Volume 5, 2017

ISACA Journal

ENABLING THE SPEED OF BUSINESS | 05

Design With the End in Mind
Blockchain: Identifying Risk on the Road to Distributed Ledgers
Barriers and Enablers to Auditors Accepting Generalized Audit Software

www.isaca.org

2017 MEMBER GET A MEMBER

RECRUIT NEW MEMBERS TODAY—SHAPE THE FUTURE OF TECHNOLOGY

The more members you recruit, the better reward you enjoy.

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

Recruit 2–3 new members and receive the world's first smart, microwave-to-erase-and-reuse notebook. Download the free app to scan your content and save your notes to your preferred cloud service. Then, microwave to erase it all and reuse! Special pens bundle included. A US $40 value.

Recruit 4–5 new members and receive your own personal home assistant. Search for answers using only your voice. Hands-free streaming to tv and supports multiple users: a US $129 value.

Recruit 6–7 new members and receive the latest gaming system designed to go wherever you do. This device transforms from home console to portable system in a snap: a US $299 value.

Recruit 8–9 new members and receive the newest smart watch with built-in GPS. Water resistant up to 50 meters with a lightning-fast dual-core processor, brighter display and many features to help you stay active, motivated and connected: a US $369 value.

Recruit 10 or more new members and receive a high-quality sound system and enjoy all your music with room-filling sound. WiFi and Bluetooth capabilities: a US $540 value.

THE MORE MEMBERS YOU RECRUIT, THE MORE WE CAN HELP THE BUSINESS AND IS/IT COMMUNITIES IMPACT TECHNOLOGY'S FUTURE.

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

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

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

SAVE
THE DATE... *or*
—REGISTER—
NOW

6th Annual

European Compliance & Ethics Institute

25–28 March 2018 | *Frankfurt, Germany*

- Hear from top compliance & ethics professionals from Europe and around the world
- Learn the latest and best solutions for compliance & ethics challenges, including anti-corruption, data protection, and risk management
- Build your professional network
- Earn the continuing education units you need, and take the Certified Compliance & Ethics Professional - International (CCEP-I)® exam

europeancomplianceethicsinstitute.org | *lizza.catalano@corporatecompliance.org*

ISACA Journal

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 September and October 2017.

The AREM Window
Jeimy J. Cano, Ph.D., CFC, CFE, CMAS

Compliant, Yet Breached
Tony Chandola, CISA, CISM, CISSP, PCI QSA, PCIP, PMP

Rethinking Cybervalue at Risk
Sudhakar Sathiyamurthy, CISA, CRISC, CGEIT, CIPP, ITIL Expert

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

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

Read more from these *Journal* authors...

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

ISACA®
Trust in, and value from, information systems

3701 Algonquin Road,
Suite 1010
Rolling Meadows, Illinois
60008 USA
Telephone
+1.847.660.5505
Fax +1.847.253.1755
www.isaca.org

Information Security in the Multi-Modal Era

Data centers used to be so simple. Big room. Big boxes. People rushing around pushing buttons and hanging tapes. Men were men and dinosaurs roamed the earth. Now it is all gone, including the sexism. In this century, so far, data centers have been dark, forbidding, small rooms—large closets, really—with small machines that have big appetites for power and cooling. And no people at all, at least not where the computers are. And now, even that sort of data center is disappearing.

Where is it going?

The answer is, "Lots of places," including third-party colocation (colo) centers, managed services in vendors' data centers (or their colo sites), and the cloud, where- and whatever that is. At any given moment, organizations are finding that their applications and the data associated with them are running in many different venues, all at the same time. This is the dawn of the multi-modal era; data center staff must adjust or be left behind. And so must security professionals.

Access Control in Multi-modal Environments

There are many causes of the movement away from central, business-owned data centers—technological, economic, sociological and geographic causes. I would rather focus on the effects, specifically, those regarding information security, recoverability and control. As information resources, both data and software, move beyond the confines of the organizations that own them, there is necessarily more potential access to those resources by people other than those employed by the organizations.

Who are those guys?[1]

At the most basic level, they are somebody else's employees. They are "touch labor."[2] They are technicians managing tasks such as backups, patching and general upkeep of customers' IT infrastructure. They are the people who manage a public cloud, which, stripped to its essentials, is nothing but a series of linked data centers operated as a utility. They are security professionals managing firewalls, encryption keys, threat detection and incident response. Some of these categories of people *require* access to their customers' data; others must *never* have that access. The task for an organization's own information security professionals is to recognize the difference and take appropriate measures to control all these external and unknown persons. *Quis custodiet ipsos custodes?* (Who guards the guardians?) must be dealt with at increasing levels of abstraction. Who, indeed, guards the guardians guarding the guardians guarding the…?

Recent history has shown us that physical access to computing equipment can circumvent all logical access controls.[3, 4] For decades, when we said "access control" we meant logical restrictions, with physical access to equipment limited to a relatively few mandarins. The barrier was a locked and monitored door to a data center. That may still be the case in a colo where, if an organization has a locked cage, there is some assurance that only visiting customer employees can get access.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2f1KJ34

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.

Enjoying this article?

- Read *Vendor Management Using COBIT® 5*. *www.isaca.org/vendor-management*
- **Learn more about, discuss and collaborate on information security management in the Knowledge Center.** *www.isaca.org/information-security-management*

If there are only a few racks in a shared row, the lock on the cabinet door is not as reassuring. And even with the locks, many customers engage colo employees to install new devices, withdraw tape backups and perform other activities that require physical presence.

The Outsourcing Challenge

At one level, the challenge of securing data and other electronic resources inside remote physical equipment is simply an extension of the problems of outsourcing, with which some organizations have dealt for years.[5] What is strikingly different today is that organizations are outsourcing different platforms, infrastructures, applications and control functions to different providers all at the same time. At any point in time, an organization may simultaneously have some of its information resources in its own data center, in a colo, at services accessed over the Web and in multiple clouds. In most cases, this was not planned; it developed over the years. And as the upcoming year passes, the mix will change.

Whatever the distribution of systems, it is likely that there will be interactions among the systems. Thus, the challenge for security specialists and operations personnel generally is to develop the capability to see and oversee all of them at the same time. For example, if an organization is experiencing an attack on a system hosted at a colo, it would be important to know if the attack spreads to related systems being hosted in another data center or in a cloud.

> **"One advantage of a multi-modal architecture is that, leaving aside the spread of a virus or worm, enterprisewide downtime is quite unlikely."**

A Cloud of Clouds

Note the use of "a cloud" and not "the cloud" in the previous sentence. Many of us have become so used to dealing with cloud-supported services as a concept that we have lost touch with the reality that an organization may use several of these services. Thus, organizations need a virtual console[6] that can provide simultaneous visibility into all the enterprise's environments. What users view is, for many organizations, not one cloud, but a cloud of clouds, once again raising the meta-level of control. Each cloud needs to be secured individually and as an ensemble.

One advantage of a multi-modal architecture is that, leaving aside the spread of a virus or worm, enterprisewide downtime is quite unlikely. A power outage, for instance, in one servicer's data center is not going to affect the others, all in locations far from one another. On the other hand, many current IT disaster recovery plans anticipate an all-or-nothing outage in a single central data center. Disaster recovery planning is going to have to be rethought for multi-modal environments, an excellent topic for a future article.

Of course, organizations will always have internal data centers, at least as long as employees work on organizational premises. There needs to be one ring that rules them all, with a nod to J. R. R. Tolkein.[7] That would be the data center that connects all the people inside the building with all the systems they use, wherever those systems may be. That data center may be no more than a closet with file servers and network connectivity, but it will be there and it, too, will need the same sort of security as bigger data centers have had in the past and still do today.

As I see it, the future will bring competition among multi-modal service providers (MMSPs). In fact, that is occurring today as some of the larger colo/hosting vendors branch out into cloud-based services. What remains to be seen is when, not if, they realize that security is a strategic differentiator among them.

Endnotes

1 A question made famous in the movie *Butch Cassidy and the Sundance Kid*, USA, 1969, asked by the heroes multiple times with increasing frustration at their inability to evade the long arm of the law
2 A rather inelegant phrase for people doing actual work on computers and storage, using their hands
3 Kushner, D.; "The Real Story of Stuxnet," *Spectrum*, IEEE, 26 February 2013, *http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet*
4 Perlroth, N.; "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times,* 23 October 2012, *www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.* The same delivery method was used for the original Shamoon. It is not clear whether Shamoon 2 was delivered the same way.
5 Tiow, B. L.; "A Security Guide for Acquiring Outsourced Service," SANS Institute, 19 August 2003, *https://www.sans.org/reading-room/whitepapers/services/security-guide-acquiring-outsourced-service-1241*. There is no shortage of literature on this subject and very little has changed over the years. See, for example, this article published in 2003.
6 I am not referring to Nintendo's tool of that name.
7 J. R. R. Tolkien (1892-1973) was an English author, poet and university professor. He is best known as the author of *The Hobbit, The Lord of the Rings* and *The Silmarillion*, among other fantasy novels.

Doing More With Less

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2vlJ7be

The Institute of Internal Auditors (IIA) defines internal auditing as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.[1] However, in many organizations, internal audit is perceived as a (necessary) cost required to ensure compliance with regulations such the US Health Insurance Portability and Accountability Act (HIPAA), the US Sarbanes-Oxley Act of 2002, the European Union Data Protection Directive, or the Payment Card Industry Data Security Standard (PCI DSS). This focus on costs often results in audit staff being kept to a minimum. Even in enterprises with a more progressive view of internal audit, it is often not possible to find people with the right skill set. Nonetheless, the IT auditor is expected to understand innovative technology, understand new regulations and ensure adequate coverage of the audit universe including new applications. So how can IT audit continue to add value? How can we do more with less?

Establish a Data Categorization Scheme

ISACA® defines information security as something that "ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when required (availability)."[2] Therefore, it makes sense (and, indeed, it is commonplace) to categorize the data in accordance with these needs. A short and well-written guide to data categorization is the US Federal Information Processing Standards Publication[3] (FIPS PUB 199) for Security Categorization of Federal Information and Information Systems. A sample data categorization scheme is shown in **figure 1**.

Categorize the Applications

The next step is to categorize the applications based upon the data they process. In effect, one wants to confirm whether each system processes data that are confidential or subject to integrity or availability rules. The best way to do this is to devise a questionnaire and ask the business owner of each application. These questions should be relevant to the enterprise. Sample questions are shown in **figure 2**.

Respondents should be advised that for every question to which they answer "yes," they should indicate the degree of impact: high, medium or low. These ratings, in turn, should be given a numerical weighting. The overall score can then be used to rate the applications (**figure 3**). Again, the scores should be set based upon the needs of the enterprise and the number of questions.

At the end of the process, one should have a list of all the enterprise's applications, each of which is rated as high, medium or low for confidentiality, integrity and availability. These ratings should be

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees and is a current member of ISACA's CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke assisted in the updates of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for ISACA's CISA Online Review Course. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email at Ian_J_Cooke@hotmail.com, Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed in this column are his own and do not necessarily represent the views of An Post.

Figure 1—Sample Data Categorization Scheme

Security Objective	Level 1	Level 2	Level 3
Confidentiality	Loss of access restrictions or unauthorized disclosure would have a **high** impact on enterprise goals.	Loss of access restrictions or unauthorized disclosure would have a **medium** impact on enterprise goals.	Loss of access restrictions or unauthorized disclosure would have a **low** impact on enterprise goals.
Integrity	Improper information modification or destruction would have a **high** impact on enterprise goals.	Improper information modification or destruction would have a **medium** impact on enterprise goals.	Improper information modification or destruction would have a **low** impact on enterprise goals.
Availability	Loss of timely and reliable access would have a **high** impact on enterprise goals.	Loss of timely and reliable access would have a **medium** impact on enterprise goals.	Loss of timely and reliable access would have a **low** impact on enterprise goals.

Figure 2—Sample Questions

Confidentiality—Would unauthorized disclosure…	• affect health and safety? • have a monetary impact (e.g., intellectual property)? • have a reputational impact (e.g., personally identifiable information [PII])? • have a legal/regulatory impact (e.g., PCI DSS)?
Integrity—Would unauthorized modification or destruction…	• affect critical business decisions? • affect health and safety? • have a monetary impact? • have a reputational impact? • have a legal/regulatory impact?
Availability—Would nonavailability…	• have a reputational impact? • affect health and safety? • have a monetary impact? • have a legal/regulatory impact?

used to decide on the controls to be applied. The higher the application rating, the more important the controls are to the enterprise. Therefore, it makes sense to spend more time protecting or, indeed, auditing these applications than the lower-rated ones. Further, the rating will dictate the type of controls. For example, a higher-rated confidentiality application may require that encryption is employed while a higher-rated availability application may require clustering or some sort of failover. It is, of course, possible that an application may be rated high across all three categories.

Figure 3—Sample Scoring Scheme

Security Objective	Level 1—High	Level 2—Medium	Level 3—Low
Confidentiality	45-60	30-45	30 or less
Integrity	45-60	30-45	30 or less
Availability	45-60	30-45	30 or less

Enjoying this article?

- **Learn more about, discuss and collaborate on audit tools and techniques in the Knowledge Center.** *www.isaca.org/it-audit-tools-and-techniques*

Establish the Criteria

The concept of criteria was discussed in my previous column.[4] To recap, "criteria" is defined as the standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter.[5] An IT auditor will add more value if the criteria used are the same as those already established by the enterprise. If such standards, including a document defining the required baseline controls for all applications—an "application standard," have not yet been defined, it is highly advisable to audit the second line[6] functions responsible and require that they are set as soon as possible. This document should be agreed to by the first-line functions and subsequently reviewed by internal audit.

As well as adding more value, auditing to the same defined standards will also result in a lot less friction with auditees and should avoid the age-old argument of "We do not apply that standard here." Further, if the auditees are aware of the standard, they are much more likely to be compliant with it.

Perform a Control Self-Assessment Based Upon the Criteria

ISACA defines control self-assessment (CSA) as an assessment of controls made by the staff of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable.[7]

Since the enterprise now has a defined application standard and is looking to increase the assurance provided by internal audit, it makes good sense to build a CSA questionnaire based upon the standard.

The CSA should require the auditee to answer questions on the application standard, providing a percentage score for each answer (the higher the score, the more satisfied the respondent is with the control in question). Further, each question should be flagged as baseline (i.e., all applications require this) or related to confidentiality, integrity or availability.

This should result in a list of applications with percentage scores for each of the security areas (**figure 4**).

Audit the Gap

The resultant gap between a perfect score (100 percent) and the actual score may be small in numerical terms, but could represent a significant risk to the enterprise. For example, Application C may have been categorized as high for confidentiality, and 22 percent does not appear to be an overly large deficiency, but it could represent failures in important controls such as the use of a deprecated encryption protocol. It is, therefore, important that this gap is assessed. This could be

Figure 4—Sample Application Standard Scores

Application	Overall	Confidentiality	Integrity	Availability
Application A	93%	96%	95%	83%
Application B	87%	80%	84%	98%
Application C	84%	78%	85%	94%

done by internal audit performing a short, sharp, focused audit on the control(s) in the question. Recommendations (if any) should then be made and followed up[8] on in the normal way. Confirmed implementation of these recommendations should, of course, result in an increased score the next time the application goes through the CSA process.

Report to the Audit Committee

When several applications have gone through the CSA process, it would be good practice to report the CSA results to the audit committee. This provides transparency and allows the IT auditor to give an opinion on the overall control environment. Further, as the CSA is repeated, applications' scores can be tracked, showing improved scores as controls are implemented and risk mitigated or a decrease in scores as emerging risk arises.

Audit a Percentage of the Applications Annually

There is always a risk with a CSA that results are inaccurate or that, over time, the auditees become a little complacent. This can result in CSA results that are not reliable. To counterbalance this, I recommend performing a full audit on a defined percentage of the applications on an annual basis. This should help to keep the CSA honest.

Conclusion

Categorizing applications by confidentiality, integrity and availability allows an IT auditor to ensure that limited resources are directed at the right risk factors at the right time. Further, performing CSAs to agreed-on criteria increases assurance coverage and helps ensure that all three lines of defense are pulling in the same direction. Finally, reporting the results to the audit committee increases transparency and allows an IT auditor to give an opinion on the overall control environment. Together, these items add real value to the enterprise.

Author's Note

The author wishes to acknowledge Frank Ennis and Paul Rochford, CISA, CRISC, CISSP, CISSP-ISSAP, of An Post for their contribution to many of the concepts used in this article.

> **"When several applications have gone through the CSA process, it would be good practice to report the CSA results to the audit committee."**

Endnotes

1 The Institute of Internal Auditors, About Internal Auditing, *https://global.theiia.org/about/about-internal-auditing/pages/about-internal-auditing.aspx*
2 ISACA®, *COBIT® 5 for Information Security*, USA, 2012, p.19, *www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx*
3 National Institute of Standards and Technology Computer Security Division, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199, USA, February 2004, *http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf*
4 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *www.isaca.org/Journal/archives/Pages/default.aspx*
5 ISACA, Information Technology Assurance Framework (ITAF), *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx*
6 Chartered Institute of Internal Auditors, Governance of Risk: Three lines of Defence, *https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/*
7 ISACA, *CISA® Review Manual 26th Edition*, USA, 2016
8 Cooke, I.; "Enhancing the Audit Follow-up Process Using COBIT 5," *ISACA Journal*, vol. 6, 2016, *www.isaca.org/Journal/archives/Pages/default.aspx*

Justine Bone
Is an information technology and security executive with a technical background in software security, risk management, information security governance and identity management. She has spent more than 15 years working in the private sector for financial, news and information security companies, plus several years serving the intelligence community. Over the past few years, she has been instrumental in evolving information security governance and strategy within the private sector. She has led MedSec as chief executive officer (CEO), served as the global chief information security officer at Dow Jones and acted as the global head of risk management at Bloomberg L.P. She was also CEO of boutique security research firm Immunity Inc., and founded an independent private intelligence service serving select US federal agencies.

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

A: We are really seeing diversification when it comes to the role of a cyber security professional. From the security operations center (SOC) to the engineering floor, from the dark web to the financial markets, these days we need folks who are not just fluent in cyber, but who have additional skills, capabilities or certifications.

I have a pet peeve: references to "soft skills." But I think we all recognize the need to go beyond purely technical capabilities. A colleague of mine recently said, "It's not soft skills, it's extrapolation in a higher form." I could not have said it better.

Additionally, most of us are happy to see cyber security getting the attention it needs from the boardroom on down. Again, communication skills are essential here. The job of the chief information security officer (CISO) is not just to present information, but also to persuade other decision makers about the best course of action.

Q: What leadership skills do you feel are critical for a woman to be successful in the field of cyber security?

A: Adaptability and a desire to continue learning are key. We need to be able to recognize shifts in policy, culture and business, and then understand the emerging technologies that might support those shifts. But that is a skill critical for any leader in cyber security. For women—I'll be honest—it is still pretty rough out there. As minorities, we are under heightened scrutiny and often need to address preconceptions by exceeding the standards applied to others. If you are pushing new ideas, this gets especially challenging because you are often doing so alone. So, being comfortable alone, being able to trust one's instinct and remaining confident in the face of adversity are some of the skills I rely on.

Q: What is the best way for someone to develop those skills?

A: With regard to confidence, it starts by understanding the problem. I have yet to meet an over-confident women in technology, so let's make a safe assumption that there is or will be a problem related to lack of confidence for most of us. *The Confidence Code*, by Katty Kay and Claire Shipman, is a book that helped me understand why this can be such a struggle. It discusses how some kids (typically boys) are encouraged to take risks, as opposed to other kids (typically girls) who are rewarded for following the rules. This serves girls well as young children in school systems, until a certain point. But, eventually, the risk takers, who have been taught that it is okay to fail, go out into the world taking

risks with confidence. Understanding this has helped me relieve stress and make tough decisions.

Q: What advice do you have for information security professionals as they plan their career paths and look at the future of information security?

A: Think about a future where cyber security is a more generalized concept. As an expert, you might pick a technical path such as vulnerability researcher, forensic investigator or engineer, but also, you could be a lawyer specializing in cyber security, a policy expert or an educator. At some point, most folks need to make a decision about how technical they want to be—and I do believe that for most people, that is a choice. I believe anyone can understand the technology just as anyone can understand math. It is a function of communication—good teaching—and the way the information is presented to successfully learn the subject.

Q: What do you think are the most effective ways to address the cyber security skills gap and, especially, the lack of women in the cyber security workspace?

A: I would really like to focus on diversity as an opportunity as opposed to focusing on women (and the lack thereof) as a problem. We have real numbers now around increased company and economic performance with increased diversity, and I would like to see more research around that.

On a more personal front, I believe I can be most effective in leading by example. I feel a responsibility to work hard and fight the tough battles to make this a more accessible career for others who may not have that same appetite for challenge! We need those people, too—we do not all have to be pioneers out there breaking new ground.

Q: You took an unconventional road to the career field you have now, having started out as a dancer with the Royal New Zealand Ballet company. How did you arrive at a career in information security?

A: I do not really arrive somewhere, as much as plan my destination in advance! I had always been interested in computers and loved math. I also have a few traits that have driven me along the way, such as unrelenting ambition and the self-discipline to see plans through. I come from a family of planners. We plan everything to such an extent that we arguably live in the future. So, I always knew that after ballet I would try something more scientific as a disruptive and ambitious change.

I like to always be learning. I also like to change my environment frequently via travel, which is how I ended up living on the other side of the world from my family, and why we are always planning our next family rendezvous.

1 What is the biggest security challenge that will be faced in 2018?

Holding technology vendors and manufacturers accountable for low-quality product.

2 What are your three goals for 2018?

Help hospitals, travel more and improve at managing stress.

3 What are your favorite blogs?

Twitter and *The Wall Street Journal*.

4 What is on your desk right now?

My headphones, two laptops, my phone and dumbbells. I try to work out quietly when I am on long conference calls!

5 Who are you following on Twitter?

I have started following investors and others in the financial sector. We have a lot to learn from that crowd.

6 What is your number-one piece of advice for other information security professionals, especially women?

Being a minority is an opportunity. Yes, we often have to over-deliver to achieve similar outcomes to others, but as a result, we know our material inside out. In addition, many of us can rely on a multitude of skills—including communications skills—that others may not have.

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

Typically, I am either working or spending time with my kids, so I try to blend in things I enjoy with both. I love experiencing new cultures and places and, luckily, get to blend that with my work. When with the kids, music and the outdoors are high on the priority list. I am also beginning to work on a book. I have not done enough yet to determine whether or not that qualifies as work!

Train Your Employees. Prep for Enterprise Success.

Competition, regulation, evolving technology—change is constant. As a global leader in training, education and certification for information systems and business professionals, ISACA® can provide enterprise employees with the knowledge and skills to take on the challenges and build on the opportunities of an ever-changing world. Our Enterprise Training and Continuing Professional Education (CPE) programs are:

- Customizable to your specific needs.
- Available at or near your location, reducing downtime and travel.
- Taught by expert trainers with real-world experience.

Learn more about ISACA Enterprise Training at: **www.isaca.org/enterprisetraining**

ISACA®

IS/IT AUDIT | RISK MANAGEMENT | COBIT/GOVERNANCE | CYBER SECURITY | INFORMATION SECURITY

Blind Spots on the Cloud Platform

Recently, an article in *The Wall Street Journal* revealed that IT outsourcing companies in India had reduced the number of H1B (worker) visa applications made to the authorities in the United States even before President Trump voiced his concerns about the negative impact of such visas on the US labor market.[1] Looked at from a high level, this should not be a surprise. On-site provision of expertise by the service providers was replaced by offshore locations. Now, much of the offshore IT service has moved to the cloud. Cheaper, better, more efficient are the drivers of computing services metrics today.

The reduction in H1B visa applications goes to the fundamental nature of shifts in computing, which rest upon physical and logical views of the system. A single physical view can support multiple logical views. Leveraging this idea, the first move was from data files to databases; next was a transition from one's own physical assets to the shared physical resources of the service provider to support logical views of the acquirer of services. Moving to the cloud would mean not having to worry as much about the physical view and instead focusing on logical views, the real value of information processing. Of course, this decoupling of physical from logical is a key factor in the launch of cloud computing.

Cloud services have grown dramatically in the recent past and continue to increase in popularity. Between 2015 and 2020, cloud computing is predicted to achieve an annual growth rate of 19 percent.[2] Cloud implies sharing, which means potential efficiency because a shared resource can be optimized across many clients. On the provider side, sharing means scaling to meet the needs of increasing numbers of customers to move more data and applications to the cloud. The unprecedented growth of this idea is vividly expressed in Amazon's magical rise in the cloud services market—no wonder its stock price crossed the US $1,000 mark recently!

> **"Cloud implies sharing, which means potential efficiency because a shared resource can be optimized across many clients."**

Interestingly, the idea of not having to own infrastructure and instead relying on a centralized resource (as in the cloud) or a decentralized resource (as in ride-hailing or Airbnb) has great appeal for innovation and growth while dramatically containing costs. Google's current experiment with Waze, a community-based traffic and navigation app in the San Francisco Bay (USA) area, has to do with

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2vfA1fh

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. He can be reached at vraval@creighton.edu.

Don Lux, MSITM
Is a MTS 1, software engineer at PayPal and a doctoral student at Creighton University. He has nearly two decades of experience in IT in various roles as a programmer, automated tester, release engineer, release manager and support engineer. He can be reached at donlux@creighton.edu.

sharing without owning: If person A is going to the same place where person B is driving today, why not connect on Waze and plan for a ride share? In another 10 years, it may be that driverless cars combined with ride-hailing platforms result in not having to own a car or have a garage in the home.

This exciting development in cloud services comes with new or additional risk. To quote an *ISACA® Journal* article, "The benefits of cloud computing are tempered by the extreme potential to introduce uncontrolled or unforeseen risks and threats to an organization's information."[3] If there is one third-party risk management instance that the IT auditor should thoroughly examine, it would be the cloud services provider(s) (CSP). When an enterprise is living in the cloud, it is beholden to a third party that can make decisions about its data and platform in ways never seen before in computing.[4]

Blind Spots

Whereas it would be difficult, if not impossible, to identify every blind spot on the cloud platform, there are a few categories that illustrate the fact that, indeed, such blind spots exist, and one needs to look for them so they can be addressed to mitigate any hidden risk behind them.

Four main sources of blind spots are:

- Interoperability between the cloud and in-house systems
- Task allocation between the provider and the acquirer
- A new definition of users
- In some areas of the cloud, the collaborative nature of work

The ability of computer systems to exchange information, or interoperability, in cloud ecosystems is becoming more critical given that part of the organization's system now resides elsewhere, with the CSP. And yet, the logical flows of data and user interactions have to be supported as if the system has never been split. By the very nature of the arrangement, interoperability is assumed in cloud services. However, many users may not even be aware if their work is happening in the cloud or on their (local) system. Depending on the scale and complexity of outsourcing, managing interoperability can be a major challenge, even when due care is exercised in the selection of the CSP. Often, confusion arises from lack of knowledge about the application, such as whether the version in use is cloud independent (e.g., Office 2010), cloud supported (e.g., Office 2013) or cloud integrated (e.g., Office 2016).

A related point is that, in essence, there are now two custodians of the whole (system), and an exhaustive tracking of who does what is difficult, especially if this is likely to change dynamically. The destiny of the acquirer is deeply connected with events unfolding in the provider space. For example, when the provider is hacked, the organization's sensitive information is at risk no matter how stringent the organization's security. The sole reliance on service level agreements (SLAs) is impractical as there are numerous minute details that need to be identified and incorporated in the task allocation. It may even be necessary for the acquirer to have the provider commit to compliance with key policies of the client and an audit of critical areas by the client. Missing or poor handling of a

task on either side can have grave consequences; therefore, it is important to know who is responsible for the task.

In the past, end users were all within the company and were subject to strict protocols and requirements. Not everyone was an end user, and tasks of managing the information-processing value chain belonged to the few. No more. In some ways, the split between physical and logical views empowers the organization to do more with information to create wealth. The traditional definition of end users is now expanded to include practically everyone using the information, creating new data or running applications from their devices. This vast expansion of the user universe is different in its culture. End users have come to expect that they can begin working on a task at the office, then pick it back up from home later in the evening without any noticeable difference between the two. They want to work with systems (anywhere, anytime, from any device), while often having little awareness or understanding of relevant risk exposures. They may not know where they are saving their documents, for example, or how safe these documents are.

Finally, because the cloud facilitates sharing, collaborative work has flourished on cloud platforms. When two or more users jointly share in the duties of a project or a task, the best protective shield that exists is represented by the weakest link in the chain. This creates uncertainty about what the exposures might be. Even tech-savvy people sometimes are not fully informed about risk and may or may not consider paying attention to it as important. A collaborative group is often focused on the core outcome of the project and may not see beyond the central project requirements.

Protection/Mitigation

Interoperability implies many communication channels and frequent access to data and systems across the boundary of the cloud. Access authorization, encryption of stored data and data in transit, and role-based user privileges—these are some of the common means of securing the client-provider communication. As to the applications supported by either side—provider or acquirer—a rigorous change-control process oriented toward the cloud environment must be followed. Recently, the change control process has received increasing scrutiny from auditors. The level and quantity of information required to make even simple changes have multiplied following this scrutiny. And documenting even a simple change could take as much as 30 minutes now compared to less than a minute a few years ago.

In defining acquirer-provider accountabilities, a periodic audit of the SLA and related documents may suggest vulnerabilities arising from vague language, implicit understandings or undocumented promises. Without review of how the two partners come together on critical tasks, it is difficult to modify existing commitments and, thus, improve expectations.

In a systems environment where the cloud presence is significant, it is necessary not only to require end users to successfully complete appropriate training, but also to do so regularly for most training, including updates. While this is a soft area because of the human element involved, it potentially offers the best hope for any kind of prevention of mishaps or incidents. Even a blog of what went wrong and how it was addressed could help users understand the gravity of the task and how seemingly trivial things trip up normal conduct. The case for end-user training cannot be overstated. For example,

Enjoying this article?

- Read ***Controls and Assurance in the Cloud: Using COBIT® 5.*** *www.isaca.org/cloud*

> **“The traditional definition of end users is now expanded to include practically everyone using the information, creating new data or running applications from their devices.”**

in the Bangladesh Federal Reserve Bank case, approximately US $90 million was stolen by hackers; the reason was that while the SWIFT[5] system appeared quite secure, the environment in which it was operating in Bangladesh caused vulnerabilities.[6] The system stayed logged on even after hours, clearly a user oversight, making it feasible for the hackers to exploit the bank.

In instances of collaborative work, it is important to strengthen the weakest link in the chain. This can be done by requiring rigorous training and having the group discuss exposures and vulnerabilities—or, simply, what could go wrong and how to avoid it. This soft approach should be supported by appropriate software, hardware and communication controls to create defense-in-depth for the collaborative environment.

“In instances of collaborative work, it is important to strengthen the weakest link in the chain.”

In sum, (public) clouds split the system tasks across independent organizations. The risk, therefore, nearly doubles, as if the two decision-making groups were acting in unison as a single entity. A tsunami at the provider location is also, for all practical purposes, a major disaster for the acquirer. Any outage at the Amazon cloud could mean outages for its customers, such as Netflix, which, in turn, would impact millions of Netflix customers. The weaker of the two entities will likely generate more worries about security risk. Confidentiality, integrity and availability objectives in the cloud environment are the products of joint efforts, with the requirements often specified by the acquirer of cloud services. In this joint effort, all providers matter. A February 2017 survey conducted by Intel Security reached the following recommendation: Organizations should look for specialty security solutions that provide an equivalent control layer across all providers.[7] The identification and mitigation of blind spots across all cloud platforms in use is a critical step for the reliable and sustainable existence of both the provider and the acquirer of cloud services.

Endnotes

1 Meckler, L.; N. Purnell; “Use of H1B Visas Fell Before Donald Trump’s Critiques of Program,” *The Wall Street Journal,* 5 June 2017, *www.wsj.com/articles/use-of-h1b-visas-fell-before-donald-trumps-critiques-of-program-1496682157*

2 Columbus, L.: “Roundup of Cloud Computing Forcasts, 2017,” *Forbes*, 29 April 2017, *www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#29787c3131e8*

3 Cadregari, C.; “Every Silver Cloud Has a Dark Lining,” *ISACA® Journal*, vol. 3, 2011, *www.isaca.org/Journal*

4 Trapani, G.; “The Hidden Risks of Cloud Computing,” Lifehacker blog, 29 July 2009, *http://lifehacker.com/5325169/the-hidden-risks-of-cloud-computing*

5 SWIFT, *https://www.swift.com/*

6 Burne, K.; R. Sidel; “Hackers Ran Through Holes in SWIFT’s Network,” *The Wall Street Journal*, 30 April 2017, *www.wsj.com/articles/hackers-ran-through-holes-in-swifts-network-1493575442*

7 Greengard, S.; “Why Cloud Security Is Still a Concern,” Baseline, 3 March 2017, *www.baselinemag.com/cloud-computing/slideshows/why-cloud-security-is-still-a-concern.html*

Design With the End in Mind

Innovations in the marketplace have accelerated sharply, and the implications have tremendous impact on the business environment. Needless to say, organizations are evolving in scale and geographical outreach that have not been witnessed before. Transforming business frontiers have created an expanding digital universe and explosive data growth, making organizations reservoirs and refineries of data. An analysis by the International Data Corporation (IDC) estimated that by 2020, the digital universe will contain nearly as many digital bits as there are stars in the physical universe.[1] Put another way, data are doubling in size every two years and, by 2020, the digital universe is expected to grow exponentially, reaching 44 zettabytes. In all likelihood, this trend will continue and intensify in magnitude. It is widely argued that new economies based on data as a form of capital, and the most coveted strategic asset, will emerge. Data such as personally identifiable information (PII), trade secrets and intellectual property (IP) free flow across organizations, reflecting lowered barriers to data movements and a decline in what consumers refer to as a "privacy friendly" environment. A typical data life cycle and possible interactions with different supply chain relationships are depicted in **figure 1**.

The fading organizational boundaries, along with increasing appreciation of cloud-based networks, big data, persistent online lifestyle, and comingling of social and business data, create potentially far-reaching privacy and data protection implications. Covert attacks and information theft by perpetrators and criminal cartels are redefining present-day norms. In many respects, the organizational digital doctrine emulates the natural history metaphor, "the struggle for privacy and survival of the secured,"[2] which is why data are both an asset and a liability.

The fragmented approaches and pointed solutions that organizations routinely accept to manage their operations and the underpinning data transactions have fallen short of addressing the consumer's right to privacy. At the same time, the silo approach to privacy has prevailed for far too long without benefit, and organizations are overdue for a paradigm shift to an enterprisewide pursuit to privacy. The enterprisewide pursuit embarks on integrating privacy and protection safeguards into products/systems/services from the earliest stages of design through the privacy-by-design paradigm.

What to Expect of Privacy by Design

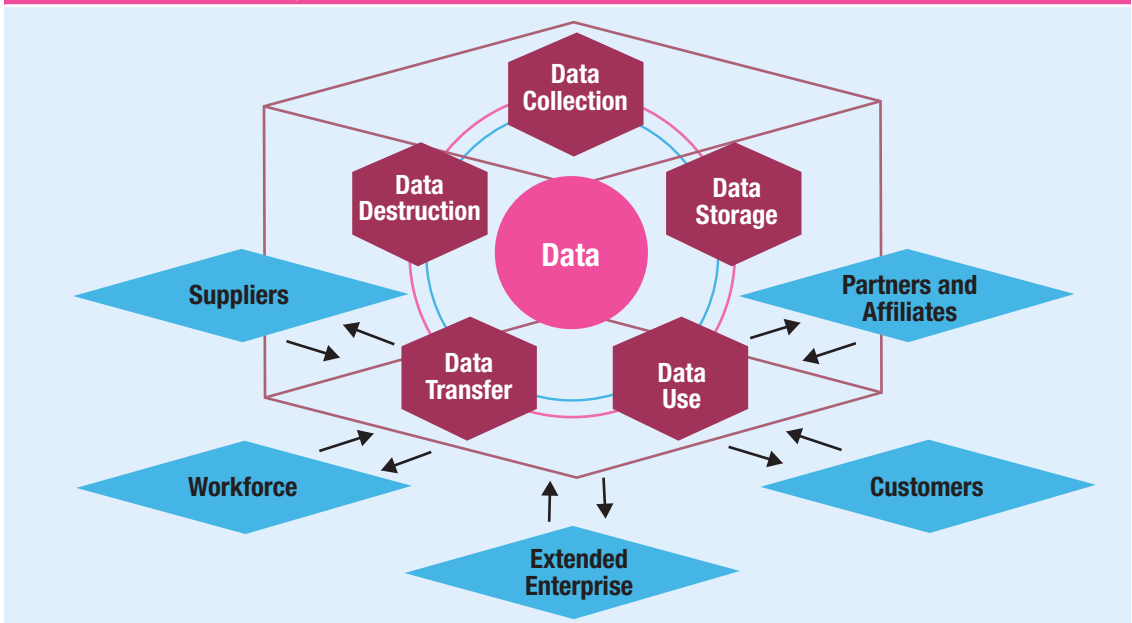
Identifying, assessing and promoting sound privacy and data protection baselines are crucial for good supervisory practices. Leading practices, industry

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2hgVija

Sudhakar Sathiyamurthy, CISA, CRISC, CGEIT, CIPP, ITIL Expert
Is a director with Grant Thornton's risk advisory services, focusing on cyberrisk. His experience has been shaped by the opportunity to help clients design and implement strategies to achieve a risk intelligent posture. Sathiyamurthy frequently advises clients on standing up and scaling cyber security and privacy capabilities and benchmarking them against laws, regulations, leading practices and industry standards. Sathiyamurthy has contributed to various cyberrisk innovation efforts and authored opinions and articles for leading journals. He can be contacted at sudsathiyam@gmail.com.

Figure 1—Illustration of a Typical Data Life Cycle



standards, corporate binding rules, and national/international laws and regulations set the baseline for privacy and data protection frameworks. The 2014 ISACA® Privacy Survey[3] reveals that International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002:2013,[4] COBIT®, EU Directive 95/46/EC,[5] American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants (CICA) Generally Accepted Privacy Principles (GAPP),[6] and US National Institute of Standards and Technology Special Publication SP 800-53[7] are the most commonly used frameworks for managing privacy. The European Union General Data Protection Regulation (GDPR)[8] explicitly embraces privacy and data protection by design as a legal obligation. The illustration in **figure 2** shows the themes embraced by the common privacy and data protection frameworks.

Multiple factors drive the need for a defensible privacy-by-design notion, and a representative list of themes is referred to in **figure 3**.

However, setting up a leading-edge program of privacy by design is often challenged by the following illustrative shortcomings:

- **Nonhomogeneity of laws and regulations**—With an uneven playing field created by the enactment of national and international privacy laws and regulations, instilling a common privacy denominator into engineering practices is not straightforward.
- **Misconceptions of data**—The misconceptions and human biases that shape the value system around the types of data (such as physical identity, social identity, genetic identity, health and wellness identity) and their sensitivities vary across nations. With a uniform definition of personal information not set in stone, changing privacy to suit individual expectations is perceived as a moving target.
- **Legacy solutions are beyond repair to integrate privacy**—Legacy solutions are not only poorly suited to address the emerging class of privacy risk, but are also overstrained with incremental repairs to fit privacy and data protection gaps.
- **Time-to-market overshadows privacy**—Products and solutions are sometimes rushed to market for competitive reasons without considerable thought to privacy implications. Organizations tend to balance privacy design requirements against business objectives and often care less about privacy demands.
- **Disarray due to competing priorities**—Product and solution design encompasses multiple interests and expertise and, hence, creates competing priorities of disparate parties (e.g.,

Figure 2—Illustration of Common Privacy and Data Protection Themes

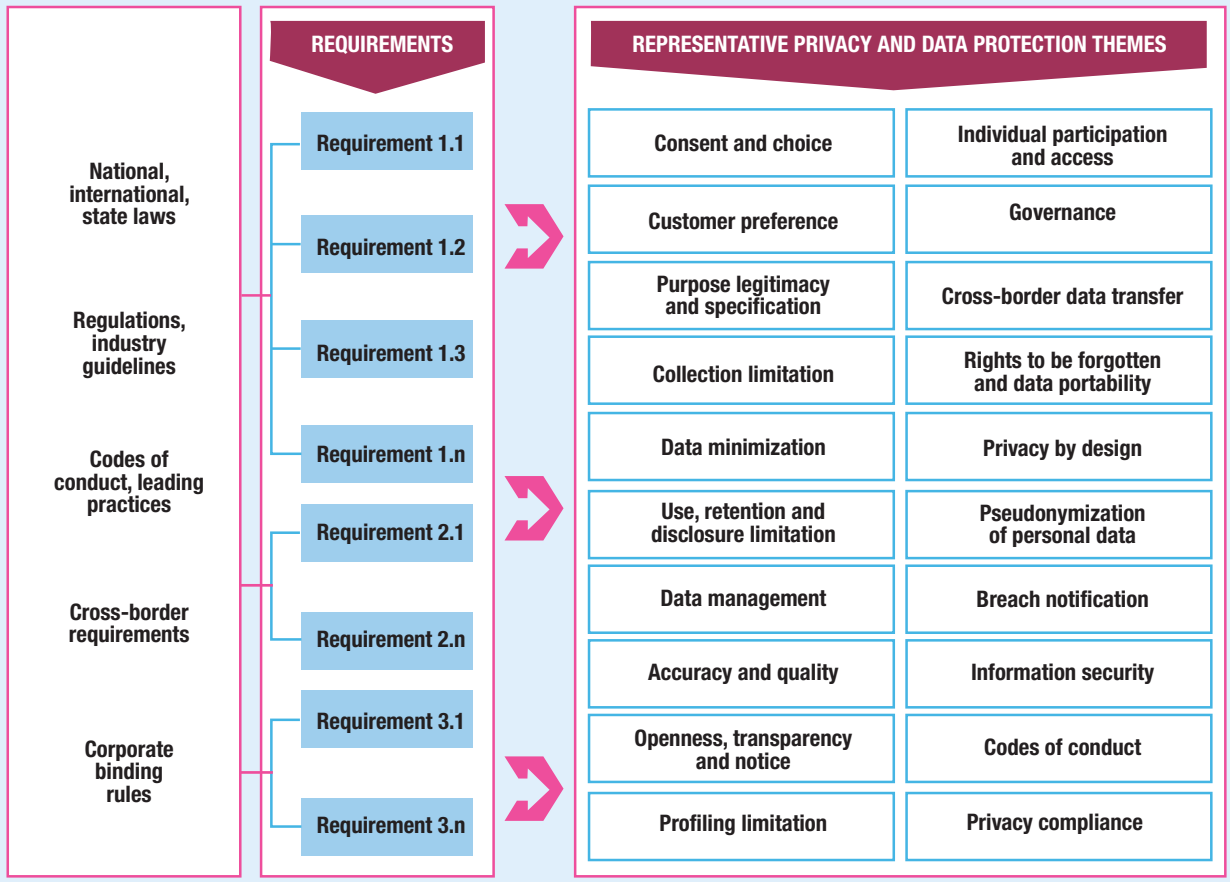
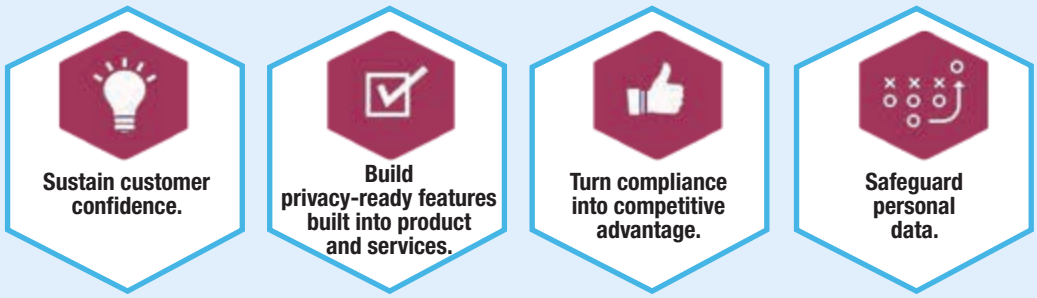


Figure 3—Business Value Drivers for Embracing Privacy by Design



business, marketing, engineering, innovation, security, privacy), which sometimes weakens the emphasis on privacy.

- **Business discomfort with privacy engineering principles**—Businesses that seek to monetize personal data (such as for online behavioral advertising) are sometimes uneasy with being inhibited to collect and use data if privacy engineering principles are implemented.
- **Institutional knowledge of personal data elements and data flow is limited**—Data protection safeguards are contingent on institutional knowledge and visibility of data elements and their flow, which, in many cases, are not fully mature.

Remember, data processed on defenseless information systems are data waiting to be stolen by an emerging class of crime groups.

- **Piecemeal approach toward privacy**—The piecemeal approach toward privacy has contributed to meeting the compliance demands that are traditionally siloed, however, the most often ignored aspect of this approach is its inherent inability to harmonize privacy across the organization's asset architecture (business processes, applications, infrastructure, facilities and functions). In the contemporary digital organization, privacy is no longer a siloed endeavor.

> **"...Privacy by design does not happen automatically; it needs to be promoted through integration with organizational influences, such as the enterprise's culture and belief system."**

In light of these shortcomings, privacy by design does not happen automatically; it needs to be promoted through integration with organizational influences, such as the enterprise's culture and belief system.

How to Achieve Privacy by Design

In a real-world scenario, integrating privacy requirements into products/systems/services is not straightforward. The significance of data flow within the product/system/service is illustrated using the analogy shown in **figure 4**. A typical information system makes quantum connections with neighboring systems, and the chain of connections extends to related systems across the organization and its supply chain constituents.

Privacy by design is multifaceted and can require reordering of priorities or reevaluation of assumptions based on fluctuations in privacy rule sets. Privacy generally is not the primary requirement of a product/system/service build-out, and it is not unusual for privacy requirements to conflict with functional requirements. Sometimes, deploying privacy by design limits the functionalities of the resulting solution. As a result, a trade-off between privacy and business value should be reviewed sensibly within the constraints of the agreed-upon purposes.

With privacy and data protection constituting the core values of the user community, there have been debates on embedding privacy and data protection principles into products/systems/services from the beginning of the design process. While the genesis of privacy by design has made its way beyond debate, tangible engineering strategies still remain unclear for many organizations. The privacy-by-design paradigm can be achieved by aligning it to the core principles illustrated using blockchain technology; an example is shown in **figure 5**.

Blockchain, in a nutshell, is a combination of protocols and technologies that create a distributed, consensus-driven database, which enables trusted transactions and data exchanges between parties without the need for arbitrators to mediate the exchange. Transactions on a blockchain are not regulated by any central authority. The entities and/or individuals involved in a given transaction provide their information (including personal information), which is then verified by nodes in the network (also known as miners). In this sense, the users forming the community act as their own authorities in a blockchain.

A typical blockchain offers distinctive features as shown in **figure 5**.

Blockchain's ability to replace intermediaries through its simplified ecosystem is indeed why this technology matters. While organizations have begun exploring the transformative and potentially disruptive advancement in harnessing blockchain technology, there is no consensus around the overarching challenges of privacy and data protection posed by blockchain technology. The following are some privacy and data protection challenges:

Figure 4—Data Flow Across the Organization Supply Chain

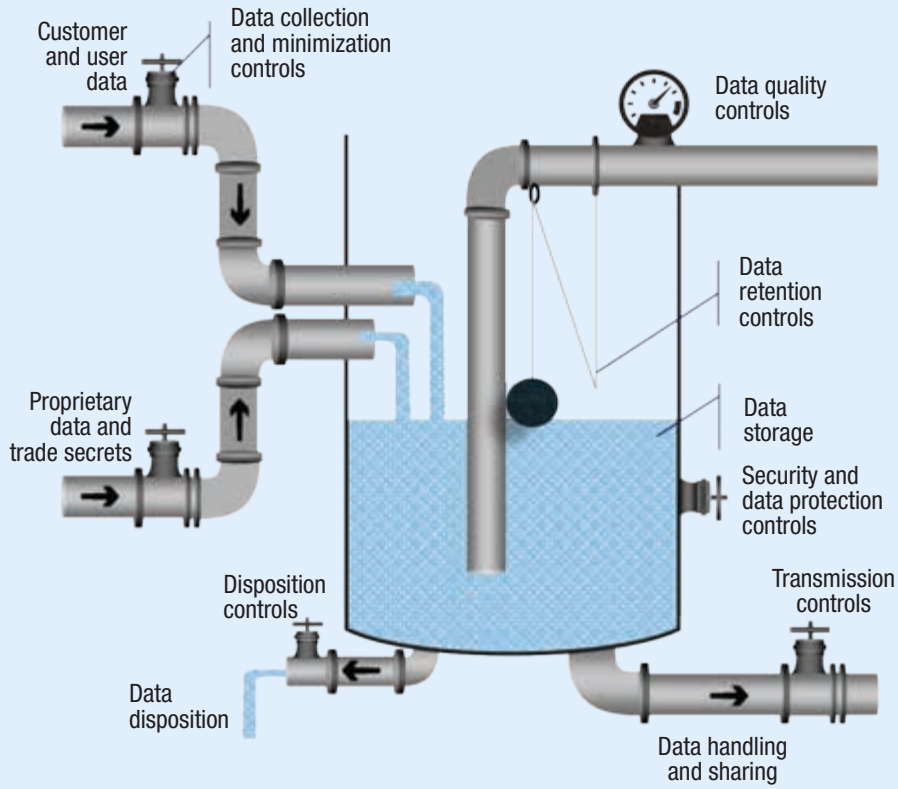


Figure 5—How Blockchain Works

- The digital trails associated with blockchain transactions and the metadata of personal details may still be sufficient to expose personal data and reveal private information about people. The exposure of metadata may have an upsetting impact on privacy.
- The distributed nature of transactions in the blockchain is recorded on a publicly available ledger and renders the transactions processed unalterable. This transparent and immutable nature of blockchain may raise issues as user's

Enjoying this article?

- Read ***ISACA Privacy Principles and Program Management Guide.*** *www.isaca.org/privacy-principles*

subsequent control over their personal data, once given away, is limited.

- If the digital key for encrypted data in blockchain is ever made public, the encrypted content would be accessible to anyone who holds the key.
- Blockchain technologies offer solutions that require arduous changes and updates to existing systems within an organization to coalesce and work in harmony.
- Evolving and nonhomogenous regulatory forces among different jurisdictions pose uncertainty regarding blockchain's operating philosophy. Blockchain nodes reside virtually in different legal jurisdictions, which can trigger practical implications from a regulatory standpoint.

> **"As new blockchain use cases emerge rapidly, ensuring defensible design of blockchain technology that accounts for user privacy and data protection is the key."**

As new blockchain use cases emerge rapidly, ensuring defensible design of blockchain technology that accounts for user privacy and data protection is the key.

The following principles[9] set the tone for privacy by design relative to blockchain technologies:

- **Proactive not reactive; preventive not remedial**—Frequently, amends for infringements of privacy and data protection obligations are usually reactive, taking effect only after the fact. In a complex distributed blockchain ecosystem, systematic monitoring and trustworthy functioning is critical to proactively sense nonconformities. Given that there are not many industry standards and regulations to govern the blockchain ecosystem and considering the potential risk that could undermine the privacy of transactions, this principle aims to prevent events that compromise users' privacy before they happen and not after the privacy risk materializes.
- **Right-sized privacy**—This principle seeks to deliver a reasonable degree of privacy by ensuring that personal information (such as financial and digital medical records) transacted in the blockchain is protected by appropriate technical and organizational measures.
- **Privacy protection embedded into design**—A typical engineering process focuses on realizing the functional requirements of the solution, and privacy and data protection assurances fall short as a result. These shortcomings are exacerbated by challenges associated with engineering privacy. This principle seeks to consider privacy needs from the very beginning of the engineering process. The viability of blockchain depends on its ability to deliver a privacy and data protection promise. The blockchain engineering process should be supported by appropriate libraries of privacy design strategies and privacy-friendly solutions to help designers support and realize a user's right to privacy.
- **Full functionality; positive-sum, not zero-sum**—This principle seeks to accommodate the legitimate interests and objectives of the individuals whose data are at stake in a positive-sum, "win-win" manner. An optimal blockchain strategy should account for solution value drivers, current opportunities, challenges and limits of the privacy-by-design principles and describe ways to ensure trustworthy functioning.
- **End-to-end security; full life cycle protection**—Confidentiality, integrity and availability considerations provide guidance on secure design choices and appropriate safeguards for privacy and data protection. Security considerations should follow the data wherever they go (from collection, storage, use, transfer, destruction) and protect blockchain technologies against malicious adversaries and cyberattacks.
- **Visibility and transparency; keep it open**—Visibility and transparency are related to the principles concerning openness. This principle seeks to assure stakeholders that blockchain services operate according to the stated promises and objectives subject to independent verification. While regulations and leading practices designed to standardize blockchain transactions could prove beneficial, independent auditing and verification

methods can provide reasonable oversight until regulatory and legal precedents catch up.

- **Respect for user privacy; keep it usercentric**—Traditional engineering design practices barely consider the privacy and data protection interests of end users. This principle seeks to rationalize and account for the interests of all parties involved in blockchain solutions and services by offering creative countermeasures and privacy-friendly solutions.

The aforementioned principles set the minimum baseline for achieving privacy by design, however, these principles are not by themselves an absolute guarantee that the product/system/service will comply with all privacy requirements. The privacy-by-design approach is a continuous process and, therefore, compliance to privacy mandates should be continually reviewed in perspective of changes and/or updates to national and international privacy laws and regulations.

Conclusion

New generations of consumers have behaviors and expectations that drive privacy-friendly versions of current products, systems and services. Legal, regulatory requirements and social practices help enlighten to better respond to consumer demands and better inform privacy-by-design solutions. The confluence of these powerful forces is a compelling driver of the need for consumer privacy improvements.

The genesis of privacy is to protect users' rights and their freedom to determine how personal information is used, which is why privacy by design is a stride toward consumer-centric design. Consumer-centric design does not operate in a "building products by techies for techies" manner. Instead, it focuses on transparent and trustworthy design that empowers users to exercise their right to and over information.

In the aggregate, institutional improvements must operate in ways that allow for the highest possible measure of consumer trust. Smart organizations will not resist this trend. They will underscore the importance of creating a privacy-friendly ecosystem and fostering privacy by design.

Endnotes

1 IDC, "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," April 2014, *https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm*

2 Sathiyamurthy, S.; "The Struggle for Privacy and the Survival of the Secured in the IT Ecosystem," *ISACA® Journal*, vol. 2, 2011

3 ISACA®, *Keeping a Lock on Privacy: How Enterprises Are Managing Their Privacy Function*, USA, 2015, *www.isaca.org/knowledge-center/research/researchdeliverables/pages/keeping-a-lock-on-privacy.aspx*

4 International Organization for Standardization, ISO/IEC 27002: 2013, *Code of Practice for Information Security Controls*, 2013

5 European Communities, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data," *Official Journal of the European Communities*, vol. 38, 23 November 1995, *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1995:280:TOC*

6 American Institute of Certified Public Accountants (AICPA), Generally Accepted Privacy Principles (GAPP), USA

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

8 European Parliament, Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," *Official Journal of the European Union*, 4 May 2016, *http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*

9 Cavoukian, A.; *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, Canada, December 2012, *www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf*

Blockchain: Identifying Risk on the Road to Distributed Ledgers

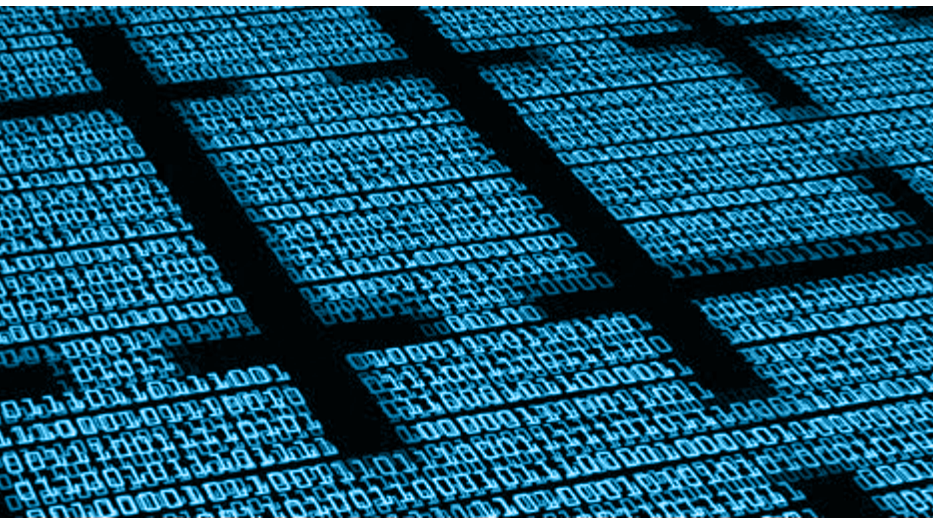
Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2hg7iBF

日本語版も入手可能
www.isaca.org/currentissue

Blockchain technology, commonly expected to drive the next wave of digital infrastructure and process innovation, is rapidly developing into maturity. Five IT risk subdisciplines are of significant interest when embarking on blockchain-driven projects: cyber and information risk, architecture and design risk, IT compliance risk, third-party and vendor risk, and integration risk.

Blockchains allow multiple entities to achieve consensus on transaction data, i.e., a single version of the truth, without the need for a trusted central authority or notary function. The technology is a new data recording paradigm that lets multiple, potentially unknown or untrusted, networked entities share and append to digital ledgers. The integrity and confidentiality of the data in the digital ledgers are cryptographically guaranteed.



Three core features—immutability, transparency and autonomy—drive the technology's ability to disrupt current products, processes and business models in a variety of industries. As the single version of the truth (i.e., immutable and up-to-date data) is available to all networked entities, the information asymmetry between the entities is reduced, and costly reconciliation activities between different information sources can be avoided. For example, a blockchain solution could provide a complete overview of a patient's medical history—resulting in significant advantages in case of emergencies—instead of housing records among multiple health care institutions as is done now. Blockchain technology also ensures that the recording of data is in accordance with mutually agreed-on conditions, enabling disintermediation of central validating entities.

It is hard not to be fascinated by something so transformative. That being said, technology-driven opportunities to improve process efficiency and effectiveness rarely come without challenges and risk. This article aims to identify IT risk that should be considered during the development of a blockchain-driven solution and provides strategies to minimize this risk.

Cyber and Information Risk

Cyberattacks may compromise the confidentiality, integrity and availability of the data recorded in a blockchain. Technical vulnerabilities that can be exploited by hackers to cause loss or harm remain omnipresent. There is no evidence to indicate that this would be different for blockchain implementations. Additionally, the response strategies for dealing with cyberincidents are often inadequate. For example, in June 2016, the DAO, a

Filip Caron, Ph.D.
Is a faculty member at the KU Leuven Research Centre for Information Management and the Leuven Institute for Research on Information Systems (Belgium). He teaches graduate courses on business analysis and process management, and he is a researcher in the field of information security and governance, risk and compliance (GRC) practices. Caron is the author of more than 30 academic publications. He can be reached at Filip.Caron@kuleuven.be.

decentralized autonomous organization based on the Ethereum blockchain, suffered a cyberattack that deployed a combination of vulnerabilities, resulting in a loss of one third of its funds (approximately US $50 million).[1] While a security patch had been proposed days before the attack, there were neither security teams nor procedures in place to act. Instead, the proposed patch needed to be adopted through a formal voting process with 23,000 eligible voters, as specified in the mutually agreed-on conditions.

Security weaknesses can also be found at the endpoints writing to a blockchain application and securely storing the cryptographic keys that are used as digital signatures. The cyberincidents at Bitcoin exchanges Mt.Gox (US $450 million lost) and Bitfinex (US $72 million lost) are notable examples of cyberattacks that centered on compromising the IT infrastructures at endpoints of the network.

Cyber security measures that could assist in mitigating this risk include:

- Conducting extensive penetration tests on the blockchain application.
- Implementing adequate endpoint security that includes the design, implementation and maintenance of controls that ensure a secure delivery of services (e.g., preventive controls such as access control and firewalls) and measures to identify the occurrence of an incident (e.g., network and system monitoring). An overview of appropriate controls can be found in COBIT® 5,[2] the International Organization for Standardization (ISO) 27000 series, and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
- Instigating incident response processes that focus on incident analysis, containment, eradication and recovery. In preparing these processes, organizations should also consider communication policies and arrangements with specialized cyberemergency response teams.

“A broad variety of both technical and organizational design decisions must be made during the development of a blockchain solution.”

Details on effective incident response strategies can be found in NIST Special Publication (SP) 800-61 Revision 2.[3]

Architecture and Design Risk

A broad variety of both technical and organizational design decisions must be made during the development of a blockchain solution. These design choices may have a significant impact on the performance of the solution and, consequently, on the achievement of the business objectives.

Technical designs for blockchain solutions may not be aligned with functional requirements. The selection of a consensus protocol, used for validating proposed additions to a blockchain-based ledger, is an often-cited design choice that impacts operational capacity. While VISA can process approximately 56,000 transactions per second (reported in 2015),[4] Bitcoin’s consensus protocol limits the payment system to only seven transactions per second.[5]

In a “code is law” environment, the completeness of the coded rule set is of primary importance. Incomplete rule sets may allow for undesirable, but not forbidden, user behavior. Incentives for strategically voting, which prevents voting based on sincere preference, have been exposed in the DAO’s code and could have a significant impact on the investment decisions of the organization.[6]

Additionally, designs could become unsuitable due to technological evolutions. Advances in quantum computing may bring about a credible threat to current state-of-the-art cryptographic systems that are used to guarantee the integrity and confidentiality of the data stored in the blockchain. These cryptographic systems rely on mathematical problems that are almost impossible to solve with current conventional computing.

> **"Compliance challenges regarding the consensus mechanisms and information security have already been identified."**

Organizational design decisions include access restrictions and role differentiation. Restricting access to the blockchain solution to a preselected, trusted set of nodes (i.e., permitted blockchains) can have important advantages such as working with trusted participants, more efficient consensus protocols and greater levels of privacy. Permitted blockchains are better suited for establishing formal governance structures and procedures to react in case of incidents and to actively manage the encoded rules. In contrast, public blockchains are open to everyone to participate in and review the encoded rules. Therefore, public blockchains tend to lower the barrier to participation and can protect users against developers willing to take control.

Differentiating the roles and responsibilities of the participants, (e.g., only allowing a trusted authority to perform the initial registration of real estate in a blockchain-based land registry, might be desirable. Several authors also indicated that blockchain might not be the most appropriate technology for a setup in which all participants are IT systems operated by the same real-world entity.[7]

Approaches that could partially mitigate architecture and design risk include:

- Establishing requirements and engineering processes comprising the effective elicitation, analysis and prioritization of business functional, technical and compliance requirements. Formal confirmation and a timely update of the requirements specifications are considered best practices. Guidance can be found in the COBIT 5 specification for the Build, Acquire and Implement (BAI) domain's BAI02 *Manage requirements definition* process.
- Adopting a security-by-design focus in the development of the blockchain solution. Technical measures include restricting access to the blockchain (i.e., creating a permissioned blockchain) and establishing role differentiation (e.g., supporting the use of trusted record validators or asset registrars). Business measures could include strict onboarding processes and ensuring geographical spread.
- Conducting strict code reviews and acceptance tests for the blockchain solutions
- Assessing technological evolutions that might support or impact the achievement of the business objectives
- Setting up formal governance structures and procedures to deal with the strategic long-term evolution (e.g., a technology renewal or a revision of the encoded rules) and incidents that need to be resolved in the short term

IT Compliance Risk

As regulations proliferate and stakeholders' expectations increase, there is an increased risk of violating regulations and industry standards that could directly impact the participants' financial position, organization and reputation. Compliance challenges regarding the consensus mechanisms and information security have already been identified. The financial industry has strict requirements for the absolute finality of a transaction, as specified in the Settlement Finality Directive (SFD). Distributed consensus protocols that are based on computational work, such as the proof-of-work protocol underlying bitcoin, typically provide only probabilistic finality. Technically, transactions are never truly final as there

is always a possibility that a longer chain is created that does not include the block of the transaction. However, as more blocks are added, it becomes less economically viable and/or computationally possible. It remains to be tested whether probabilistic finality complies with the SFD requirements.

> **"It is not uncommon that the blockchain software vendor is a start-up or scale-up organization."**

A wide variety of industry-specific and generally applicable regulations regarding the confidentiality, integrity and availability of data have been put in place. In the US, blockchain solutions for sharing and recording patient records are subject to the US Health Insurance Portability and Accountability Act (HIPAA), whereas in Europe, requirements for personal data are strengthened and unified by the General Data Protection Regulation (GDPR). The GDPR includes, among others, requirements for the export of personal data outside the European Union.

The variety of regulations may make it difficult to determine the appropriate regulations for the blockchain solution as participants and copies of potentially sensitive data ledgers may be dispersed over multiple jurisdictions with varying regulatory objectives.

Measures for dealing with IT compliance risk as it applies to blockchain include:

- Reviewing broader regulatory requirements and standards, including both industry-specific and generally applicable rules
- Monitoring regulatory developments and evolutions in the standard-setting processes
- Engaging with the relevant regulators, preferably at an early stage of the design phase, to ensure adherence to policy objectives. Some authorities have set up specific frameworks (e.g., the regulatory sandboxes of the UK's Financial Conduct Authority) that allow innovators in the financial industry to test their ideas without immediately incurring all the normal regulatory consequences.
- Defining restrictions on access to the blockchain solution (e.g., only allowing identified and vetted partners in order to comply with anti-money laundering regulations) and restricting the allowable locations for participants who maintain copies of the ledgers to avoid noncompliance in specific jurisdictions

Third-Party and Vendor Risk

While the bitcoin peer-to-peer electronic cash system has been designed to operate without trusted third parties, most blockchain projects are developed in the context of a strategic partnership with a blockchain software vendor. Associated with these strategic partnerships is another type of third-party risk—the risk that the vendor will not be able to deliver reliable and secure services.

It is not uncommon that the blockchain software vendor is a start-up or scale-up organization. While start-ups may be successful, many start-ups may have strategic evolution issues, regulatory compliance issues, unstable financial conditions and/or lack proper human resources. For example, in mid-2015, Ripple, a start-up blockchain software vendor, announced that it would discontinue the development of its Codius platform.[8] In the same year, Ripple was fined by the US Department of the Treasury for violating several regulatory requirements, including failing to implement adequate anti-money laundering programs into its products.[9] Ripple has since agreed to remedial actions. Financial risk is also a frequent concern. Many blockchain start-ups fail due to a lack of funding.[10] Finally, attracting blockchain experts—and avoiding attrition—can be challenging for start-ups.[11]

Actions for managing risk associated with blockchain software vendors include:

- Implementing risk management strategies that cover the continuous life cycle of third-

party relationships, including the planning, due diligence, third-party selection and termination phases. The US Office of the Comptroller of the Currency (OCC) Bulletins 2013-29 and 2017-7 provide guidance on third-party relationships in the financial industry, whereas the US Health Information Technology for Economic and Clinical Health (HITECH) act explicitly specifies requirements for "business associates" in the health care industry.

- Conducting postcontract compliance assessments and continuous monitoring programs
- Actively managing third-party relationships to acquire insight into the long-term strategic objectives of the third party and establishing formal communication lines that can be used in case important risk to the vendor materializes
- Requesting internal and external audit assurance on the current state of the third party, its controls and its services, e.g., International Standards for Assurance Enagement (ISAE) 3402, Assurance Reports on Controls at a Service Organization.[12]

Integration Risk

When organizations face technological changes that could disrupt their products, processes and business models, their managers may be tempted to react hastily and push for a premature technology renewal. These organizations risk that their technology renewal strategy will be inadequate, either due to a lack of integration with existing systems (technology perspective) or business processes that are not appropriately adapted (business perspective). A Deutsche Bank research analyst concluded that traditional banks' struggle with legacy systems is a major inhibitor of technological innovation.[13] Interfaces for integrating new technologies in existing systems cannot be developed within an acceptable time frame. Other proposals, (e.g., the Swedish Lantmäteriet's proposal for a real estate transaction system) stretch the integration requirements even beyond the internal systems.[14]

Furthermore, integration issues might arise when reconciliation between multiple blockchain-based ledger systems is needed. For example, in its utopian view of capital markets using blockchains, Euroclear flags the need for synchronization between ledgers holding different asset types (e.g., cash and derivatives).[15] In the same report, Euroclear argues that certain participants in the capital market could be disintermediated, which would impact the activities and business processes of the remaining financial institutions.

> **"An analysis of blockchain solution development risk reveals the potential benefits of establishing formal governance structures and procedures."**

To mitigate integration risk, an organization might:

- Focus on developing repeatable testing procedures and extensive testing plans, in addition to stressing the importance of requirements engineering
- Manage organizational change enablement as detailed in COBIT's BAI05 *Manage organisational change enablement* process to prepare and commit stakeholders for business change
- Opt, where possible, for generally accepted blockchain technology and interface standards

Conclusion

An analysis of blockchain solution development risk reveals the potential benefits of establishing formal governance structures and procedures. While this finding contradicts the base premise for which blockchain was pioneered in a cryptocurrency setting, it may prove invaluable for risk prevention and recovery.

As with blockchain technology, the regulatory framework around it has not yet fully matured, which elevates the likelihood of compliance risk materialization. Furthermore, permitted blockchains with strict onboarding and effective access management might be more appropriate to satisfy the business, technical, security and compliance requirements for contemporary ledger solutions.

Endnotes

1 Finley, K.; "A $50 Million Hack Just Showed That the DAO Was All Too Human," *Wired*, 19 June 2016, *https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human*

2 ISACA®, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/Pages/default.aspx*

3 National Institute of Standards and Technology, *Computer Security Incident Handling Guide Revision 2*, NIST Special Publication 800-61, USA, 2012, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

4 Visa, "Visa Inc. at a Glance," USA, 2015, *https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf*

5 Croman, K., *et al*.; *On Scaling Decentralized Blockchains*, 2016, *http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf*

6 Mark, D.; V. Zamfir; E. G. Gun Sirer; *A Call for a Temporary Moratorium on "The DAO,"* 26 May 2016, *https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWyS-dQ4lsBacR2dUgGTtV98C40/edit#*

7 Buterin, V.; "On Public and Private Blockchains," Ethereum blog, 7 August 2015, *https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/*

8 Glatz, F.; "The Quiet Death of Ripple's Codius Project: Why Decentralized Infrastructure Has Still a Long Way to Go," Medium, 13 June 2015, *https://medium.com/@heckerhut/the-quiet-death-of-ripple-s-codiu-project-782c11a17c02*

9 Department of the Treasury Financial Crimes Enforcement Network, "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger," USA, 5 May 2015, *https://www.fincen.gov/sites/default/files/shared/20150505.pdf*

10 CB Insights, "Startup Failure Post-Mortems," blog post, 10 February 2017, *https://www.cbinsights.com/blog/startup-failure-post-mortem/*

11 Nash, K.; "Blockchain Experts, a Rare Breed, May Demand Big Bucks," *The Wall Street Journal*, 12 May 2016

12 International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls and a Service Organization*, 15 June 2011, *www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf*

13 Allison, I.; "Deutsche Bank Mulls the Potential of Blockchain and the Problem of Legacy Systems," *International Business Times*, 24 August 2015, *www.ibtimes.co.uk/deutsche-bank-mulls-potential-blockchain-problem-legacy-systems-1516686*

14 Lantmäteriet (The Swedish mapping, cadastre and land registration authority), Telia Company, ChromaWay, Kairos Future, "The Land Registry in the Bockchain," July 2016, *http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf*

15 Wyman, Oliver; *Blockchain in Capital Markets: The Prize and the Journey*, Euroclear, February 2016, *https://www.euroclear.com/dam/Brochures/BlockchainInCapitalMarkets-ThePrizeAndTheJourney.pdf*

Instilling a Culture of Security Starts With Information Governance

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2vFygbZ

Change is difficult. Fear of the unknown, weariness of new approaches and apathy are change barriers individuals face in their personal lives and at work. In a corporate setting, these obstacles are exacerbated by the sheer number of people impacted, geographic factors, and reliance on existing systems and processes for continuity. Often, culture can be the underlying culprit to making important changes within an organization. Existing culture, whether official or perceived, can be a real hurdle to effectuating and implementing change. It is further complicated when dealing with compliance, privacy and security issues, given their sensitive and legal nature.

Corporations in highly regulated industries or with global operations face countless challenges in maintaining compliance with regulations and securing their data and the sensitive data they house on behalf of customers. In the United States alone, sanctions imposed on the private sector by regulators have steadily increased, and numerous class action lawsuits have been filed against corporations following major breaches of customer data. A Cisco report from 2016 found there were 780 breaches with a total of nearly 178 million records stolen in 2015, and the average cost of each lost or stolen sensitive record increased six percent from 2015 to 2016.[1] Adequately preparing for regulatory inquiries and litigation and arming against data breaches are complex endeavors that must be approached holistically and strategically. All of this begins with proactive and strategic information governance (IG).[2]

In practice, IG remains ethereal and abstract, with very little consistency from person to person on how it is defined. Broadly, IG is the practice and framework of proactively managing the valuation, creation, storage, use, archival and deletion of data within an organization. Efforts may also include migrating to cloud systems, establishing data privacy programs, implementing legal hold and enabling stronger regulatory compliance. Proactive IG allows legal, compliance and IT teams to take incremental, measurable steps toward bolstering programs, policy and culture shifts that are rooted in security and compliance and are necessary for dealing with today's data challenges.

A company that is facing privacy and security challenges does not need to radically change the way it does business, but rather can leverage culture to implement and foster the necessary procedural and technological transformations needed to strengthen security. Certain steps can be taken to build a strong respect for and practice of security into the cultural fabric of any organization, across all departments and areas of the business. Company activities such as moving to the cloud, responding to data requests for litigation or regulatory inquiries, staff training and education, and employee use of personal mobile devices for work can all significantly impact security and must be considered as part of efforts to strengthen the overall security culture. Executive leadership, strategic change management, technology implementation, incentives, customized training, mobile policies, and involvement of legal and compliance in executing IG and data security programs can all help shape a culture of security that is sustainable long term.

T. Sean Kelly
Is a senior director within FTI Technology's information governance and compliance services practice. He advises clients on all aspects of e-discovery and information governance, with a particular focus on developing and implementing legal-hold processes and technology and the legal impacts of migrating to Microsoft Office 365. He leverages more than a decade of experience in both legal technology and litigation support to advise clients on evolving technologies and the shifting landscape associated with cross-border transactions for global enterprises. Kelly previously worked for Johnson & Johnson, where he was responsible for e-discovery issues across business sectors, advising internal stakeholders and outside counsel on best practices in collection, forensic technology, document review and controlling cost.

Establishing a Task Force

First and foremost, any effort geared toward making changes to the corporate culture or implementing new IG practices will require a cross-functional team of key stakeholders that may include records management, legal, compliance, security, IT and operations. The task force will be instrumental in ensuring that new programs—and cultural shifts—are meeting the needs of the entire organization and addressing challenges that may arise from any given department.

Executive Sponsorship

Once key stakeholders are on the same page, they must secure board and/or executive sponsorship for the effort. The key to gaining buy-in is communicating the program's benefits that will specifically address the executive's unique pain points. If the executive sponsor is the general counsel, building the risk case for that person is critical—this includes the risk of not disposing of data that have met their retention requirement and are not subject to legal hold. If sponsorship is solicited from the chief information officer or another IT leader, he/she may be more likely to embrace a project that addresses data minimization and defensible disposal. Business leaders and board members will be more focused on the costs, overall impact to the bottom line and mitigated risk. The proposal should also take into consideration the cost avoidance of possible data breaches and penalties for failing to comply with various regulations in any region where the company does business.

Structure and Fresh Thinking

With executive sponsorship secured, the team must analyze the current infrastructure, policies and processes. This includes evaluating systems, how they are used in day-to-day operations, and employee attitudes toward security and compliance in the current environment.

"Any effort geared toward making changes to the corporate culture or implementing new IG practices will require a cross-functional team of key stakeholders."

Often, change goals get lost in a sea of discussions about headcount and resourcing requirements. But the people part of the equation is essential to enabling long-term transformation. According to a 2014 information governance survey, only 8 percent of organizations report that records management metrics for electronically stored information are mature, and only an additional 29 percent report that those metrics are improving.[3] To improve these metrics, organizations must invest in existing staff, while also bringing in new people who embody and demonstrate the values that will be part of the new culture. The introduction of new thinking and ideas, managers with a unique perspective, and experts with innovative strategies will lead to companywide behavioral changes that can refresh and renew the culture.

Incentives

A key part of gaining companywide adoption for any new program is to help employees understand what is in it for them. This can help affect behavior and attract new capabilities. There are a handful of household-name companies that are known for maintaining strong incentive programs that are directly linked to company culture. What their approaches have in common is linking performance and monetary incentives to an evaluation of how employees are living and acting by the cultural guidelines.

> **When rolling out any new program, it is imperative to have a computer-based training module in place for all users.**

By understanding what incentivizes people and linking those incentives to employees' active participation in embracing new processes, such as compliance and security protocols, IG stakeholders can significantly improve the enthusiasm and pace at which new culture standards are adopted. The IBM X-Force 2016 Cyber Security Intelligence Index reported that in 2015, 60 percent of all attacks were carried out by insiders, either those with malicious intent or those who served as inadvertent actors.[4] This is an important reminder of why security must be instilled from the top down, across the entire workforce.

Change Management

Understanding how to effectively manage and enable change—and approaching it as a journey toward stronger security and compliance—is essential. During an effort to change the culture for stronger security awareness, the task force must communicate the fundamental legal and regulatory drivers behind the proposed changes and ensure the company understands just how important these factors are to the organization's overall success and business continuity.

One of the most widely accepted methods for implementing change management is the Kotter 8-step Change Model,[5] which was developed to help organizations become adept at progress. Some of the key tenets of this model, which will help with strengthening attitudes toward security, include creating urgency, clearly communicating the vision, identifying and eliminating obstacles, setting short-term realistic goals that foster a sense of achievement among those involved, and making changes permanent by solidifying adoption and addressing opposition head-on. These steps can again be tied to incentive programs to provide employees with attainable goals that align with the new security programs.

Training

When rolling out any new program, it is imperative to have a computer-based training module in place for all users. The information governance survey mentioned earlier reports that half of organizations indicate employees never receive records information management training.[6] Executive sponsors can be particularly helpful in ensuring that the training is mandatory for everyone in the organization—a key factor in maintaining long-term change. Outside advisors can be particularly useful at this stage, as they are able to help internal teams outline the critical security vulnerabilities and necessary components of the program, develop audience-specific training materials, identify what users will need to be trained on, and determine what the depth of that training should be.

Training should not be out of the box from software providers, nor should it necessarily be the same for everyone in the organization. Training collateral should be security- and privacy-focused and tailored to the organization's specific needs. Materials must show users what the new policies look like within the context of their work environment and how they impact data breach prevention and regulatory compliance. It is also useful to build a dedicated page available to all internal users that offers reference guides and a frequently asked questions section dedicated to explaining new policies and tools that are being used and why.

Mobile Workforce

The entrance of the Internet of Things (IoT), mobile devices and text messages into the world of e-discovery has created a number of challenges that impact compliance and security. Data on a custodian's mobile or Internet-connected device, including text messages or other data that have been collected from the device—whether company owned or personal—might be in scope in almost any investigation or litigation and can be more vulnerable to a data breach or leaks. These devices are evolving especially quickly, and architecture and software

tools that are new today may be antiquated tomorrow. Corporations that are proactive about both their mobile workforce and any company-related usage of IoT products and maintain up-to-date and enforceable policies will find it much easier to navigate compliance and security issues. IoT specifically should be vetted by IG stakeholders within an organization to determine possible risk areas and how data from those devices may need to be mitigated.

Another related and growing area of consideration is enterprise migration to cloud services such as Google Apps for Work and Microsoft Office 365. According to Microsoft, Office 365 alone has more than 60 million commercial customers, and adoption is expanding at a rate of 50 percent quarter over quarter.[7] The movement of critical corporate data to the cloud raises security and data protection concerns, and analyst reports have shown the incidence of advanced email threats rising for corporations of all sizes. IBM reported that the average client organization monitored by its Security Services experienced 52,885,311 security events, 1,157 attacks and 178 incidents.[8]

Cloud migration brings a long list of IG priorities and considerations, ranging from e-discovery needs, retention and legal hold requirements, migration methodology, and technical quality control and testing. These issues are complex and should be addressed in advance of a migration to ensure proper handling across IT, legal, compliance

> **"Maintaining change and enforcing adoption of new processes is critical to shaping a culture of security that grows and strengthens over time."**

and security, and to build in training and change management that map back to the broader efforts of weaving security into the company's culture. When looking at policies for mobile device data, counsel should address data privacy concerns and software limitations for managing security. Key considerations include:

- **Device ownership**—Making a distinction about who owns the device and what access the organization has to the data on that device is important and must be outlined by an acceptable-use policy that applies to all devices and gives consent for the company to control the device through mobile device management, including remote access, data collection and wiping the device.
- **Data privacy**—Multinational corporations must be mindful of the wide variety of data protection laws around the globe and prepared to deal with conflicts between privacy laws and corporate policies in regions where the data reside; development of individual policies that are tailored to the data protection laws of each region can help lay the groundwork for securing data in compliance with each jurisdiction.
- **Software**—Every company should have mobile device management software in place, which eases some of the challenges with securing, managing

Enjoying this article?

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

and collecting data from mobile devices; the software should offer strong scalability to grow as the company grows and provide features that allow the corporation to control the device on the back end without visibility to users.

Enforcement

Maintaining change and enforcing adoption of new processes is critical to shaping a culture of security that grows and strengthens over time. There are a handful of approaches and technologies that enable compliance monitoring, and they work by flagging violations of new protocols and enabling stakeholders to take remedial action. In conjunction with monitoring, tying compliance to employee performance evaluations is very effective to driving adoption. When employees understand that a lack of participation with training programs or violation of new policies will adversely impact their performance ratings or compensation, they are much more likely to dig in and commit to the changes. Employee metrics for compliance with new policies can be directly tied to the organization's incremental goals for implementing those policies and measuring adoption.

Education around how detrimental security breaches can be and the cost they impose on the organization can also help employees understand the negative impact. In many cases, it is not that employees are ambivalent about security; it is that they simply do not understand how their actions impact data security, nor how consequential a breach can be. Once they have been educated about the overall importance of security to the long-term health of the company, most employees are much more supportive of security efforts and are vigilant in reporting policy violations.

Conclusion

Failure to handle data properly and instill a deep respect for privacy and security can result in damaging data breaches, and it has for hundreds of companies. Beyond the legal and compliance risk that comes with a data breach, it also breaks trust and causes doubt to become part of the company's reputation. Thus, it is critical that the legal, compliance and security requirements are viewed as opportunities to instill a high standard for ethics and privacy into the company's culture.

When each and every employee embodies trust, ethics, security and privacy, these values will translate to the services or products the company provides. By embracing this mindset, a corporation's leadership can set the correct tone from the top down, building advocacy for actionable programs that ensure safe and responsible handling of sensitive data, in addition to strong compliance and efficiency.

Endnotes

1 Cisco, *The Zettabyte Era: Trends and Analysis*, 2016, *www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf*
2 FTI Consulting, "Information Governance & Compliance Services," *www.ftitechnology.com/solutions/information-governance-and-compliance-consulting-services*
3 Cohasset Associates, ARMA International, AIIM, *2013 | 2014 Information Governance Benchmarking Survey,* 2014, *www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/C/Compliance-Benchmark-Report.aspx?TempAuth=True*
4 IBM, *X-Force 2016 Cyber Security Intelligence Index*, 2016, *https://www.ibm.com/security/data-breach/threat-intelligence-index.html*
5 Kotter International, 8-step Process, *https://www.kotterinternational.com/8-steps-process-for-leading-change/*
6 *Op cit,* Cohasset Associates
7 Microsoft, "Microsoft Cloud Strength Highlights Third Quarter Results," 27 April 2017, *https://news.microsoft.com/2017/04/27/microsoft-cloud-strength-highlights-third-quarter-results-2/#11Ct2akfPsVWgmyz.97*
8 *Op cit,* IBM

Barriers and Enablers to Auditors Accepting Generalized Audit Software

日本語版も入手可能
www.isaca.org/currentissue

Although generalized audit software (GAS) has been shown to significantly improve the efficiency and effectiveness of audits,[1, 2] many auditors do not use this technology.[3, 4, 5, 6, 7] In fact, one auditor noted that, "Non-IT auditors seem overwhelmed and even intimidated by GAS tools." The study described in this article employed an online survey of 277 auditors who use generalized audit software (GAS) to determine the factors that positively and negatively affect its usage.

The research on GAS has tended to overlook the influence of barriers that inhibit its usage[8] and has merely focused on factors that enable its use. However, the factors that serve as barriers for rejection of systems are just as worthy of study as the factors that enable acceptance of systems.[9] Research has shown that barriers to a system's use, when present, tend to dissuade users; however, they do not, by their absence, encourage use. For example, just because a system is available and reliable does not mean that it is more likely to be used. On the other hand, if a system is not reliable or available, this could lead to outright rejection by users.

Barriers to IT acceptance are significant and deserve study in their own right—both as they occur alone and as they interact with enablers.[10] In practice, because barriers can bias users' perceptions of positive factors, they may, in fact, be more influential in encouraging a user to reject the system.[11] Examining both negative and positive factors in system use can provide a richer understanding of adoption factors and might, in the end, encourage greater GAS use.[12, 13]

Considering how important the interplay of barriers and enablers to GAS use can be, the study examined both kinds of factors when surveying IT, financial and operational auditors.

Figure 1 presents characteristics of the 277 auditors who completed the survey. The majority had at least five years of audit experience and had used GAS for more than two years. The industries most represented in the sample were public accounting, banking and finance, and government and nonprofit. Most auditors in the sample were financial auditors and most worked in an internal audit capacity. The auditors surveyed used a variety of GAS solutions, with the majority using IDEA, followed by ACL.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2f1IFlh

Marianne Bradford, Ph.D.
Is a professor of accounting in the Poole College of Management at North Carolina State University (NCSU), USA, where she teaches enterprise resource planning (ERP) systems. Her background is with Ernst & Young in the IT Risk Assurance group. At NCSU, she is faculty coordinator for the SAP University Alliance and has been teaching business processes and controls in SAP for nine years. She is also the author of *Modern ERP: Select, Implement and Use Today's Advanced Business Systems*, now in its third edition. Bradford's research interests include ERP implementation issues, security and auditing.

Dave Henderson, Ph.D.
Is an associate professor of accounting at the University of Mary Washington (Virginia, USA), where he teaches principles of accounting, managerial accounting, accounting for decision making and control, and accounting information systems. He has nearly 20 years of experience in the information technology and accounting fields in various roles including assistant professor, financial analyst, financial systems developer and project manager. Henderson's research interests focus on accounting information systems (AIS) technology adoption and development, Internet financial reporting, and internal auditing.

Figure 1—Characteristics of Survey Participants and GAS Used

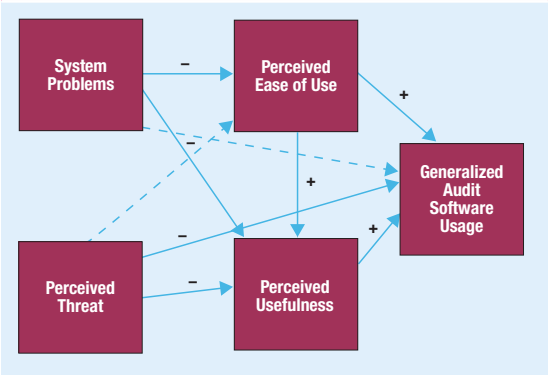
Characteristic	Number	Percentage
Length of time in audit profession		
• More than 15 years	88	32%
• 10–14 years	50	18%
• 5–9 years	90	32%
• 0–4 years	49	18%
Length of time using GAS		
• More than 10 years	38	14%
• More than 6 years and up to 10 years	64	23%
• More than 2 years and up to 6 years	110	40%
• Two years or fewer	59	21%
• Did not answer	6	2%
Industry		
• Public accounting	81	29%
• Banking and finance	46	17%
• Government and nonprofit	45	16%
• Health care	21	8%
• Higher education	15	5%
• Manufacturing	14	5%
• Professional services	16	6%
• Other	30	11%
• Did not answer	8	3%
Role on audit team		
• Financial auditor	122	44%
• Operational auditor	66	24%
• IT auditor	89	32%
Type of auditor		
• Internal	163	60%
• External	114	40%
GAS software used by auditors*		
• IDEA	217	66%
• ACL	69	21%
• ActiveData for Excel	17	5%
• MS Tools	12	4%
• Other	13	4%

*The total adds to more than 277, as some auditors used more than one GAS software package.

Factors Affecting Generalized Audit Software Use

Figure 2 illustrates both barriers and enablers of GAS use for auditors. This model is not meant to be comprehensive, but it is a starting point for considering what affects GAS usage in an audit. The survey had multiple questions to measure each of the factors shown in **figure 2**. Bold lines in the model indicate that the factor affects GAS use, whereas a dashed line indicates that the factor does not affect GAS use; the direction found in the study is indicated with a plus (+) sign, indicating it encourages use, or minus (-) sign, indicating it discourages use.

Figure 2—Barriers and Enablers of GAS Usage



The survey included eight questions describing common uses of GAS in the audit (**figure 3**, which ranks the uses from highest to lowest per audit role). Interestingly, across the financial, IT and operational audit roles, GAS is used mainly for sampling during an audit, followed by data mining. Conversely, the least used application of GAS across the three audit roles is regression analysis, followed by calculating ratios.

The study results revealed that two established factors in prior research encourage GAS usage: perceived ease of use and perceived usefulness.

Figure 4 reveals that, across audit roles, financial auditors perceive GAS as less easy to use than the other audit roles do. The means across audit roles for perceived usefulness (**figure 5**) show that, overall, operational auditors perceive GAS as the most useful.

When discussing GAS, perceived ease of use has been shown to have a positive influence on the use

Figure 3—Uses of GAS in an Audit

Respondents were asked to rate the following statements on a scale from "strongly disagree = 1" to "strongly agree = 7."	Financial Auditor Mean	IT Auditor Mean	Operational Auditor Mean
I use generalized audit software for retrieving information from a database.	5.44	5.44	5.47
I use generalized audit software for calculating ratios during an audit.	3.32	4.61	3.83
I use generalized audit software for recalculation of data during an audit.	5.28	5.58	5.15
I use generalized audit software for audit sampling during an audit.	**6.36**	**5.91**	**6.12**
I use generalized audit software for detecting fraud during an audit.	5.27	5.65	5.55
I use generalized audit software for data mining during an audit.	5.76	5.89	6.07
I use generalized audit software for regression analysis during an audit.	**3.21**	**4.09**	**3.44**
I use generalized audit software for substantive testing during an audit.	5.53	5.63	5.64
I use generalized audit software controls for testing during an audit.	4.39	5.55	5.40

Legend
Most used GAS application
Least used GAS application

Figure 4—Perceived Ease of Use

Respondents were asked to rate the following statements on a scale from "strongly disagree = 1" to "strongly agree = 7."	Financial Auditor Mean	Operational Auditor Mean	IT Auditor Mean
Using generalized audit software is not difficult.	5.11	5.37	5.41
Overall, I believe that generalized audit software is easy to use.	5.11	5.25	5.29

Source: D. Henderson, M. Bradford, A. Kotb. Reprinted with permission.

Figure 5—Perceived Usefulness

Respondents were asked to rate the following statements on a scale from "strongly disagree = 1" to "strongly agree = 7."	Financial Auditor Mean	Operational Auditor Mean	IT Auditor Mean
Using generalized audit software improves the quality of work I do.	5.98	6.04	5.97
Using generalized audit software makes it easier to do my job.	5.97	5.93	5.89
Using generalized audit software improves my job performance.	5.89	6.04	5.86
Overall, generalized audit software is useful in my job.	6.18	6.28	6.15

of GAS among auditors.[14] In addition, the strong positive influence of perceived usefulness has been shown to be quite significant in the context of GAS[15, 16, 17, 18, 19] and is the single most important predictor among accountants of technology acceptance.[20, 21, 22]

The survey obtained open-ended responses as to why others might "feel differently" about these two factors. One financial auditor stated, "Many think GAS is difficult to use. Also, many don't realize how much the software can do. Most of this has to do with lack of training." Additionally, an IT auditor noted, "Financial and operational auditors tend to

Enjoying this article?

- **Learn more about, discuss and collaborate on audit tools and techniques in the Knowledge Center.** *www.isaca.org/it-audit-tools-and-techniques*

think the time required to use GAS does not justify any benefits." Another financial auditor held the opinion that "[GAS] is seen as too expensive and too time consuming to train all of the staff. The decision is short sighted." One operational auditor shared that "IT auditors generally have other tools that can do the same data manipulation." Another operational auditor stated, "IT auditors are used to having query options using Structured Query Language (SQL), so [they] may not find generalized auditing software helpful."

System problems are also shown to be a significant barrier to GAS use. In past research, slow system response times have been one such barrier because they indicate to the user that something is wrong and they threaten the user's perception of the system as a whole.[23]

Regarding the use of GAS, some issues that signal system problems include difficulty extracting data, lack of system documentation and failure of the GAS to work as promised.

As stated earlier, barriers may well discourage GAS usage when they are present, but they do not necessarily encourage usage when they are absent. Having difficulty extracting data would likely affect GAS usage negatively. Ease of data extraction, on the other hand, would not automatically increase system usage because users expect that of a system. Based on the means for all of the audit roles (especially financial) shown in **figure 6**, it appears that data extraction problems represent the most salient barrier to GAS usage. Additionally, IT auditors perceive that documentation provided by vendors is not sufficient, likely because they are using GAS for more advanced purposes. However, overall, IT auditors perceive fewer problems with using GAS. According to one respondent, "IT auditors seem to be more comfortable using it than the other two groups. They evidently understand how to use it better than the other two groups or grasp the concepts and retain them better."

Respondents cited perceived system problems with GAS. Among them, an IT auditor stated, "Those who have not previously used generalized audit software and rely on spreadsheet or database software tend not to trust GAS, think that GAS is too hard to learn and think that it will impact audit time frames." Another IT auditor mentioned that "financial auditors have the perception that using GAS requires technical skills and, hence, it is only useful to IT auditors. However, GAS could be used by all types of auditors once they understand the functionality and what can be done using them." A financial auditor stated that while some auditors use the software willingly and as intended, "outliers will see it as too complicated to use sufficiently."

> **"Barriers may well discourage GAS usage when they are present, but they do not necessarily encourage usage when they are absent."**

Another significant barrier to GAS use is perceived threat. In the study, perceived threat is defined as the extent to which auditors believe that using GAS threatens their ability to perform audit procedures or the extent to which they feel a loss of power or control over the work. An important early paper on the subject found that accountants resisted adopting a new financial system because they believed they would lose control over their data and lose power within their organization.[24] The paper concluded that the new system represented a threat to employees due to a perceived loss of control, potentially resulting in workarounds, sabotage of the system or outright rejection.[25]

Figure 6—System Problems			
Respondents were asked to rate the following statements on a scale from "strongly disagree = 1" to "strongly agree = 7."	Financial Auditor Means	Operational Auditor Means	IT Auditor Means
Generalized audit software is too slow to be useful.	2.09	2.01	1.94
Generalized audit software frequently does not work the way it should.	2.38	2.25	2.29
Generalized audit software does not provide enough documentation to effectively use.	2.44	2.33	2.56
The data required for using generalized audit software cannot be easily extracted.	3.16	2.90	3.03

The idea of perceived threat was reinforced in a study concluding, "When a system is introduced, users will first assess it in terms of the interplay between its features and their abilities or needs. They will then make projections about the consequences of its use. If anticipated conditions are threatening (for instance, a change to how they perform their job), resistance behaviors will result."[26] The means across audit roles for perceived threat in **figure 7** are low compared to the other factors in the model, which suggests that, although it is significant, auditors do not think GAS use interferes with their ability to perform their duties as much. IT auditors have the lowest sense of threat from using GAS.

One operational auditor surveyed noted that older, non-IT-savvy professionals tend to feel more threatened by new software tools, saying, "I think it depends on what generation they are from." Another respondent made this point: "If an auditor is not comfortable with the analytical thinking required to successfully apply generalized audit software, they'll tend to want to apply methods where they are in total control and the generalized audit software isn't computing 'behind the scenes'." An IT auditor noted, "Those who have not previously used generalized audit software and rely on spreadsheet or database software tend to not trust generalized audit software, as their spreadsheet/database formulas are 'tried and true' (even if the formulas are inaccurate)."

These results point to a need for management to incorporate education, training and communication when adopting GAS. As part of a change management strategy, education is a key part of adopting any new technology. It can demonstrate the "why" of the technology's utility.

After education comes training, which serves as the "how" in adopting the technology. Training may also serve as a response to negative feelings regarding the technology. Finally, management must communicate support for GAS usage to reduce negative perceptions toward the software.[27] Communication should relay essential information on why GAS can be useful in the audit. However, communication should be a two-way street. Employees should be solicited for feedback on their concerns about the technology and should feel comfortable asking questions and expressing their concerns about its use.[28]

Figure 7—Perceived Threat			
Respondents were asked to rate the following statements on a scale from "strongly disagree = 1" to "strongly agree = 7."	Financial Auditor Means	Operational Auditor Means	IT Auditor Means
I may lose control over the way I work if I continue to use generalized audit software.	1.95	1.94	1.79
I may lose control over the way I perform audit procedures if I continue to use generalized audit software.	1.97	2.00	1.84

Internal vs. External Auditors

Because internal and external auditors have different responsibilities, they may perceive the relevance and importance of GAS differently. Prior studies show that internal auditors and external auditors work with GAS to different purposes and extents and may have different perceptions.[29] The authors were curious about whether the survey results supported this dichotomy, so the sample was split into these two groups and analyzed separately. The results show that, indeed, internal and external auditors perceive GAS in different ways. A major difference is that internal auditors perceive more of a threat from using GAS than external auditors and, thus, may be especially sensitive to the introduction of GAS. According to one respondent, "Internal auditors are generally more resistant as they do not see how it applies to operations, but consider it more relevant for financial calculations." Another respondent noted, "From an IT auditor's perspective, this is the biggest hurdle in getting data analysis started and used on a regular basis in an internal audit function." In IT-dependent environments, auditors must maintain sufficient knowledge of IT, which includes GAS.[30] Internal auditors, who do not maintain their knowledge of IT, including GAS, may not be able to advance their careers in new assignments and better positions.

Splitting the data also showed that system problems are more salient for external auditors than for internal auditors. According to one respondent, "I think [external] financial auditors are hesitant to adopt something new, primarily because the Big 4 accounting firms are so focused on doing things the same way over and over and not adapting."

Discussion and Conclusion

According to the study's results, negative factors affect GAS usage and bias enablers. In looking at **figure 1**, it can be seen that both barriers (system problems and perceived threat) affect enablers of ease of use and usefulness and also usage directly (exceptions are shown with dotted lines). Determining perceived threat to be significant reaffirms the findings of the study,indicating that auditors may be resistant to GAS usage because they believe that it threatens the way they are accustomed to conducting audits and that it threatens the use of tools they are already comfortable with and trust.[31] Overcoming these negative barriers may, therefore, be necessary if positive factors are going to substantially affect GAS usage.

Other findings show that:

- Factors that inhibit usage continue to be significant even post-adoption.
- Organizations should invest in training and other change management practices that mediate all types of barriers to using GAS.
- Barriers to GAS use are affected by the role of the auditor—that is, internal vs. external auditor.

GAS usage among auditors remains low. This study may be of use to software vendors and auditing firms in promoting the usage of GAS among all types of auditors. Software trainers should understand the relevance of perceived threat, especially concerning loss of job control, and emphasize that GAS adds to, rather than replaces, auditors' functions and duties. Organizations should supplement technical training (with an emphasis

on extraction of data for analysis) with appropriate change management practices to decrease resistance to change. Sponsorship, coaching, communication and training are all important if GAS is to be integrated into the audit. Also, proactive resistance management is part of any change management program. This entails identifying the source of resistance early on and how objections for using GAS can be answered before they manifest themselves and become engrained in the culture of the organization.[32] IT auditors in the survey sample, whether internal or external, were seen as being more confident with GAS, and one stated, "IT auditors are more apt to utilize generalized audit software as it was fully intended."

> **"Because internal and external auditors have different responsibilities, they may perceive the relevance and importance of GAS differently."**

On a positive note, survey respondents appear to believe that GAS is useful and easy to use. Trainers can use these results as evidence of the positive aspects of using GAS, especially when emphasizing that GAS enhances, rather than substitutes, auditor functions.

Endnotes

1 Bierstaker, J.; D. Janvrin; D. J. Lowe; "What Factors Influence Auditors' Use of Computer-assisted Audit Techniques?," *Advances in Accounting*, vol. 30, iss. 1, 2014, p. 67–74

2 Curtis, M.; E. Payne; "Modeling Voluntary CAAT Utilization in Auditing," *Managerial Auditing Journal,* vol. 29, iss. 4, 2014, p. 304–325

3 Debreceny, R.; S. Lee; W. Neo; J. Toh; "Employing Generalized Audit Software in the Financial Services Sector: Challenges and Opportunities," *Managerial Auditing Journal,* vol. 20, iss. 6, 2005, p. 605–618

4 Janvrin, D.; J. Bierstaker; D. Lowe; "An Examination of Audit Information Technology Use and Perceived Importance," *Accounting Horizons,* vol. 22, iss. 1, 2008, p. 1–21

5 Payne, E. A.; M. B. Curtis; *Can the Unified Theory of Acceptance and Use of Technology Help Us Understand the Adoption of Computer-aided Audit Techniques by Auditors?*, USA, 2010

6 *Op cit*, Janvrin, Bierstaker, Lowe

7 *Op cit*, Payne, Curtis

8 Cenfetelli, R.; "Inhibitors and Enablers as Dual Factor Concepts in Technology Usage," *Journal of Association for Information Systems*, vol. 5, iss. 11, 2004, p. 472-492

9 Goode, S.; "Something for Nothing: Management Rejection of Open Source Software in Australia's Top Firms," *Information and Management*, vol. 42, iss. 5, 2005, p. 669–681

10 Cenfetelli, R.; A. Schwarz; "Identifying and Testing the Inhibitors of Technology Usage Intentions," *Information Systems Research*, vol. 22, iss. 4, 2011, p. 808–823

11 *Op cit*, Cenfetelli 2004

12 Bhattacherjee, A.; N. Hikmet; "Physicians' Resistance Toward Healthcare Information Technology: A Theoretical Model and Empirical Test," *European Journal of Information Systems,* vol. 16, iss. 6, 2007, p. 725–737

13 *Op cit*, Cenfetelli 2011

14 Kim, H. J.; M. Mannino; R. Nieschwietz; "Information Technology Acceptance in the Internal Audit Profession: Impact of Technology Features and Complexity," *International Journal of Accounting Information Systems,* vol. 10, iss. 4, 2009, p. 214–228

15 *Op cit*, Bierstaker

16 Braun, R.; H. Davis; "Computer-assisted Audit Tools and Techniques: Analysis and Perspectives," *Managerial Auditing Journal,* vol. 18, iss. 9, 2003, p. 725–731

17 *Op cit,* Curtis

18 *Op cit,* Kim

19 Mahzan, N.; A. Lymer; "Examining the Adoption of Computer Assisted Audit Tools and Techniques: Cases of Generalized Audit Software Use by Internal Auditors," *Managerial Auditing Journal,* vol. 29, iss. 4, 2014, p. 327–329
20 Bedard, J.; C. Jackson.; M. L. Ettredge; K. M. Johnstone; "The Effect of Training on Auditor's Acceptance of an Electronic Work System," *International Journal of Accounting Information Systems*, vol. 4, iss. 4, 2003, p. 227-250
21 *Op cit,* Bierstaker
22 *Op cit*, Cenfetelli 2011
23 Loraas, T.; C. J. Wolfe; "Why Wait? Modeling Factors That Influence the Decision of When to Learn a New Use of Technology," *Journal of Information Systems*, vol. 20, iss. 2, 2006, p. 1–23
24 Markus, M. L.; "Power, Politics, and MIS Implementation," *Communications of the ACM*, vol. 26, iss. 6, 1983, p. 430–444
25 *Ibid.*
26 LaPointe, L.; S. Rivard; "A Multilevel Model of Resistance to Information Technology Implementation," *MIS Quarterly*, vol. 29, iss. 3, 2005, p. 461
27 Curtis, M.; J. G. Jenkins; J. Bedard; D. Deis; "Auditors' Training and Proficiency in Information Systems: A Research Synthesis," *Journal of Information Systems*, vol. 23, iss. 1, 2009, p. 79–96
28 Robert Half Management Resources, "Time for Change: 5 Basic Tenets of Change Management," 16 March 2015, *http://roberthalf.com/management-resources/blog/time-for-change-5-basic-tenets-of-change-management*
29 *Op cit*, Debreceny
30 Kotb, A.; A. Sangster; D. Henderson; "E-business Internal Audit: The Elephant Is Still in the Room!" *Journal of Applied Accounting Research*, vol. 15, iss. 1, 2014, p. 43–63
31 *Op cit,* Markus
32 Prosci, *Five Levers of Organizational Change Management, https://www.prosci.com/change-management/thought-leadership-library/five-levers-of-organizational-change-management*

Addressing Shared Risk in Product Application Vulnerability Assessments

Service organizations with a bespoke application in a regulated industry have special challenges in addressing application vulnerabilities. At one vendor that hosted an application containing sensitive data, fixes were not deployed to the clients' systems in a timely fashion despite there being little technical impediment. When the service provider's risk team ultimately found the key to getting security fixes accepted, it was in a nuanced appreciation of risk—specifically, the risk of appearing negligent.

The Problem

Application vulnerabilities have both proximate and secondary risk factors. The proximate risk factors are obvious—data breaches impact the affected individuals whose personal information is compromised. But the secondary risk lies in the legal exposure to the client organization, i.e., risk for which the technology service organization—whose product allowed the breach—would be responsible. Data breaches frequently give rise to legal action, i.e., action that is often rooted in negligence. As of 2016, 75 percent of cases arising from a data breach include negligence.[1] In a legal sense, negligence is defined as "a breach of duty to take proper care."[2] Negligence can be determined with some simple questions:

- Does a duty of care exist between the parties?
- Has that duty of care been breached by the offending party?
- Has damage resulted from that breach?

The definition of "duty of care" changes based on the jurisdiction. In most of the Commonwealth, it is a three-part test. "Harm must be reasonably foreseeable as a result of the defendant's conduct, the parties must be in a relationship of proximity, and it must be fair, just and reasonable to impose liability."[3] In some US jurisdictions, the first test alone determines duty of care; in others, it is absent.[4]

While an exhaustive review of how this subject is applied in different jurisdictions is beyond the scope of this article (and, quite frankly, the author), the salient point is this: However the duty is legally defined, a service provider has a responsibility to secure information, and a breach of that responsibility opens the provider to a liability rooted in negligence. Regulators have, for years, been active in enforcing due care in the case of data breaches. The US Federal Trade Commission, for instance, speaks of filing some 60 actions against "companies that put consumers' personal data at unreasonable risk."[5] It is, therefore, imperative that the providers of an application containing any form of sensitive data in a regulated environment understand the local legal and regulatory implications.

In the case of the technology service provider in this article, relevant regulators include the Canadian

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2tRkr5R

Michael Werneburg, CIA, PMP
Is a technology risk practitioner in Toronto, Ontario, Canada. In a 23-year career spanning three continents, he has worked with firms ranging from small start-ups to some of the world's largest financial institutions. His passion is leveraging risk to effect change across technology organizations.

Office of the Superintendent of Financial Institutions (OSFI), which considers such relationships materially important to the stability of federally regulated financial institutions.[6] Industry-specific legislation such as the US Gramm-Leach-Bliley Act (finance) and the US Health Insurance Portability and Accountability Act (HIPAA) explicitly dictate the controls and practices by which data are meant to be secured. In 2016, the attorney general's office of California clarified a specific set of controls as its standard for reasonable security.[7]

> **"Even within a service organization, it is not always easy to obtain permission to approach a client concerning necessary security fixes."**

Leading back to an application vulnerability, regulatory requirements and service audit regimes (such as the ubiquitous Service Organization Control [SOC] 2) dictate that an application vulnerability scan is performed no less than annually. They also require that the report be shared with the client. By the time a breach has occurred, the technology provider and its clients all have these annual reports in hand. By that time, it is hard to avoid the appearance of negligence if the vulnerabilities documented in those reports have not been addressed in a timely fashion, especially when those vulnerabilities are shown to put sensitive information assets at risk.

Who Does Not Want Application Fixes?

If it sounds odd that application stakeholders would not want security fixes, it is worthwhile to look at how regulated industries behave. In this example, the service provider was active in the wealth management sector. That sector typically has a conservative approach to change, strong regulatory oversight, and—when it comes to releasing software—a focus on business features over nonfunctional factors. In such an environment, the service provider cannot dictate the nature or timing of a security release, regardless of who hosts the application.

First, it is not always easy for a service provider to explain the necessity of security fixes to the client stakeholder responsible. Client stakeholders who typically manage the relationship with a service provider and who decide on and schedule expensive test-and-release procedures may not appreciate or comprehend security fixes in the first place. Frequently, the parties making these decisions have priorities relating to functional requirements—what the application does for the organization—and are not rewarded for venturing into activities that deal with nonfunctional requirements. That makes those decision makers hard to motivate through describing security fixes in terms of abstract scenarios and recent vulnerabilities. A service organization's risk team might find themselves going to great lengths, discussing the finer points of medium-priority findings vs. high or critical. Or if they finally convince the stakeholders of the urgency of a fix, they might discover that a freeze has been introduced or that the client's budget for testing and deployment is not there.

Even within a service organization, it is not always easy to obtain permission to approach a client concerning necessary security fixes. Plenty of stakeholders within the service organization have conflicting objectives, perhaps involving delivering new features, containing support costs or managing client relationships that are in a sensitive phase. In almost all cases, the service organization views its clients' budgets as finite, and many priorities compete for the same budget and not all demands can be met. The product owner, the account representative, the overworked software development and software quality assessment teams, budget oversight, and even the support team that was burned for a failed security patch

deployment years prior can stop security patches from heading to clients—and they often do.

Supposing the risk team overcomes internal resistance and finds the right parties to work with on the client side, they will still have to deal with the slow-moving nature of regulated clients. Universally, clients will only accept a release once they have conducted their own acceptance testing. Any application release testing can take a great deal of effort, scheduling and expense on their part. But security fixes, with their nonfunctional nature, can be notoriously difficult for a software quality assurance function to properly regression test, and fixes sometimes require a test environment that meticulously matches the production environment. The release process at cautious, regulated firms is, likewise, highly risk-averse and demands exhaustive release notes. And again, security fixes can be hard to explain to the satisfaction of such stakeholders—especially when it comes to proving that no unintended side effects lie dormant.

And yet, that shared risk of being found negligent after a breach does not go away on its own.

Leveraging Risk

After trying for years to use logic to schedule security fixes, the risk team finally found a way to address security using the industry's risk-averse culture in its favor. Working with the service organization's executive team, the risk team developed a three-step process that focused not on vulnerabilities and impacts, but on the underlying risk inherent in the relationship: the potential legal and regulatory impacts and the relevance of negligence to the conversation.

Implementing this three-step process began as soon as the annual third-party application vulnerability assessment report was in the service provider's hands. The three steps are:

1. Work with the service organization's application developers, the project management office and the delivery team to develop estimates of:
   - The complexity of the technical fixes
   - Possible impacts to the users from the fixes, if deployed
   - Possible schedules for fix delivery

   At the enterprise mentioned previously, this step helped ensure the buy-in of internal stakeholders. It also helped the risk team filter out issues that could not be fixed for technical reasons, false positives and issues for which fixes were already in the pipeline. And it helped the clients understand the context of the third-party report.
2. Write an interpretation of the assessment report that is rich in application context and, therefore, easy for clients to understand; include impact assessments and potential schedules; and frame the vulnerabilities in terms of the joint losses that could arise from negligence if the fixes are not addressed in a timely fashion. A custom report should go to each client featuring only those portions of the scan report that impact their version of the bespoke application. This enables client-side stakeholders other than information risk personnel to understand the issues, properly weigh priorities and encourage their active participation in the conversation as informed parties.
3. Discuss the service provider's report with each client and request a signature acknowledging the report.

"But security fixes, with their nonfunctional nature, can be notoriously difficult for a software quality assurance function to properly regression test."

It was this final step that drove home the risk to the application owner on the client side: They were being asked to acknowledge risk on behalf of their employer. Acknowledging the risk is not the same as accepting it, as the conversation that followed proved. In that conversation, the client interpreted signing the report as an act of actively seeking advice on which risk they felt they had to live with and

Enjoying this article?

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

which should be mitigated with fixes. This led to a discussion of which fixes to prioritize and how soon the service organization could get those scheduled.

In this scenario, the risk team had normalized the process of securing security fix releases. As a result, what would follow would be a business-as-usual addition of new releases to the service organization's workload.

This process is not one that should be developed after the service has entered production. It should be enshrined in the contract between the technology service provider and its clients. Sources such as the Open Web Application Security Project (OWASP)[8] have published thorough guidance on contractual language relating to the inclusion of product security in the software development and delivery life cycle. Some of these requirements include:

- A recognition by the client that they are bound to participate in the process of approving fixes arising from application vulnerability scans
- A recognition that those fixes will be released according to an agreed-upon schedule

Doing so from the outset eliminates the objections, any ambiguity in terminology and all of the other drag experienced by the service organization.

Conclusion

The vendor in the wealth management sector discussed in this article took years to find a way to assure the release of application vulnerability scans. At issue was the culture of the sector in which it was engaged. The culture had:

- A conservative approach to change
- Strong regulatory oversight that places a heavy emphasis on third-party risk arising from technology service provider relationships
- A strong focus on business features over nonfunctional factors such as security

The risk team ultimately found a way to leverage the first characteristic against the latter two. Even in the most change-adverse environments, responsible parties realize that it is hard to justify accepting an increment of risk of being found negligent for the purpose of sparing the organization some inconvenience and routine expense associated with resolving application security issues.

Endnotes

1 Bryan Cave LLP, *2016 Data Breach Litigation Report*, 6 April 2016, *https://www.bryancave.com/en/thought-leadership/2016-data-breach-litigation-report.html*
2 Duhaime's Law Dictionary, "Negligence Definition," *www.duhaime.org/LegalDictionary/N/Negligence.aspx*
3 e-lawresources.co.uk, "Negligence—Duty of Care," *http://e-lawresources.co.uk/Duty-of-care.php*
4 *Ibid*.
5 Federal Trade Commission, *Privacy and Data Security Update (2016),* USA, January 2017, *https://www.ftc.gov/reports/privacy-data-security-update-2016#how*
6 Canadian Office of the Superintendent of Financial Institutions, *Outsourcing of Business Activities, Functions and Processes*, May 2001, *www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx*
7 Harris, K.; *California Data Breach Report 2012-2015*, February 2016, *https://oag.ca.gov/breachreport2016*
8 Open Web Application Security Project, "OWASP Secure Software Contract Annex," *https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex*

Anatomy of an IoT DDoS Attack and Potential Policy Responses

In recent years, the impact and frequency of cyberattacks have significantly increased, from millions of personal records compromised to hundreds of millions and even a billion records in the case of Yahoo.[1] This has put both personal wealth (e.g., in the case of bank accounts, insurance information) and potentially human life (in the case of the US Office of Personnel Management hack, where personal information—including that of secret agents—was compromised, putting them at physical risk)[2] at risk on an unprecedented scale.

Meanwhile, the threat vector in the form of Internet-connected devices (Internet of Things [IoT]) has been utilized by hackers more extensively to direct extremely large distributed denial-of-service (DDoS) attacks at targeted companies to bring down their services. The strong emergence of the IoT threat vector needs to be properly understood in deliberations on the right type of policy and technology response to create defenses to protect data and systems. This article discusses popular definitions of IoT; current and future proliferation levels; a high-level anatomy of an IoT attack—in this case, the DYN attack; the business case for legislation; and the level and type of organized government intervention that may (unfortunately) be required.

What Is IoT and How Big Will It Get?

An interesting definition of IoT comes from the European Telecommunications Standards Institute (ETSI). It refers to IoT as "a dynamic global network infrastructure with self-configuring capabilities, where physical and virtual 'things' have identities, physical attributes and virtual personalities, and use intelligent interfaces to connect both between themselves and to data networks."[3] Additionally, the International Telecommunication Union (ITU) definition of IoT can be found in its recommendation ITU Y.2060. It states that an IoT "is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks."[4]

Some examples of IoT devices include smart home applications such as Internet-connected thermostats, smoke alarms, Wi-Fi and electric bulbs. Internet-connected automobiles (e.g., the Tesla car) is another popular example.

Virtually every appliance and device can potentially be connected to the Internet. PricewaterhouseCoopers (PwC) research predicts that by the year 2020, anywhere between 30 to 50 billion devices will be connected to the Internet.[5] Such high levels of Internet proliferation can be incredibly beneficial to individuals, businesses and society at large by automating mundane jobs or making jobs more efficient and safe. It also provides a platform for innovation when combined with advancements such as cloud computing, robotics and smart grids, which renders the number of innovation permutations infinite. By 2020, the

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2vf0bNz

Hari Mukundhan, CISA, CISSP
Has 15 years of extensive cyber security, IT audit, IT operations, project and program management experience across a wide range of clients and businesses. He is currently a cyber security manager in a leading private organization. He can be reached at harimukundhan@yahoo.com.

global annual economic potential realized through productivity and innovation from machine and machine communication across all sectors will range from US $1.4 trillion to US $14.4 trillion.[6]

> **"With great proliferation comes greater concerns about whether these devices can be leveraged to expose behavior patterns, compromise physical safety and security, or even launch an Internet attack on a given target."**

With great proliferation comes greater concerns about whether these devices can be leveraged to expose behavior patterns, compromise physical safety and security, or even launch an Internet attack on a given target. For example, an innocuous-looking Wi-Fi-connected light bulb can be made to talk to another connected light bulb and both can be enslaved to launch a DDoS attack. One such attack that happened in 2016 almost brought down the Internet.

Anatomy of a Recent Cyberattack Using IoT Devices

On 21 October 2016, at approximately 6:00 am CST (UTC -6), Internet users in the eastern portion of the United States were unable to access some of the top and most visited sites such as Twitter, PayPal and Amazon. This was due to a coordinated DDoS attack[7] on DYN, a domain name service (DNS) company. At a high level, DNS resolves website names to IP addresses at the back end, while hiding the complexities from the end user. Without DNS, users would have to remember the IP address for a website instead of the website name itself (a much more difficult prospect).

While DDoS attacks have been happening for a long time, what was peculiar about the attack on DYN was the size of the attack (which was unprecedented in its scale and seriousness), how it was attacked and, more importantly, why it was attacked.

A typical denial-of-service (DoS) attack overwhelms the web server resources with so many requests from one computer connected to the Internet—for example, a flood of Internet Control Message Protocol (ICMP) ping requests—that the server is so busy responding to the pings that it does not have enough resources to respond to legitimate requests from users and, thus, returns an error message (e.g., 404 Page Not Found). This may make an organization unable to offer its services to its customers, leading to potentially significant financial, operational, reputational and legal risk.

On a larger scale, if the attacker uses not just one computer, but thousands of unique IP addresses, it is considered to be a distributed DoS, or DDoS, attack. In terms of numbers, an average DDoS attack size, according to an Arbor Networks study, was 986 Mbps in the first half of 2016, with the largest attack clocking in at 579 Gbps.[8] It is worthwhile to note that an attack of one Gbps is considered large enough to take most organizations offline. At such high volumes, it is also quite difficult to discern which IP address is legitimate and which is not, making it that much more difficult to fend off.

TCP SYN Flooding

So, what is a DDoS attack? One of the more common types of DDoS attack is TCP SYN flooding,[9] which exploits an inherent vulnerability in the Transmission Control Protocol (TCP),[10] a set of rules to establish and maintain a reliable conversation between two computers over the Internet.

When one computer (a client, e.g., a laptop), attempts to connect to another computer (a server, e.g., a website), a series of messages, or data packets, is first exchanged between the two to establish reliable connectivity over the Internet.

First, the client requests a connection to the server via a SYN message. The server then acknowledges the

request via the SYN-ACK message back to the client. The client then responds back with an ACK message, thereby establishing a connection between the client and the server, i.e., a laptop and a website. This is called a TCP three-way handshake (**figure 1**).[11]

In the case of TCP SYN flooding, the client sends the SYN message and receives a SYN-ACK from the server, but does not respond back to the server with an ACK message. The server waits for the ACK message for some time before moving on. However, precious server resources are consumed during this process and, during that time, while it waits for the ACK message, it cannot respond to legitimate requests from other clients. If the number of such client requests exceeds a server's capacity to process them, the server is overwhelmed and will become unavailable, i.e., it denies service to the users (DoS).

Another variant of this attack is the client falsifying its IP address (also knowns as IP spoofing) so that the server sends a SYN-ACK to the spoofed IP address in the original SYN message it received, and the spoofed IP address never responds with an ACK message because it never sent a SYN message to the server in the first place. In the case of the DYN attack, it is not entirely clear what type of DDoS attack was launched, but the Mirai botnet, a cluster of 100,000 or so compromised and enslaved IoT devices, was configurable to deliver different types of DDoS attacks, including TCP SYN flooding.[12]

Attack Delivery Model—Mirai Botnet

As defined by Kaspersky Labs, "The word Botnet is formed from the words 'robot' and 'network.' Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer and organize all of the infected machines into a network of 'bots' that the criminal can remotely manage."[13]

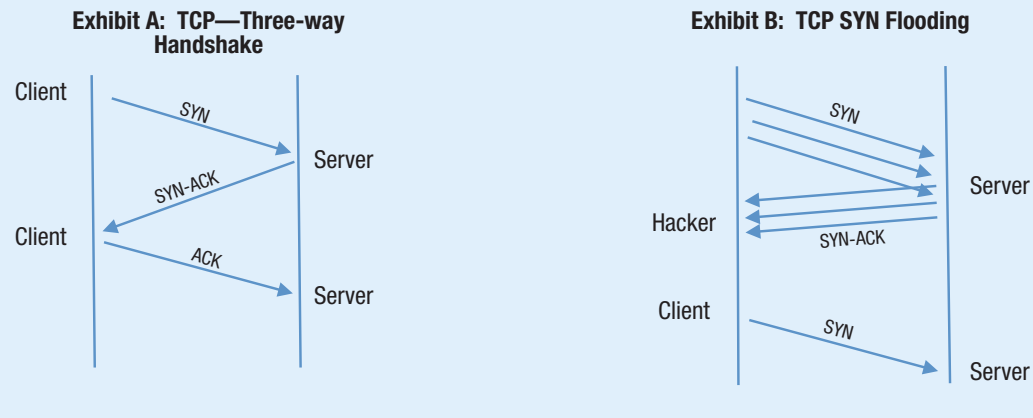
The key features of the Mirai botnet are that the source code was designed to recruit hundreds and thousands of IoT devices and the source code was released[14] a few days before it was used[15] for the DYN attack. DYN disclosed that probably 100,000 IoT devices[16] (scaled down from tens of millions), such as digital video recorders and closed circuit television cameras, were used for the attack. Moreover, it was simplified to a point that script kiddies launched the attack, not advanced persistent threats, such as state actors, that people usually tend to imagine.

DDoS as a Service: Threat Capability, Motives and Likely Frequency

So, what does the DYN attack mean to the Internet? What were the attackers' motives? How capable is the botnet/IoT DDoS threat, and how frequent and large can it become?

The Mirai botnet's source code is now being incorporated into 12 other botnets since the

Figure 1—A Typical TCP Three-way Handshake



Enjoying this article?

- Read ***Internet of Things: Risk and Value Considerations.*** *www.isaca.org/internet-of-things*
- **Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center.** *www.isaca.org/information-security-policies-and-procedures*

code was released. Botnets will now be readily available to provide DDoS services for customers with malicious intent.[17] As the number of available IoT devices increases, perpetrators will have that many more devices to enslave via readily available botnets[18] or DDoS services with which they can launch unprecedented attacks.

The motivations to launch an attack are numerous. They can range from an enemy country launching an attack for political reasons to a competitor or an angry employee launching an attack against a company to a cybercriminal trying to extract ransom from a wealthy company. It could even be a political or cyberwar situation, wherein a state or a nonstate actor with advanced capabilities can carry out a large-scale coordinated attack to bring down access to the Internet for a large number of people.

“As the number of available IoT devices increases, perpetrators will have that many more devices to enslave via readily available botnets or DDoS services with which they can launch unprecedented attacks.”

Market Failure—A Key Cause

IoT products are widely believed to be weak on security, with easily guessable passwords and unsecured ports. Security journalist Brian Krebs reports being able to identify many of the IoT vendors using easily guessable usernames and passwords.[19] Moreover, many vendors do not provide an interface to change passwords nor do they update the firmware, leaving these devices highly vulnerable to attack.

Since there are no statutory or market requirements for IoT vendors to develop secure devices, and since such an effort will surely increase the manufacturing cost, vendors are not competing to create secure products. This can, therefore, be considered a market failure that calls for some level of government intervention to ensure that baseline security for the device is present. To quote the well-respected Bruce Schneier:

> *The market can’t fix this because neither the buyer nor the seller cares. Think of all the CCTV cameras and DVRs used in the attack.... The owners of those devices don’t care. Their devices were cheap to buy, they still work.... The sellers of those devices don’t care: They’re now selling newer and better models, and the original buyers only cared about price and features. There is no market solution because the insecurity is what economists call an externality: It’s an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution.*[20]

Smart Regulations

The success of the Internet is largely due to its openness to collaboration and innovation without government intervention. In the United States, there were no Internet regulations up until 2015, when lawmakers decided to address net neutrality.[21] Therefore, careful thought has to be given to the type and level of government intervention that now appears to be warranted in the IoT space to overcome a market failure while at the same time not stifling innovation.

Following are some of the key aspects to consider when drafting the regulations:

IoT security standards
A minimum baseline of IoT security standards should be introduced, along with a mechanism for vendors to demonstrate compliance with the standard, i.e., certification of compliance. The standards should be internationally applicable and involve all the stakeholders, e.g., government, civil society, IoT vendors, academia and other private companies. But it should also be noted that while having a few security standards would probably raise

the overall security bar, it is definitely not a guarantee against getting hacked. In the United States, active discussions seemed to have kicked off with the US Department of Commerce soliciting feedback[22] on formulating an approach to betterment of IoT. The US Federal Trade Commission (FTC) has basic security guidelines for IoT products.[23]

A few IoT standards and guidelines are emerging:

- IoT Security Guidance by the Open Web Application Security Project (OWASP) provides guidance to help manufacturers build more secure products in the IoT space.[24]
- Strategic Principles for Securing the Internet of Things (IoT), from the US Department of Homeland Security, provides a set of nonbinding principles and suggested best practices to build responsible levels of security in the IoT space.[25]
- Security Solutions, One M2M Technical Specification, defines security specifications in the IoT space.[26]
- The Alliance for Internet of Things Innovation by the European Commission addresses standardization, interoperability and policy issues in the IoT space.[27]
- The Institute of Electrical and Electronics Engineers (IEEE) "has created a number of standards, projects, and events that are directly related to creating the environment needed for a vibrant IoT."[28]

Legal Foundational Components

For standards to be effective, the following legal foundation components need to be established consistently across both buyer and seller markets:

- **Market access laws**—Countries should enact laws that will allow market access only to security-certified products that are in compliance with globally acceptable IoT baseline security standards. However, this has the risk of increasing the cost of the product and putting it out of reach of some or many consumers.
- **Enforcement**—A compromised IoT has the potential to directly impact day-to-day life not only by disrupting routine, but also by posing significant safety risk. Examples include a remotely disabled carbon monoxide detector or a device taking control of a car. In 2015, researchers were able to take complete control of a Jeep Cherokee remotely while it was driving at a high speed.[29] In fact, the DEF CON Hacking Conference has a dedicated section just for car hacking.[30] Given such heightened concerns, the role of enforcing existing and new laws and standards needs to be thought through. Will consumers buy only devices they know are secure? Would they care enough to result in vendors that create unsecure devices being driven out of the market? Will standards, legislation and enforcement be effective to reduce the number of unsecured products in the market? Or will compliant products actually attract the determined hacker who would like to delegitimize the regulations? Only time will provide the answer as the market matures.
- **Product recalls**—After the Jeep Cherokee hack was demonstrated by researchers in *Wired*,[31] Chrysler recalled 1.4 million vehicles to update their software since it posed a significant risk to human lives.[32] That raises questions about what would require a product recall. Would a recall apply to only the products that threaten human safety or health, or should it also apply to products that threaten privacy, national security, etc.? Should product recalls be applied retroactively? For example, if an individual bought an Internet-connected thermostat two years ago and it is not compliant with a newly released regulation, can the person get the product

> **"Since there are no statutory or market requirements for IoT vendors to develop secure devices, and since such an effort will surely increase the manufacturing cost, vendors are not competing to create secure products."**

updated? And if the product's firmware cannot be updated, are there technological solutions available to block such devices from the Internet—and is it even fair and legal to do so? By the way, the complexities of recall may increase as the number of devices multiplies into millions and billions. Many complex concepts need to be taken into consideration while formulating policies.

- **Globally coordinated efforts**—Whatever form the regulation takes, one thing is certain: It has to be a globally coordinated effort. A country can create draconian laws or simply decide to keep IoT open for all, but the threat posed may come from the outside as long as the country decides to stay connected to the Internet in some form. For example, IoT devices may be produced in country A, consumed in country B, enslaved by hackers in country C and used for attacking DNS servers in country D. Therefore, major consumer and producer countries and all major countries that are connected to the Internet should be at the table to create a global framework to define operation in this space.

> **"Major consumer and producer countries and all major countries that are connected to the Internet should be at the table to create a global framework to define operation in this space."**

Conclusion

This is an age in which machine-to-machine communication is expanding significantly, creating new types of cyberrisk or exacerbating existing risk, thus impacting not only privacy and wealth, but also human safety. Such a transformation of the environment requires IS professionals to maintain a solid understanding of the technologies and risk involved so that appropriate levels of controls can be built not only at the IoT product level, to ensure that the product meets an internationally acceptable standard, but also at the organizational network level, to protect against attacks that can be launched by these devices. In addition, global coordination by nation states, professional organizations, standards bodies, corporations, academia and civil society would be required to craft the right level of policy responses to safeguard against this newly emerging attack vector.

Endnotes

1 Goel, V.; N. Perlroth; "Yahoo Says 1 Billion User Accounts Were Hacked," *The New York Times*, 14 December 2016, *https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=1*

2 Hirschfeld Davis, J.; "Hacking of Government Computers Exposed 21.5 Million People," *The New York Times*, 9 July 2015, *https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0*

3 ETSI, "Standards for an Internet of Things: A Workshop Co-organized by EC DG Connect and ETSI," 3-4 July 2014, *www.etsi.org/news-events/events/771-2014-etsi-ec-dg-connect-iot*

4 International Telecommunication Union, "Y.2060: Overview of the Internet of Things," 15 June 2012, *www.itu.int/rec/T-REC-Y.2060-201206-I*

5 Chitkara et al.; "The Internet of Things: The Next Growth Engine for the Semiconductor Industry," PricewaterhouseCoopers, May 2015, *www.pwc.com/gx/en/technology/publications/assets/pwc-iot-semicon-paper-may-2015.pdf*

6 Schindler, H.R., *et al*.; *Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of Things*, RAND Europe, 2013

7 York, K.; "Dyn Statement on 10/21/2016 DDoS Attack," Vantage Point, 22 October 2016, *http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/*

8 Arbor Networks, "Arbor Networks Releases Global DDoS Attack Data for 1H 2016," press release, 19 July 2016, *https://www.arbornetworks.com/arbor-networks-releases-global-ddos-attack-data-for-1h-2016*

9 CERT Software Engineering Institute, "TCP SYN Flooding and IP Spoofing Attacks," 19 September 1996, *https://www.cert.org/historical/advisories/CA-1996-21.cfm?*

10 TechTarget, "TCP (Transmission Control Protocol)," *http://searchnetworking.techtarget.com/definition/TCP*

11 Techopedia, "Three-way Handshake," *https://www.techopedia.com/definition/10339/three-way-handshake*

12 Symantec, "Mirai: What You Need to Know About the Botnet Behind Recent Major DDoS Attacks," 27 October 2016, *https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks*

13 Kaspersky Lab, What is a Botnet?, *https://usa.kaspersky.com/resource-center/threats/botnet-attacks*

14 Krebs, B.; "Source Code for IoT Botnet 'Mirai' Released," Krebs on Security, 1 October 2016, *https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/*

15 Woolf, N.; "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say," *The Guardian*, 26 October 2016, *https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet*

16 Hilton, S.; "Dyn Analysis Summary of Friday October 21 Attack," Vantage Point, 26 October 2016, *http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/*

17 Krebs, B.; "Alleged vDOS Proprietors Arrested in Israel," Krebs on Security, 10 September 2016, *http://krebsonsecurity.com/2016/09/alleged-vdos-proprietors-arrested-in-israel/*

18 Mathews, L.; "World's Biggest Mirai Botnet Is Being Rented Out for DDoS Attacks," *Forbes*, 29 November 2016, *https://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#32473c2f58ad*

19 Krebs, B.; "Who Makes the IoT Things Under Attack," Krebs on Security, 3 October 2016, *https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/*

20 Schneier, B.; "Lessons From the Dyn DDoS Attack," Schneier on Security, 8 November 2016, *https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html*

21 Pagliery, J.; "FCC Adopts Historic Internet Rules," CNNMoney, 26 February 2015, *http://money.cnn.com/2015/02/26/technology/fcc-rules-net-neutrality/index.html*

22 National Telecommunications and Information Administration, *Fostering the Advancement of the Internet of Things*, USA, 12 January 2017, *https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things*

23 Federal Trade Commission, *Careful Connections: Building Security in the Internet of Things*, USA, January 2015, *https://www.bulkorder.ftc.gov/system/files/publications/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf*

24 Open Web Application Security Project, IoT Security Guidance, *https://www.owasp.org/index.php/IoT_Security_Guidance*

25 Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, USA, November 2016, *https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf*

26 OneM2M, *OneM2M Security Solutions*, 1 August 2014, *http://onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf*

27 Alliance for Internet of Things Innovation, *https://aioti-space.org/*

28 Institute of Electrical and Electronics Engineers Standards Association, "Internet of Things," *http://standards.ieee.org/innovate/iot/*

29 Greenberg, A.; "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, 21 July 2015, *https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/*

30 Hern, A.; "Car Hacking Is the Future—and Sooner or Later You'll Be Hit," *The Guardian*, 28 August 2016, *https://www.theguardian.com/technology/2016/aug/28/car-hacking-future-self-driving-security*

31 *Op cit,* Greenberg

32 Goldman, D.; "Chrysler Recalls 1.4 Million Hackable Cars," CNNMoney, 24 July 2015, *http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/*

Can Penetration Testing Tools Help an Audit?

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2uNmQRZ

Sometimes, it can feel as though auditors get the short end of the stick when it comes to the tools available to assist in the work that they do. It seems like they are always strapped for budget to acquire tools, while adjacent professionals such as security operations folks, have a wealth of tools available—many of them freely available—to help support everything from vulnerability scanning to log file analysis to sorting through malware.

However, believe it or not, sometimes these tools overlap with those that might directly advance an audit in certain situations. During a normal audit situation, an auditor requests evidence to establish that given controls are operating effectively. For example, the auditor might, as a system administrator, pull up a configuration screen, request a tool be run and review the output, or he/she might review a report or log file information. There are good reasons why auditors are not usually the ones in front of the keyboard firing off commands, though. Specifically, having the operations (ops) staff actually do the ops work helps preserve the independence of the auditor (i.e., it helps maintain a separation between those performing and those reviewing). Also, quite frankly, those closest to the business systems under evaluation are probably those best able to navigate them.

Ed Moyle
Is director of thought leadership and research at ISACA®. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers, and senior security analyst with Trintech. Moyle is coauthor of *Cryptographic Libraries for Developers* and a frequent contributor to the information security industry as an author, public speaker and analyst.

However, that is in an ideal world. In the real world, depending on the type of audit or assessment being performed, sometimes things do not go as planned and flexibility is required. Consider, for example, the situation where a larger organization is conducting an on-site review of a much smaller (think small or medium-sized business [SMB] or "mom and pop" shop) service provider. Will that SMB have the technical expertise to supply everything the auditor might want? Maybe. But also, maybe not. It is here where, if direct interaction between the examiner and the systems is permissible (not in every situation will it be), getting a little "hands on" on the auditor's part can spare everyone some time and energy.

But where are some good places to find tools that an auditor might need should this situation occur? Sure, they can go out and research on the Internet what they might need in response to a given situation, but that is pretty time consuming. One approach is for auditors to look to catalogs of tools that already exist, are already bundled together in a highly portable format, and can be unpacked and used at a moment's notice.

One fruitful location that has all those properties? Penetration testing (pen testing) Linux distributions. For those who are not familiar with the concept, penetration testing (sometimes referred to as "red team" exercises) is a type of security testing whereby the tester emulates the same methods and tradecraft that would be employed by an adversary against an environment. In essence, testers are trying to get in the same way that an attacker would. To support this type of work, these testers typically employ a specialized testing environment that is "kitted out" with a wide variety of attack tools to accomplish that goal. Over time, specialized Linux distributions have emerged as *de facto* standard options for that environment: distributions such as Kali *(https://www.kali.org/)*, BlackArch *(https://blackarch.org/)* and the Samurai Web Testing Framework *(www.samurai-wtf.org/)*, for example.

If the idea of using a pen testing environment to directly support an audit sounds bizarre, consider the following. These environments are portable, usually being downloadable as a virtual machine image ready to be run on a platform such as VMWare Player or VirtualBox (directly on an auditor's field laptop.) Likewise, they come packaged with hundreds, if not thousands, of versatile tools that can accomplish a wide variety of tasks, many of which are directly applicable to collecting or reviewing evidence needed for an assessment. Will every tool on there be directly applicable to the project the auditor is working on right now? Of course not. But being able to, for example, check an International Bank Account Number (IBAN), search a gigabyte of data for Permanent Account Numbers (PANs) or Social Security numbers (SSNs), rapidly parse log file data, mirror a website, or perform any number of other things with a few keystrokes can greatly increase the efficiency of how evidence is reviewed. And, in some situations, it can help the auditor collect those data in the first place.

"These environments are portable, usually being downloadable as a virtual machine image ready to be run on a platform such as VMWare Player or VirtualBox."

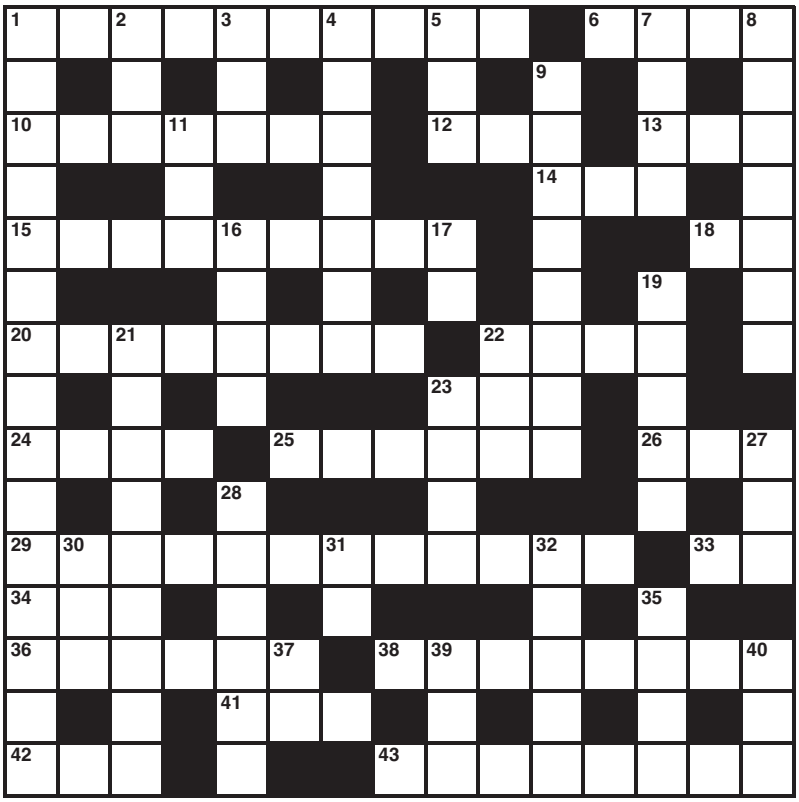
Now, note that no one is saying every auditor needs to go out and become fully versed with every pen testing tool out there. And, as mentioned, care should be exercised and diligence employed when considering directly interfacing with a production system (remember, let the ops folks do ops), but, in the event that it is "give up or do it yourself," doing it yourself can be a useful option.

crossword puzzle

by Myles Mellor
www.themecrosswords.com

ACROSS

1 Data center where companies rent spaces for servers and computing hardware
6 Multimedia signal processing, for short
10 Software that repeatedly reminds a person to pay during a free trial
12 US Data Act, abbr.
13 *The Confidence Code* authors, Katty ____ and Claire Shipman
14 Connect
15 One of the key words in ISACA's definition of information security
18 Loudspeaker system for short
20 Contemplate
22 Internet area accessible only to those with special software where they can remain anonymous, goes with 26 across
23 Intelligence
24 Go over to the other side
25 Actually working as a website or application
26 See 22 across
29 Another keyword in ISACA's definition of information security
33 Branch of engineering related to computers
34 Testing area
36 Taking the place (of), 2 words
38 Set of techniques or tools for process improvement, 2 words
41 Confidentiality agreement, abbr.
42 Green light
43 Used or applied in investigation of facts or evidence in court



DOWN

1 Another keyword in ISACA's definition of information security
2 Fall behind in technological development, e.g.
3 Assessment of controls made by the staff of the unit or units involved, abbr.
4 Establishing layers
5 Not functioning
7 Create
8 Give recompense for, 2 words
9 Lessen the risk or consequences
11 Suffering
16 Main point
17 Year, for short
19 Throws off
21 Items in a calculation that may change or alter in value
22 Badly lit
23 Intention
27 Unit of information
28 Customer
30 Group active in innovation
31 Play __ the book
32 Flavor
35 Long periods of history
37 Dublin University, for short
39 Going public letters
40 Circumference part

Answers on page 58

quiz#174

Based on Volume 3, 2017

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

TRUE OR FALSE

ATLURI ARTICLE

1. Thingbots are botnets of infected Internet of Things (IoT) devices that can be used to launch attacks that are not like the Dyn attack, which affected more than one million devices, of which about 96 percent were IoT devices.
2. If hardware vulnerabilities are not mitigated, the rest of the controls, methodologies, frameworks, time, resources and investment to make IoT devices secure cannot be effective.
3. Like other network devices, the most common IoT device threats at the enterprise/network level are eavesdropping, man-in-the-middle (MiTM) attacks and bandwidth theft.

PATEL ARTICLE

4. Layers including the edge layer may be hosted on-premises or in the cloud.
5. The data layer includes activities such as data ingestion, data engineering and data transformation using Structured Query Language (SQL) or NoSQL technologies with traditional databases/warehouses or big data technologies.
6. Earlier big data technologies offered only file or operating system (OS)-level security and offered lower-level security, for example, Apache Sentry9 with role-based authorization.
7. A strategy can be just monitoring data received from IoT devices, or it can include processing data received from IoT devices and altering the behavior of IoT devices based on acceptable limits of data readings from the devices.

SUBRAMANIAN AND SWAMINATHAN ARTICLE

8. The cost of fixing a defect postproduction is approximately four times more than fixing it in the development stage.
9. When white-box products, whose design and source code are not available, are used, only a standard vulnerability assessment can be performed on the applications or application program interfaces (APIs) in the test phase.
10. The test methodology should consider all use cases pertaining to the complete IoT environment, and every such use case should have one or more misuse case (security test case) associated with it.
11. Unwanted logical and physical ports should be turned off in such devices and servers, and physical security procedures should be tightly employed to recover against attacks such as device/sensor theft, tampering and unauthorized access.

RAJENDRAN ARTICLE

12. Platforms such as iOS and Android—the two most popular mobile platforms today—are immune to the threat of reverse engineering.
13. Code obfuscation is a well-known technique that makes reverse engineering of a mobile application difficult, and this technique is often used by the development community.
14. Automated tools can identify design inconsistencies unless efforts are made to do a threat-model and architecture review.
15. Because open source comes from multiple parties and is introduced in the application code by developers from in-house and/or outsourced partners, it is essential that the inventory tracks the open-source component in the code and determines if these components are affected by known vulnerabilities.
16. Whitelisting may be helpful when the volume of applications that an enterprise releases is high and when there is an increased need for the use of third-party code.
17. Dynamic analysis finds incorrect coding that can potentially cause security risk.
18. Integrating static analysis with continuous integration servers, e.g., Jenkins, minimizes the need for manual intervention, reduces dependency on the security team and fixes bugs that might turn into security vulnerabilities before they become unmanageable.

CPE quiz

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

Take the quiz online

http://bit.ly/2vfs7C0

CPE quiz #174

THE ANSWER FORM

Based on Volume 3, 2017

TRUE OR FALSE

ATLURI ARTICLE

1. _____
2. _____
3. _____

PATEL

4. _____
5. _____
6. _____
7. _____

SUBRAMANIAN AND SWAMINATHAN ARTICLE

8. _____
9. _____
10. _____
11. _____

RAJENDRAN ARTICLE

12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____

Name _____

PLEASE PRINT OR TYPE

Address _____

CISA, CRISC, CISM or CGEIT # _____

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 +1.847.253.1755. 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, CRISC, CISM or CGEIT CPE credit.

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

1 C	O	2 L	O	3 C	A	4 T	I	5 O	N	■	6 M	7 M	S	8 P
O	■	A	■	S	■	I	■	F	■	9 M	■	A	■	A
10 N	A	G	11 W	A	R	E	■	12 F	O	I	■	13 K	A	Y
F	■	■	O	■	■	R	■	■	■	14 T	I	E	■	B
15 I	N	T	E	16 G	R	I	T	17 Y	■	I	■	■	18 P	A
D	■	■	■	I	■	N	■	R	■	G	■	19 S	■	C
20 E	N	21 V	I	S	A	G	E	■	22 D	A	R	K	■	K
N	■	A	■	T	■	■	■	23 W	I	T	■	E	■	■
24 T	U	R	N	■	25 U	P	T	I	M	E	■	26 W	E	27 B
I	■	I	■	28 C	■	■	■	L	■	■	■	S	■	I
29 A	30 V	A	I	L	A	31 B	I	L	I	32 T	Y	■	33 I	T
34 L	A	B	■	I	■	Y	■	■	■	A	■	35 A	■	■
36 I	N	L	I	E	37 U	■	38 S	39 I	X	S	I	G	M	40 A
T	■	E	■	41 N	D	A	■	P	■	T	■	E	■	R
42 Y	E	S	■	T	■	■	43 F	O	R	E	N	S	I	C

standards guidelines tools and techniques

ISACA Member and Certification Holder Compliance

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

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

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

ITAF™, 3rd Edition

(www.isaca.org/itaf) provides a framework for multiple levels of guidance:

IS Audit and Assurance Standards

The standards are divided into three categories:

- **General standards (1000 series)**—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- **Performance standards (1200 series)**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

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

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

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

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

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

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

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

Reporting
2401 Reporting
2402 Follow-up Activities

IS Audit and Assurance Tools and Techniques

These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programs, reference books and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf*.

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

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

Comments may also be submitted to the attention of the Director, Thought Leadership and Research via email (standards@isaca.org); fax (+1.847.253.1755) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

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

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

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

ISSN 1944-1967

Subscription Rates:

US:
one year (6 issues) $75.00

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

Remittance must be made in US funds.

advertisers/ websites

leaders and supporters

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

Enter **JOURNAL20** at checkout and receive a 20% discount off your order

Blockchain Fundamentals — Web Download

by ISACA

WEB DOWNLOAD
Product Code: WBCB
Member / Nonmember:
$25.00 / $50.00

Blockchain has the potential to become a major force for innovation and change the way you process everything with records-from registrations, records of ownership, transfers of value and stock purchases, to identities and healthcare. The current digital world is built on ledger systems that worked well in past generations, but that fail to provide you with the capability to address the ledgers that are needed in an Internet-driven world. The basic blockchain characteristics that successfully create a secure and trustable infrastructure to support the Bitcoin cryptocurrency system are disrupting how we create and use ledgers, which, in turn, has the potential to bring significant value to the global economy and provide new capabilities that enhance government and business functions. Blockchain use is not limited to cryptocurrencies. Other blockchains are being developed so that input and output transactions contain ledger entries for numerous other items, including financial instruments, public records, contract information, other items demonstrating ownership or professional capability, and identities. Using trusted technologies to create its unique structure, blockchain features-such as openness, decentralized infrastructure, ability to transact anonymously while ensuring identity, and elimination of third-party attestation-can propel blockchain to become the enabling technology that streamlines digital-age transactions.

Data Privacy Audit Program — Web Download

Data Privacy considers the obligations of organizations around the information that can be used on its own or in conjunction with other information to identify, contact or locate an individual. This consideration exists for the data lifecycle from collection to use, disclosure and retention through disposal.

by ISACA

WEB DOWNLOAD
Product Code: WAPDP1
Member / Nonmember:
$25.00 / $50.00

Browse a variety of publications featuring the latest research and expert thinking on standards, best practices, emerging trends and more at ***https://support.isaca.org***

FEATURED BOOKS

COBIT 5 for Risk

by ISACA

PRINT
Product Code: CB5RK
Member / Nonmember:
$60.00 / $100.00
WEB DOWNLOAD
Product Code: WCB5RK
Member / Nonmember:
$50.00 / $90.00

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

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

COBIT 5 for Risk provides:

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

Please note: *COBIT 5 for Risk* is also available as a web download to both ISACA members and nonmembers.

Securing Mobile Devices

by ISACA

PRINT
Product Code: CB5SMD1
Member / Nonmember:
$35.00 / $75.00
WEB DOWNLOAD
Product Code: WCB5SMD1
Member / Nonmember:
$25.00 / $60.00

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

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

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

Responding to Targeted Cyberattacks

by ISACA

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

Also available as a free Web Download to members.

A Breach WILL Eventually Occur!
Is your enterprise prepared?

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

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

This publication covers a few of the basic concepts that will help answer the key questions posed by a new outlook that a breach WILL eventually occur.

2 EASY WAYS TO ORDER:

1. Online—Access ISACA's bookstore online anytime 24/7 at ***https://support.isaca.org***
2. Phone—Contact us M–F between 8:00AM – 5:00PM Central Time (CT) at +1.847.660.5505

CGEIT Review Manual, 7th Edition

by ISACA

PRINT
Product Code: CGM7ED
Member / Nonmember:
$85.00 / $115.00
EBOOK
Product Code:
EPUB_CGM7ED
Member / Nonmember:
$85.00 / $115.00

The *CGEIT® Review Manual 7th Edition* is designed to help individuals prepare for the CGEIT exam and understand the responsibilities of those who implement or manage the governance of enterprise IT (GEIT) or have significant advisory or assurance responsibilities in regards to GEIT. It is a detailed reference guide that has been developed and reviewed by subject matter experts actively involved in governance of enterprise IT worldwide.

The manual is organized to assist candidates in understanding essential concepts and studying the following updated job practice areas:

- Framework for the governance of enterprise IT
- Benefits realization
- Resource optimization
- Strategic management
- Risk optimization

The *CGEIT® Review Manual 7th Edition* features an easy-to-use format. Each of the book's five chapters has been divided into two sections for focused study. Section one of each chapter contains the definitions and objectives for each of the five CGEIT practice areas, as well as the corresponding tasks performed by GEIT professionals and knowledge statements necessary to perform these tasks. It also includes:

- A map of the relationship of each task to the knowledge statements
- Self-assessment questions and explanations of the answers
- Suggested resources for further study

Section two of each chapter consists of content and reference material that supports the knowledge statements. The material enhances CGEIT candidates' knowledge and/or understanding when preparing for the CGEIT certification exam. In addition, the *CGEIT® Review Manual 7th Edition* includes definitions of terms most commonly found on the exam.

The manual is an excellent as a stand-alone document for individual study or as guide or reference for study groups and chapters conducting local review courses, and it can be used in conjunction with the CGEIT® Review Questions, Answers & Explanations Manual 4th Edition The manual also serves as a useful desk reference that can be added to the libraries of professionals involved in the governance of enterprise IT.

Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT

by ISACA

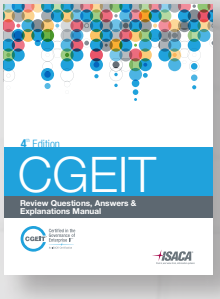
WEB DOWNLOAD
Product Code: WCGEIT
Member / Nonmember:
FREE / $15

How do organizations know they are effectively utilizing enterprise technology resources to best realize business goals? Do organizations know the extent to which their business goals are dependent on technology? How do they know the technology they have in place is providing value and realizing the expected return on investment?

Governance of enterprise IT (GEIT) is the systematic process of answering these and other related questions. Implementing a GEIT system can bring many benefits to an organization, including lower costs, greater control, more efficient and effective use of resources, and overall better strategic alignment and risk management. The primary purpose of adopting and using a GEIT system is to deliver value to stakeholders. This guide provides the necessary steps to implement GEIT to help the enterprise achieve its goals and demonstrate value delivery.

This guide is intended for people who are new to GEIT or have recently been tasked with implementing a GEIT structure. Whether the enterprise is already familiar with GEIT concepts and practices or is exploring the possibilities, this guide will help provide an understanding of the steps to implement GEIT and examples of the benefits of GEIT, so that buy-in from senior leadership can be obtained and a framework to guide implementation efforts can be used.

CGEIT Review Questions, Answers & Explanations, 4th Edition



by ISACA

PRINT
Product Code: CGQ4ED
Member / Nonmember:
$60.00 / $75.00

The *CGEIT® Review Questions, Answers & Explanations Manual 4th Edition* is designed to familiarize candidates with the question types and topics featured in the CGEIT exam.

The 250 questions in this manual have been consolidated from the *CGEIT® Review Questions, Answers & Explanations Manual 2015* and the *CGEIT® Review Questions, Answers & Explanations Manual 2015 Supplement*.

Many questions have been revised or completely rewritten to be more representative of the CGEIT exam question format and/or to provide further clarity or explanation of the correct answer. These questions are not actual exam items but are intended to provide CGEIT candidates with an understanding of the type and structure of questions and content that has previously appeared on the exam. This publication is ideal to use in conjunction with the *CGEIT® Review Manual 7th Edition*.

To help candidates maximize—and customize—study efforts, questions are presented in the following two ways:

- Sorted by job practice area—Questions, answers and explanations are sorted by the CGEIT job practice areas. This allows the CGEIT candidate to refer to questions that focus on a particular area as well as to evaluate comprehension of the topics covered within each practice area.
- Scrambled as a sample 75-question exam—The 75 questions are arranged in the same percentages as the current CGEIT job practice areas. Candidates are urged to use this sample test to simulate an actual exam and to determine their strengths and weaknesses in order to identify areas that require further study. Answer sheets and an answer/reference key for the sample exam are also included. All sample test questions have been cross-referenced to the questions sorted by practice area, making it convenient for the user to refer back to the explanations of the correct answers.

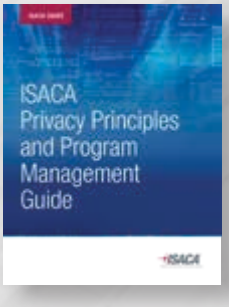
Risk Scenarios: Using COBIT 5 for Risk

by ISACA

PRINT
Product Code: CB5RS
Member / Nonmember:
$35.00 / $70.00
WEB DOWNLOAD
Product Code: WCB5RS
Member / Nonmember:
$25.00 / $60.00

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

Privacy Principles and Program Management Guide



by ISACA

PRINT
Product Code: IPP
Member / Nonmember:
$45.00 / $90.00
WEB DOWNLOAD
Product Code: WIPP
Member / Nonmember:
$35.00 / $70.00

The main purpose of *ISACA Privacy Principles and Program Management Guide* is to provide readers with a harmonized privacy framework. The book offers a set of privacy principles that align with the most commonly used privacy standards, frameworks and good practices, as well as fill in the gaps that exist among these different standards. This practical guide can support or be used in conjunction with other privacy frameworks, good practices, and standards to create, improve and evaluate a privacy program specific to the practitioner's enterprise. Special guidance on how to use the COBIT 5 framework to implement a more robust privacy program is included in this publication.

2 EASY WAYS TO ORDER:

1. Online—Access ISACA's bookstore online anytime 24/7 at ***https://support.isaca.org***
2. Phone—Contact us M–F between 8:00AM – 5:00PM Central Time (CT) at +1.847.660.5505

ISACA®
Trust in, and value from, information systems

RECOGNIZED GLOBALLY. IN-DEMAND LOCALLY.

MAKE AN ISACA CERTIFICATION YOUR NEXT MOVE!

Secure your seat and your future—take the first step today!

Register for an upcoming exam at *www.isaca.org/2017exams-Jv5*

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

What are the advantages of computer-based testing?

- > More opportunities to take an exam
- > Larger test center network—over 880 locations and growing
- > Faster exam results
- > Test centers designed specifically for testing
- > Increased flexibility for changing exam times

Register for an upcoming exam at *www.isaca.org/2017exams-Jv5.*

Take the first step towards obtaining a globally respected ISACA certification and becoming recognized as one of the most-qualified professionals in your field of information systems.

Want to see how ISACA members save?

JUST ASK

www.isaca.org/JustASK

Does your audit software allow you to carry key facts and insights to senior management meetings?

R-CAP™ brings Audit Universe & KPIs to your fingertips.

Audit Life-Cycle and Risk Management Solution

available on AppExchange

works with Google Drive

- Observations Tracking
- Risk and Controls Matrix
- Regular Business Monitoring
- Audit Timesheet Management
- Efficient Work-Paper Documentation
- Insightful Dashboards & Reports
- Resource Scheduling

Built by Auditors, For Auditors.

For your free 30 day trial email at **contactus@rcap.online**

www.rcap.online

TRONIXSS