidated information from numerous PCI Council publications to help the reader better understand the true scope of payment card security
- Techniques to determine the scope of compliance, documenting cardholder data flows and defining the Cardholder Data Environment
- Provides guidance on implementing controls to comply with all 12 PCI DSS requirements and maintain compliance
- PCI DSS requirements mapped to COBIT® 5 processes and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 270012 controls
- Detailed explanation of compliance requirements for third-party services and cloud computing providers

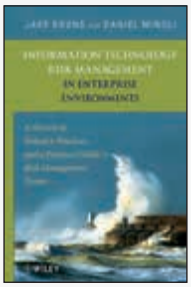
Member: US $35.00
Non-member: US $65.00
Product Code: APG
eBook Product Code: WAPG

Information Technology Risk Management in Enterprise Environments

by Jake Kouns and Daniel Minoli

This book provides a comprehensive review of industry approaches, practices and standards on how to handle the ever-increasing risks to organizations' business-critical assets. Through a practical approach, this book explores key topics that enable readers to uncover and remediate potential infractions. The authors present an effective risk management program by providing:

- An overview of risk assessment, mitigation and management approaches and methodologies
- Processes for developing a repeatable program for technological issues and human resources
- Definitions of key concepts and security standards in the area of risk management
- Analytical techniques for assessing the amount of risk and the benefit of risk remediation
- Information on the development and implementation of a risk management team

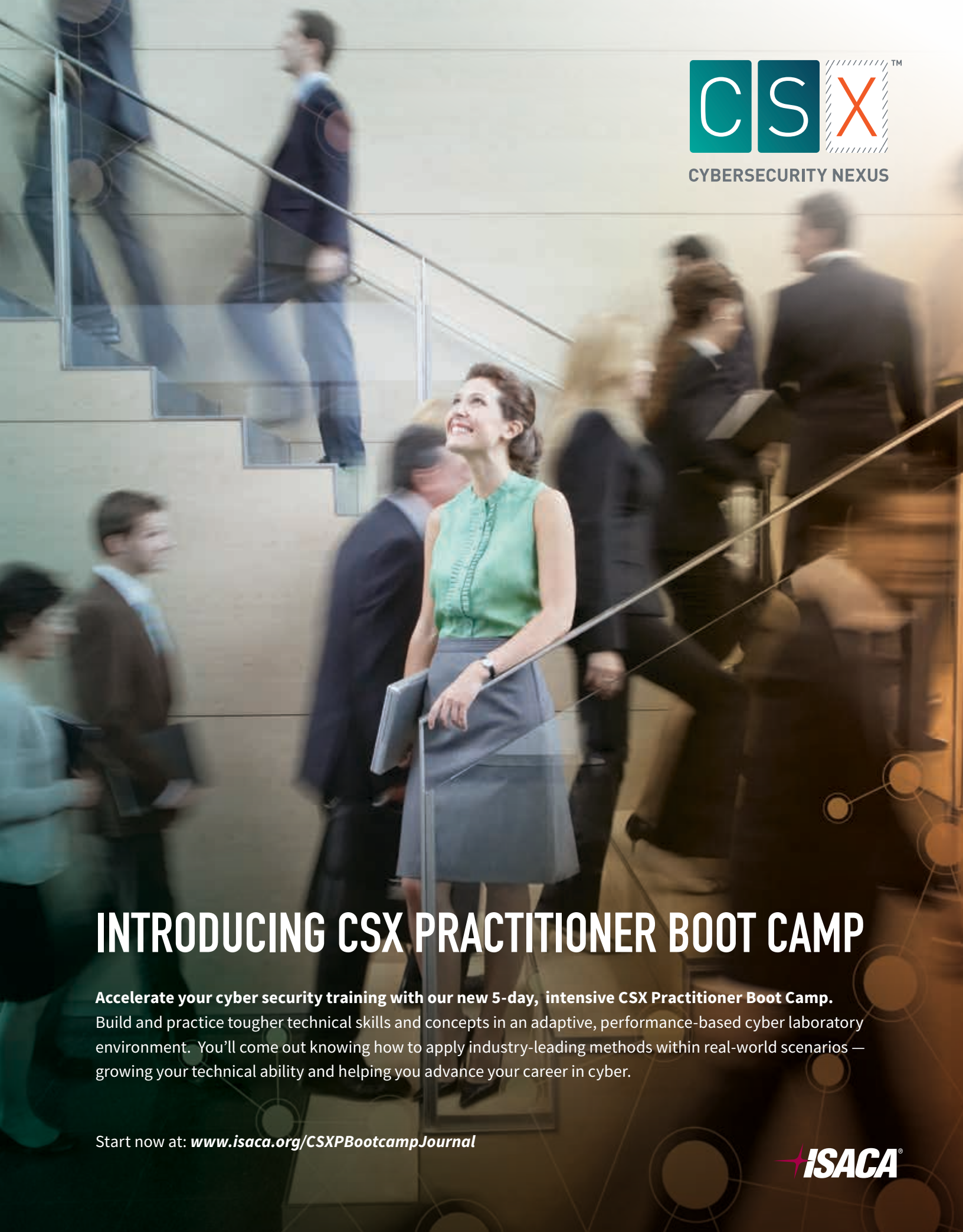


Member: US $104.00
Non-member: US $114.00
Product Code: 84WRM

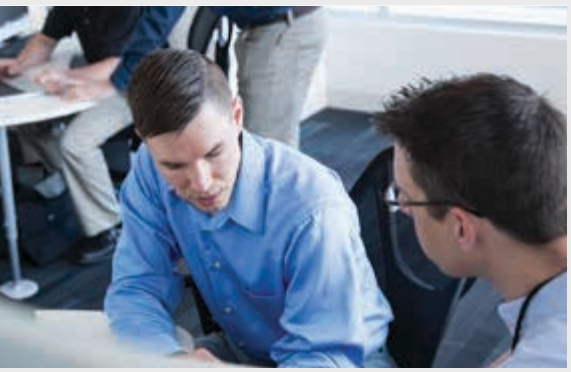
2 EASY WAYS TO ORDER:

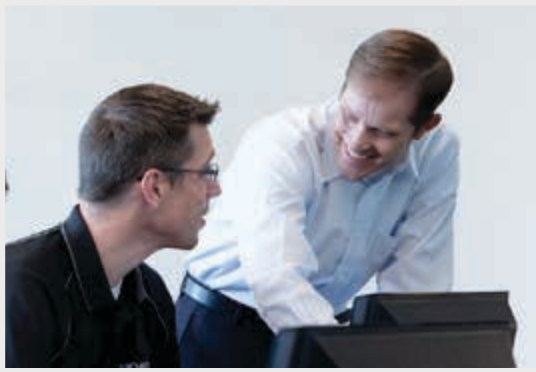
1. Online — Access ISACA's bookstore online anytime 24/7 at ***www.isaca.org/bookstore***

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


CSX™
CYBERSECURITY NEXUS
INTRODUCING CSX PRACTITIONER BOOT CAMP
Accelerate your cyber security training with our new 5-day, intensive CSX Practitioner Boot Camp.
Build and practice tougher technical skills and concepts in an adaptive, performance-based cyber laboratory environment. You'll come out knowing how to apply industry-leading methods within real-world scenarios — growing your technical ability and helping you advance your career in cyber.
Start now at: ***www.isaca.org/CSXPBootcampJournal***
ISACA®

TRAIN LIKE YOU FIGHT





CHIRON'S TEAM OF EXPERT INSTRUCTORS BRING YEARS OF RELEVANT, REAL-WORLD EXPERIENCE INTO THE CLASSROOM.

Chiron's cyber protection program trainees are challenged and tested with real-world scenarios based on today's dynamic, agile and constantly evolving threat environment. Unlike simulated training, Chiron's classes are held in a laboratory setting unrestricted by rigid network security constraints that hamper the hands-on learning experience.

Our customized training approach creates qualified Information Operations professionals that are tested and equipped to handle the real-life cyber threats of today.

- OFFENSIVE AND DEFENSIVE CYBER OPERATIONS
- ADVANCED THREAT SIMULATION
- NETWORK FORENSICS AND THREAT ANALYSIS
- MALWARE REVERSE ENGINEERING
- SIMULATED TRAINING ENVIRONMENT

LEARN MORE ABOUT OUR TRAINING:

410-672-1522, ext. 113 | training@chirontech.com

or visit chirontech.com

CHIRON