Volume 1, 2015

ISACA® Journal

Analytics and Risk Intelligence

Featured articles:

Implementing an Information Security Continuous Monitoring Solution

Auditing SQL Server Databases Using CAATs

Are Your Data Secure in the Cloud?

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

The Conference You Have Been Waiting For

Gain Actionable Insights, Tools and Practical Guidance at ISACA's First-of-its-Kind **COBIT Conference**

14-15 MARCH 2015 · ORLANDO, FLORIDA

COBIT Conference registration includes access to the opening keynote at North America CACS Conference 2015!

Earn up to 14 CPEs! Register and pay by 20 January to save US $200!*

The power of COBIT 5 is in what you do

- AUDIT & ASSURANCE
- RISK MANAGEMENT
- INFORMATION SECURITY
- REGULATORY & COMPLIANCE
- GOVERNANCE OF ENTERPRISE IT

Learn more at *www.isaca.org/cobitconference15jv-1*

* Registration fees must be paid in full by 12pm on 20 January 2015 or regular registration rates will apply. If registration fees are paid in full after 12pm on 12 March 2015, onsite registration rates will apply. Both early bird and regular pricing can be used in conjunction with group discounts.

COBIT® 5
AN ISACA® FRAMEWORK

DATA PRIVACY DAY

PLUG IN ON **28 JANUARY**

LEADERS IN PRIVACY

As an International Data Privacy Day champion, ISACA recognizes and supports the ideal that individuals, organizations, businesses and government all share the responsibility to be aware of privacy challenges and encourages everyone to bring information privacy into their daily thoughts, conversations and actions.

NEW PRIVACY RESOURCES AVAILABLE

EVENTS

- **14 January**
  Privacy is Good for Business Twitter Chat
- **22 January**
  ISACA Professional Guidance Webinar on Privacy

PUBLICATIONS

- *Vendor Management Using COBIT 5*
- *Controls and Assurance in the Cloud: Using COBIT 5*
- *Personally Identifiable Information (PII) Audit/Assurance Program*
- *Securing Sensitive Personal Data or Information Under India's IT Act Using COBIT 5*
- *Privacy and Big Data*
- *Privacy Framework* (coming 2nd Quarter 2015)

CONFERENCES

COBIT 5 AN ISACA® FRAMEWORK

2015 COBIT Conference
14-15 March | Orlando, Florida, USA

north america CACS

2015 North America CACS
Computer Audit, Control & Security Conference
16-18 March | Orlando, Florida, USA

For more information visit ***www.isaca.org/privacyjv1.***

ISACA®
Trust in, and value from, information systems

VOLUME 1, 2015

ISACA® Journal

Columns

Features

Plus

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

Online-Exclusive Features

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

Online Features
The following is a sample of the upcoming features planned for January.

Book Review: The Fifth Domain: Wake Up Neo
Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA

Porters' Elements for a Business Information Security Strategy
Yuri Bobbert

Return on Security Investment—15 Things to Consider
Ed Gelbstein, Ph.D.

Book Review: Cybersecurity for Industrial Control Systems
Reviewed by A. Krista Kivisild, CISA, CA

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

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

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

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

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

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

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

SOURCE: BUREAU OF LABOR STATISTICS, 2014

Do you have what it takes to answer the call?

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

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

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

Capella University

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

Microwave Software

Let me tell you about my microwave. When I bought it, it was called a microwave oven and I was going to roast turkeys in it in half an hour. I am sure it was white then, but it has turned a pale, sickly yellow. I never did cook a turkey in it and all I ever use it for now is to defrost sauces, reheat coffee and nuke the ice cream so it is soft enough to scoop. Even though it is more than 20 years old, it still works and it does what I need it to do, so there is no reason to buy another with a lot of features in which I have no interest.

I am certain that the data centers in every organization older than 20 years have applications running in them that are just like my microwave. They are old software serving a limited purpose, often for a limited number of business functions (or for just one). They work; they do what their users want them to do, thus there is no reason to buy a new system with a lot of features in which those users have no interest. Ominously, they are indicative of the reason that the problems of cybersecurity will not be solved any time soon.

SOFTWARE, OLD AND NEW

As I was writing this article, a news report announced the discovery of a flaw in a widely used software product called Bash. It is freeware that is incorporated into 70 percent of the machines that connect to the Internet. Created in 1987, the software has been maintained by a volunteer, who evidently introduced the flaw in 1992. According to the report, the bug, known as Shellshock, can be used to take over entire devices, "potentially including Macintosh computers and smartphones that use the Android operating system."[1] Ubiquitous software with a flaw undetected for 22 years! If ever there was microwave software, this is it.

Corporations and government agencies have accumulated their application portfolios over a period of years. Many still have programs written in COBOL, running on mainframe computers and written when most of their employees were in grade school. Others modernized their systems in anticipation of the new millennium, now 15 years behind us. In many companies, applications exist because they served a predecessor corporation that has long since been acquired and absorbed, but which lives on in ancient software. Each of these applications operates atop an infrastructure, often shared with other programs. They each get data from somewhere and send results somewhere else. If not well controlled, they expose those data to theft and misuse.

It is my experience that very few organizations know how all their applications work, which programs they interface with, or how they use operating system and middleware services. Yes, that is an over-broad generalization, and, yes, there might be some organizations that understand all their systems—all of them, no exceptions, 100 percent. But I stick to my assertion—just because it is a generalization does not make it wrong.

Here is the challenge: Are all applications, data and infrastructural elements[2] protected at the same level? Or do the "critical" systems receive the greatest security, control, recoverability and audit attention, while the rest are relegated to "tier 2"? As I said in different context in a previous article, there is no such thing as tier 2.[3] Small, lightly used, nearly forgotten systems may be running on the same platforms or in the same highly interconnected infrastructures as those depended upon by large numbers of users for essential business functions. If they are not protected as though they were critical, these systems can expose the ones that are more highly valued when a cyberattacker comes along looking for a weak spot to penetrate.

IT IS ONLY

Beware the "Oh, it is only…" response. It is only the forecasting system, which, if illicitly tweaked just a bit, causes a manufacturer to over- or undersupply products to the marketplace. It is only the training system that enables sensitive tasks to be staffed just by qualified personnel. It is only the library system that can be used to display—or to hide—

Do you have something to say about this article?

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

Go directly to the article:

information critical to lawmakers. These are not randomly chosen examples, nor are they hypothetical. They are the equivalents of my microwave, sitting on the kitchen counter or in the data center or the office or the store for so long that they are hardly noticed. But cyberattackers notice and exploit them. For example, the instrument that caused so much damage to Target and Home Depot was not a server array. It was *only* a cash register.[4]

The problem of cyberthreats is not going to be solved[5] just by replacing microwave software with gleaming new products. Newness is not enough. Should some technoarchaeologist read this piece 20 years hence, I am sure he/she will chuckle about some buggy software introduced in 2015. The fact is that in any significant enterprise, there are so many programs acquired over such a wide span of time, developed to run on so many different infrastructures, that there are almost certainly going to be holes in the code and in the interfaces of which a patient attacker might take advantage. Advanced persistent threats (APTs) reward just such patience.

THE HEART OF THE MATTER

The jumble of systems, new and antiquated, well and poorly controlled, leads me to conclude that: Cyberthreats are not a security problem. They are a systems problem.

> Cyberthreats are not a security problem. They are a systems problem.

There is only so much information security professionals can do to build barriers and walls and fences and domes around information systems and data. Ultimately, flawed software cannot be secured. It can only be made more difficult—not impossible—to penetrate.

Those responsible for information systems, beyond the chief information officer (CIO) up to the highest ranks of management, must accept that cyberattacks will occur and that some of them will succeed.[6] That being the case, an equal investment should be made in preparing for recovery from such attacks as is given to preventing and detecting them. The *Framework for Improving Critical Infrastructure Cybersecurity*[7] lists "recover" as one of the five functions of cybersecurity. However, I have seen very little money spent on recovering from cyberattacks. This will have to change.

The most important step, to my mind, in mitigating the threat of cyberthreats is for organizations to gain a thorough understanding of all the software running in their environments, the flow of data and control among them, the interfaces among them and within their infrastructures, and the exposures presented by what I have termed microwave software. In too many organizations, neither management nor staff knows these things. Their ignorance is bliss for the malefactors in the darkest regions of our hyperconnected world. They are looking for and finding such exposures. This should be all the incentive required for legitimate organizations to become, at least, aware of what is running in their data centers and, at best, to make all the software—both up to date and microwave—work harmoniously and safely together.

ENDNOTES

[1] Perlroth, Nicole; "Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant," *The New York Times*, 24 September 2014, *www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html?module=Search&mabReward=relbias%3Ar%2C%7B%221%22%3A%22RI%3A9%22%7D*

[2] Better known as "configuration items" in ITIL terminology. See ITIL, *www.itil-officialsite.com/InternationalActivities/TranslatedGlossaries.aspx.*

[3] Ross, Steven J.; "Shedding Tiers," *ISACA Journal*, vol. 2, 2014

[4] Kuchler, Hannah; "Home Depot Attack Bigger Than Target's," *The Financial Times*, 19 September 2014, *www.ft.com/cms/s/0/7f9a2b26-3f74-11e4-984b-00144feabdc0.html#axzz3EMhI2Uy9*

[5] I am not even sure that there will ever be a solution as such. As technology advances, so do the tools and incentives for those who would undermine information systems. If we cannot win the war, we can at least reduce the number and severity of casualties.

[6] See my previous article: Ross, Steven J.; "Bear Acceptance," *ISACA Journal*, vol. 4, 2014.

[7] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 12 February 2014

Monitoring From the Cloud—Insights on Demand

Michael P. Cangemi, CISA (retired), CPA, CGMA, is an author and business advisor, with a significant focus on technology for business and specifically continuous monitoring and analytics for governance, risk and compliance (GRC) and business process improvement. He is the former president, CEO and director of Etienne Aigner Group Inc., and president and CEO of Financial Executives International. He is the president of Cangemi Company LLC, which he founded, and through which he serves as senior advisor and director to various companies and manages his other business interests. Cangemi was the editor in chief of the *ISACA Journal* from 1987 to 2007.

Using a computer to automate and implement continuous monitoring (CM) in IT has been around for decades. It was adopted early by IT auditors and IT security specialists, and later used to monitor transactions by operations and financial managers.[1] Since the early 1990s, monitoring has been a key component of internal controls systems as defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).[2] Consequently, many companies utilize continuous transaction monitoring.

However, there have always been many hurdles to overcome to make it truly effective, including the high cost of software acquisition, getting on the company's IT platform and the complexity of remediating exceptions within the software itself. These hurdles have made monitoring transactions an uphill battle.[3]

"Although many companies have made impressive strides in adopting and deriving value from their initial CM efforts, in general, current usage remains slight relative to its potential."[4] Reasons cited include the need for capital investment and building the business case for the capital investment.

BIG DATA AND THE CLOUD

The growth of big data has added to the interest in and need for more continuous monitoring to advance business processes. To accompany the growth of big data, and uncomplicated continuous transaction monitoring, a star in the software industry has emerged—the cloud.

The cloud computing system is made up of two "ends," a front and a back end, usually connected by the Internet. The front end is the side the client sees, and the back end is made up of data servers and storage systems. Together, they comprise the total cloud. Since information and applications are stored in one place, cloud computing eliminates the need to load different software systems onto individual computers and allows for greater access and collaboration between employees and team members.

The cloud-based approach is changing the software industry, with many technology companies moving from enterprise resource planning (ERP) to Software as a Service (SaaS) models. Rather than be defeated by changing times, one company, described below, revolutionized its product offering to remain competitive and expand the use of analytics and monitoring.

Oversight Systems, a technology company in Atlanta, Georgia, USA, had been in business for nine years, and pre-2012, the mainstay of its business was providing continuous transaction monitoring for clients on a daily basis. The software was popular, but installation of the software onsite at a client's office meant a high purchase price and lengthy sales cycle.

In 2013, Oversight decided to change its entire approach for two reasons. First, after many years, the markets had shifted and most clients found they did not need onsite, daily transaction monitoring. Second, this technology shift meant many clients wanted a lower-cost, lower-maintenance solution. Oversight decided to move to a SaaS model instead, and its latest product, Oversight Insights On Demand, is the result of that shift. Insights on Demand is a web-based application with specific monitoring applications designed to deliver analytics quickly and effectively.

For example, spending managers can use the modules to assist them in making better business decisions. The application still monitors 100 percent of training and education (T&E) and payment card (P-card) data, but delivers the analysis of those data at the desired frequency of the company.

While examples of companies making the switch to the cloud and/or adding SaaS modules are rising, a preeminent example of a leader in the trend is Salesforce.com, now the world's leading cloud-based customer relationship management (CRM) application.[5] A tangent benefit of the cloud is the expanding breadth

of implementation from very large companies to small and medium-sized entities.

The implementation of CM has been hampered by many hurdles over the years, including, as noted previously, the high cost of software acquisition, hardware costs and annual maintenance, building the related business case for capital expenditures, getting software onto the company system in data centers, and the complexity of remediating issues with the software.[6] Clearly, the advantages of the new model based in the cloud are manifold. For example, according to Oversight Chief Executive Officer Patrick Taylor, "The cloud-based model means all data are safely stored and retrievable. Costs are lower because equipment purchases are avoided, and by making the service available on demand, companies can determine frequency of analysis, offering them more flexibility in the costs."

Major concerns of the cloud-based approach are the obvious privacy and security issues, especially in light of recent data breaches such as the Heartbleed bug in early 2014 and the Target data breach in late 2013. While security and privacy are always concerns with cloud-based software, the monitoring systems can address these concerns by using hashing algorithms that anonymize information that may be considered sensitive and by not asking for nonessential sensitive data, such as full social security and credit card numbers that are not needed for the analytics process.

Convenience and pricing aside, there are additional advantages to the cloud-based model. Since data for multiple customers are stored in one place, algorithms and statistics improve as the customer base enlarges. This allows for ever-improving analytics, which become more refined, benefiting all companies using the system.

"Now we have one cloud auditing another cloud," Taylor said of Oversight's Insights On Demand product. "We use everyone's data to benchmark individual client progress and savings. Having more customers and data means we can better determine the outliers, which allows us to better find risk and fraud. The cloud reduces the gray area while simultaneously making a monitoring system more manageable."

Insights On Demand early adopters are already reaping the benefits of the new approach. For example, a travel manager in the manufacturing industry knew she needed a better way to develop analytics around her company's T&E spending, but did not have enough budget to buy a software solution. She knew she would need a business case to prove the solution provided value before she could spend the money. Since Oversight now offers a free trial, where the company analyzes 90 days' worth of data, she was able to prove return on investment (ROI) before she purchased the product.

IMPROVING POLICIES FOR ONGOING IMPROVEMENT

Digging deeper into policies, one can see the black and white of the travel policy and the inevitable gray area of employee behavior. Fraud is a very small percentage of any T&E program, but there are still many ways a program can lose money, other than blatant fraud. A cloud-based CM system helps shrink the amount found in that gray area by letting employees know someone is watching their spending habits for noncompliance.

ROLE FOR INTERNAL AND IT AUDIT

"Although CM is a business operations issue, internal auditors, due to their familiarity with continuous auditing (CA), often become the champions of CM programs."[7]

In my time as a chief audit executive, I looked for ways to go beyond audit and add to the control infrastructure of the business. I call these "positive deliverables."[8] Recommending CM is a classic example of a positive deliverable from audit and compliance departments.

The cloud allows improved monitoring for compliance, fraud and independent audit in near-real time with a significant potential savings impact. Even though the security concerns are very real, they can and are being addressed and I have no doubt the cloud is here to stay.

ENDNOTES

[1] Cangemi, Michael P.; "From Continuous Auditing to Continuous Monitoring: You Should Be the Champion," *ISACA Journal*, vol. 4, 2012

[2] COSO was formed in part to help define internal control after the passage of the US Foreign Corrupt Practices Act.

[3] Ramamoorti, Sridhar; Michael P. Cangemi; William M. Sinnett; "The Benefits of Continuous Monitoring," Financial Executives Research Foundation (FERF), 2011, *www.ferf.org* or *www.canco.us*

[4] *Ibid*.

[5] Salesforce.com, *www.salesforce.com/*

[6] *Op cit*, Ramamoorti

[7] *Ibid*.

[8] Cangemi, Michael P.; Tommie Singleton; *Managing the Audit Function, 3rd Edition*, John Wiley & Sons, *www.canco.us*

Timo Heikkinen, CISA, CGEIT

Timo Heikkinen is a senior audit manager for Nordea Bank in Helsinki, Finland. With more than 15 years of IS auditing experience, he is responsible for the execution of Nordea Group's overall internal audit strategies and planning, managing and leading business-IT and outsourcing-related audits across the Nordea Group. He is also a member of ISACA's Relations Board.

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

A: The IS auditor's core role has not changed much over the years. The IS auditor is and should be primarily responsible for providing an objective assurance on the risk and control processes of the organization. In that way, the IS auditor is in the best position to improve risk and control practices in the organization. Many things (e.g., emerging technologies, regulatory obligations, outsourcing) have, of course, changed how the IS auditor's audit universe looks now compared to what it was earlier. Those things have all brought new challenges to the IS auditor's working environment. My piece of advice for IS auditors is to constantly keep your knowledge updated and build a trusted partnership with key management representatives.

> "There is a tendency to trust and expect too much of third parties, but as an IS auditor, trust is not a good control."

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

A: One of the biggest risk factors that IS auditors should be closely monitoring is risk related to services being provided by third parties. Whenever an organization outsources something, it cannot outsource the management responsibilities related to risk and controls. There is a tendency to trust and expect too much of third parties, but as an IS auditor, trust is not a good control. Business management needs to understand and manage risk related to services being provided by third parties.

Q: *How do you believe your software engineering background has supported your career and current role as a senior audit manager?*

Enjoying this article?

- Learn more about, discuss and collaborate on career management and compliance in the Knowledge Center.

www.isaca.org/knowledgecenter

A: My software engineering background has helped me to understand in practice not only how the applications are being developed and maintained, but also the nature of controls that need to be implemented to applications.

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

A: Certainly, my certifications have enhanced my career. Having a certification shows a true commitment and dedication to your chosen occupation. At my organization, the Certified Information Systems Auditor® (CISA®) designation is mandatory for all IS auditors. Therefore, our company strongly encourages and supports all new hires in obtaining the CISA certification.

Q: *What will be the biggest compliance challenge in 2015? How will you face it?*

A: I would say that in the banking sector, which I represent, the biggest compliance challenge is coming from the regulatory side. We face new challenges to ensure compliance with both existing and emerging regulations. To face these challenges, auditors need to ensure that management is aware of and has taken appropriate actions to sustain ongoing compliance with these regulations.

Do you have something to say about this article?

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

Go directly to the article:

WHAT'S ON YOUR DESK RIGHT NOW?

- A laptop
- Cell phone
- Family photos
- The latest edition of *ISACA Journal* (currently I'm reading an article about business case management)
- A bottle of water

HOW HAS SOCIAL MEDIA IMPACTED YOU PROFESSIONALLY?

1. Social media has brought IS audit professionals around the globe closer to each other and allowed for better and increased sharing of information.
2. As an IS auditor, I must be aware of social-media-related risk, e.g., data privacy, and ensure that such risk is sufficiently managed in my organization.

WHAT ARE YOUR FAVORITE BENEFITS OF YOUR ISACA MEMBERSHIP?

1. The great deal of good and valuable information about various audit-related topics
2. Networking through volunteering. As a member of different international-level boards and committees, I have been able to meet and connect with some of the finest IT professionals around the world.

WHAT DO YOU DO WHEN YOU ARE NOT AT WORK?

- Spend time with my family.
- Play football (soccer) and watch my sons playing football (soccer) and ice hockey.
- Just simply, enjoy life.

Perspectives From a Seasoned Practitioner

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

It was a bit of a surprise and a huge compliment to be invited to contribute to this column after many years reading the words of Tommie Singleton in this space. I shall do my best not to disappoint. To give you a hint as to where this column is going during the upcoming year, let us start with a summary of some lessons learned in my many years dealing with information systems, technologies and audits.

Change is fast and profound. Over the last five decades, technical innovation and new legislation relating to data and information have caused major dislocations. These, in turn, have created the need for new approaches to IS/IT audit. Some of these changes are outlined in **figure 1**.

While this table is certainly incomplete, the conclusion is that continuous learning is inescapable. Thus, we are required to learn how to learn and then how to unlearn and relearn.[1] Failure to do this is a guarantee of professional stagnation and failed careers.

In the IS Audit Basics column, I plan to reflect the lessons I learned both as an auditee and as an IS/IT executive and auditor. I intend for them to be thought-provoking as opposed to sets of procedural "do this" statements.

WHAT WE KNOW WE KNOW

Dependency on IS/IT has become irreversible and its governance and management rely on audit competencies and independence. Innovation cycles are likely to remain short and bring with them new vulnerabilities and management challenges.

Besides, internal and external threats keep changing and, unless mitigated, these could have an adverse and potentially serious effect on organizations. The frameworks for information assurance, security, risk and governance evolve as experience is gained and lessons are learned.

The same is true for audit standards and guidelines. It is prudent to assume that the domains of IS/IT audit have become so large that it is now unlikely that anyone can know everything about it. This makes the development of IS/IT audit strategies that much harder.

On the positive side, the audit profession offers many opportunities for personal and professional growth: progression to chief audit executive (CAE), membership in audit committees, consultancy and senior management roles. The choice is yours, but only if you are prepared.

Figure 1—Historical Timeline of Data-related Technical Innovation

The 1960s	Migration from analog to digital, emergence of digital, integrated circuits; IBM 360 series of mainframes; minicomputers from many vendors; SCADA used in industrial control; proliferation of programming languages (e.g., ALGOL, COBOL, FORTRAN, BASIC). Data speeds were 2.4 kbps at best and fax machines Group 2.
The 1970s	Transaction processing becomes the norm; early cellular data communications and optical fiber networks; Internet email and early personal computers; BASIC becomes widespread.
The 1980s	First 16-bit PCs; local area networks (LANs) enter the corporate world; packaged software for office applications becomes available from several vendors; malicious software (malware) appears. Firewall products on offer; data protection legislation is introduced in the UK.
The 1990s	Client-server claims "the mainframe is dead"; graphical user interfaces become ubiquitous; executive awareness of the critical dependence on IS/IT; Internet access makes its way into enterprises; web 1.0 grows explosively; pioneers enter e-commerce; European Data Protection and US Heath Insurance Portability and Accountability Act (HIPAA) legislation are enacted; Y2K becomes a concern.
The 2000s	Technology users become proficient; malware becomes professional; COBIT 3rd Edition is published and widely adopted; social networks' popularity gives rise to corporate issues. Mobile technologies are transformed by smartphones and tablets; bring your own device (BYOD) and mobile apps become an enterprise issue. Risk-based audits are widely adopted.
The 2010s	Cloud computing; big data; concerns about the theft of intellectual property; threats to individual privacy and the militarization of cyberspace; the Internet of Things (IoT) and wearable technologies. COBIT® 5 covers several volumes of guidance and separates governance from management.
Beyond	Who knows?

The following is a good reminder of what the concept of "auditor" covers:[2]

- A.....Analytical
- U.....Unbiased
- D.....Diplomatic
- I.....Independent (and inquisitive)
- T.....Thorough
- O.....Objective
- R.....Reliable

Having worked with (and learned much from) many capable auditors, there have been occasions when I came across others who would have done far better to have pursued a different career. Why? Because they showed themselves to be one or more of the following: arrogant, disorganized, undisciplined, opinionated, cynical or emotionally incontinent. Let us say that they were not respected by their victims.

YOUR CREDIBILITY AND OTHER GOOD THINGS OF WHICH TO BE CONSCIOUS

Credibility is *the* essential asset for any auditor. If your independent assessments cannot be backed by your credibility, they are worthless and, therefore, as an auditor, so are you. Credibility is built over time by developing knowledge and experience. It helps to:

- Fully understand what your CAE considers to be "good enough"
- Make certain at all stages that anything you say and write is supported by evidence—be it audit tests that you have personally conducted or documentation you have reviewed
- Maintain confidentiality by discussing audit findings and results with only those who need to know
- Remember that gossip, rumors and other inside information are not evidence
- Not jump to conclusions

Integrity is another fundamental requirement for an auditor, involving honesty, fair dealing (or objectivity) and truthfulness.

Finally, after passing the Certified Information Systems Auditor® (CISA®) examination, you are likely to be dealing with experienced professionals from whom you can learn much. Make sure you take the time to do so, as this is the best way to broaden your understanding and experience of the audit process and the interpersonal and political dimensions of the job. Ask lots of questions, particularly "Why?," until you are satisfied with your understanding.

It is good to remember that while management understands the role and importance of audits, when the time comes, auditors are rarely welcome. After all, when the auditors descend on a team carrying out project or operational work, the result is disruption: The auditors need documentation and access to data, request meetings over a period of several weeks or more, and keep asking awkward questions.

Bear in mind that some auditees may have had bad experiences if previous auditors created the impression that they were focused on criticism, assigning blame or engaged in the mindless pursuit of perfection. Besides, if members of previous audit teams were not well informed about the role of IS/IT in the organization—its criticality, structure, resources, past performance and related issues—they may have been perceived as not making good use of the time assigned in the audit plan or focusing on irrelevant areas.

It is important for auditors to understand the auditee's history: What was the scope of past audits? What actions were recommended (particularly those worded "shall" rather than "should")? And, how many of these implementations were re-audited? It is also important to find out how many of the recommendations were not implemented and why.

Knowledge of the audit history should include the approach taken by your predecessors, the audit strategy, the adopted standards and guidelines, and, especially, the interpersonal relations between past auditors and auditees. A history of disagreements, conflict and lack of trust is hard to recover from and can easily result in mistrust and resistance.

ABOUT THE NEXT COLUMN

The next column will continue this introduction to the realities of IS/IT audits by exploring what makes an audit successful from the perspective of the many parties involved: the auditors, the CAE, the audit committee, senior management and, not least, the auditees.

Given that audits are an activity carried out by people who interact with other people, topics related to soft skills will appear in future columns because successful audits depend on how such interactions take place.

CONCLUSION

You can be confident that IS/IT technologies will continue to change and with them, audit practices. Be prepared!

ENDNOTES

[1] Alvin Toffler, *www.alvintoffler.net/?fa=galleryquotes*

[2] Tangient, "Introduction to Audit," boruetthsm, *boruetthsm.wikispaces.com/file/view/Auditing.ppt*

Are Your Data Secure in the Cloud?

John Nye, CISA, CISM, CRISC, CISSP, is the director of technology risk solutions at ProcessUnity *(www.processunity.com)*, a cloud-based provider of governance, risk and compliance (GRC) solutions. He is responsible for the governance of ProcessUnity's Software as a Service (SaaS) solutions and advises clients in the art of third-party vendor risk management. Nye has worked with firms such as @stake, Symantec and Moody's as an assessor of third-party risk and has served as an information security executive for a midsized technology service provider, protecting information and managing corporate risk from both sides of the due-diligence table.

I was involved with hosting my first Internet-accessible, web-based, multitier, multitenant, shared infrastructure software solution in 1998. It was an x.509 digital certificate authority. Back then we didn't call it a "cloud solution," but we might today. In the years since, I have been involved in two other cloud solutions: a customer contact campaign management (auto-dialing) solution for call centers and, in my current role, a governance, risk and compliance solution with a focus on vendor risk management. All three of these solutions offer some common traits to subscribers:

- Access to specialty expertise
- Streamlined or even transparent upgrades and maintenance
- Effortless scalability
- A chance to share their confidential data with a trusted third party
- The opportunity to rely on a vendor for the success of a critical business process

Clearly, there are pros and cons in this list. In a differential comparison against on-premise solutions, the traditional benefits of outsourcing—access to expertise and seamless technology operations—can usually be achieved within the enterprise at some reasonable expense. Tactically, a business is usually better off selecting the best solution, regardless of whether it is internal or outsourced. Strategically, outsourcing can allow an organization to focus on its core competencies. Regardless of the business drivers for outsourcing, once appropriate third-party management and governance is included, outsourcing is not necessarily a material cost saver.

However, when one adds the massive scalability of cloud solutions to the outsourcing equation, the economics change drastically. The economies of scale achieved through the use of cloud solutions drive costs down to the point where they are difficult, possibly even negligent, to ignore.

For some organizations, the decision to move to the cloud is both obvious and instant. For others, cloud solutions represent intolerable risk. Certainly the challenges of assuring quality, protecting information and meeting service availability requirements in today's extended enterprises are present in the cloud, just as they are with other outsourced solutions. Yet in the cloud, these risk factors are more greatly feared. Why?

The answer is simple: fear of the unknown. This is true in two ways. First, transparency can be a challenge. The word "cloud" itself seems to say, "You do not need to know what is inside." Indeed, the icon of a cloud, so familiar as the shape of the Internet on network diagrams, tells us that what is inside is large, complex and irrelevant to the discussion. In the traditional notion of an enterprise with a clearly defined perimeter connected to the Internet—an external and untrusted entity—this obfuscation of complexity and expression of irrelevancy is completely reasonable. However, when outsourcing a business function to a cloud provider, nothing could be further from the truth. As risk management professionals, part of our responsibility is to evaluate the risk of outsourcing to third parties and to assess or audit their controls. It is our job to look inside the cloud, but, unfortunately, this is not always possible and, indeed, the right to audit seems to be more challenging to obtain as the cloud provider becomes larger and more cost-effective.

Second, cloud providers frequently implement familiar controls in unfamiliar ways. Let us take the simple example of comparing an on-premise enterprise software solution to a Software as a Service (SaaS) cloud solution. When the enterprise wants to regulate access to its data, one of the most common controls is to host the applications that contain the data inside its firewalls to prevent unwanted access via the Internet, which is to say, the enterprise uses network-based source Internet Protocol (IP) address filtering. Unfortunately, this technique does not work for many cloud providers. For example, when clients access solutions over the Internet and multiple clients share a single platform, universal access is allowed.

Certainly, firewalls should be in place, but they allow, rather than prevent, access to key applications via the Internet. Fortunately, the control objective is to regulate access to the data, not the application. So, instead of using a network-based solution (i.e., a firewall) to indiscriminately regulate access to the application, one can implement the source IP address filtering directly in the application to regulate access to the data. In this way, desired policies can be enforced on a per-client basis,e.g., by limiting access to a client's data to users connecting from that client's enterprise.

This is just one example of how a control might be implemented differently by a cloud provider than a typical enterprise or even a noncloud service provider. For those of us whose role as a risk manager includes evaluating whether our cloud providers are achieving the necessary control objectives, we need to be prepared to understand how our cloud providers operate in order to evaluate the design and effectiveness of their controls. And, we will want to consider how such control designs change the traditional priority of other controls.

Let us take another look at the previous example. In the case of the on-premise enterprise application, the firewall meets (at least) two control objectives. First, it authenticates the user's source IP address to ensure that the user is onsite at the enterprise. Second, it protects the application from attack by Internet-based attackers. In the case of the cloud solution, the source IP authentication has been moved to the application, but that application has been exposed to the Internet, thereby modifying its attack surface and exposing it to new threats. Clearly, application security controls should be a higher priority for the cloud application than for the on-premise enterprise application. Not only is the cloud application exposed to the Internet, it is also responsible for some of the controls previously provided by the firewall.

> "Be prepared to understand how your cloud providers operate in order to evaluate the design and effectiveness of their controls."

Understanding how cloud providers operate is key. Without this information, you cannot understand their (or your) risk. And, if you do not understand their risk, you cannot determine if their controls are designed or operating effectively. To a fellow risk professional, such a mantra will come across as both obvious and academic. However, in the world of third-party risk management, where one-size-fits-all assessments are used in an attempt to compress standards-based, formal controls audits into assessments lasting only a day or two, the peril of assumption warrants the reminder. To avoid this mistake, particularly if there are time constraints, ask these questions about any cloud provider at the beginning of an assessment:

- What type of cloud solution is it (e.g., Infrastructure as a Service [IaaS], Platform as a Service [PaaS], SaaS), and how does that inherently impact control design?
- Does the cloud provider use virtualization or other new technology and, if so, how has the provider addressed the organization's control objectives as these new technologies reshape how the Open Systems Interconnection (OSI) model[1] is implemented?
- Has the cloud provider implemented provisioning tools? If so, do these tools enhance governance, inadvertently subvert the provider's security architecture, or both?
- The cloud is relatively new. How new, as a business, is the cloud provider and what does that mean about its financial and business stability?
- Cloud providers frequently do not want to manage their clients' individual users and, instead, support some form of delegated access management. What options are available from the cloud provider for access and identity management? What options are available for access control review and for log review? And, do these features meet the organization's governance and operational needs?

- Is the cloud solution stand-alone, or does it involve multiple providers (e.g., a SaaS solution hosted on a PaaS solution)?
- Is there an opportunity for risk concentration that would not be present in an on-premise enterprise solution? How does the organization's business impact analysis change if multiple applications are moved to the same IaaS provider? How many of the organization's peers outsource the same function to the same cloud provider and, if many, how would a potentially marketwide incident impact the organization?

These questions are hardly comprehensive, but they serve to focus one's perspective at the beginning of an assessment of a cloud provider. Understanding how cloud vendors operate allows you to move beyond fear of the unknown into the comfortable place of rational, risk-based decision making.

One of the most common questions I am asked—by colleagues, clients and lay persons alike—is: "Is the cloud secure?" In response, I point out that some cloud providers are more secure than others. But, typically, when I am asked this question, it is by someone curious about well-known, consumer-oriented solutions (such as Netflix), or one of the larger, business-oriented public cloud solutions (e.g., Google Apps or Amazon EC2). Insofar as we can agree that even the best-governed solutions can experience security incidents and that when we say "secure," we actually mean "well governed with effectively designed and operating controls based on a meaningful analysis of risk," my response is: "Most large cloud providers are probably secure, but without better access, I cannot prove it."

Although I have not been fortunate enough to have obtained direct audit privileges at all of the larger cloud providers that I have used, I am still generally comfortable using them. For example, a key part of any security program is a secure, repeatable host build and the ability to apply patches. Intuitively, I know that any organization operating millions of hosts is going to have host build and change management under control. My evidence is that they operate successfully—something they simply could not do at their scale without careful planning, superb consistency and excellent change management. But, such evidence is circumstantial. I am also of the opinion that most cloud providers, due to their specialization in one or a small number of solutions, can generally do a better job of securing those solutions than their clients. For instance, when I was responsible for the security and compliance of a cloud-based telephony autodialer, a number of controls specific to telephony fraud were implemented that only a handful of the roughly 400 clients would have understood. In this way, the organization's specialization allowed us to mitigate risk that would have gone unmitigated had the solution been on premise with clients.

From the perspective of a risk professional, one of the greatest downsides of using one of the public cloud providers is the inflexibility of the engagement model. Similar to business-to-consumer services, subscribers to public cloud solutions basically have to agree to the contract provided by the solution provider. It is unlikely that such contracts will grant meaningful audit rights or include other specific terms and conditions that may be desirable to the business or required by regulators.

This does not mean you have to give up on assurance completely. In the case of the business-oriented public cloud providers, security assurance documents (e.g., ISO 27001 certifications, SOC audit reports) are usually available for review by potential subscribers. Such documentation will likely answer many of the assurance questions and should be able to allow you to make a reasonable, rational, risk-based business decision about whether to subscribe to the service or not. Unfortunately, particularly if you are regulated, this may not be sufficient to meet your due-diligence obligations.

With smaller providers, these dynamics are reversed. You will be more likely to negotiate the contract you want and audit or assess the provider directly. And you had better do so because, as you move away from the mega scale of the largest providers, you will not be able to intuitively equate operational viability with good governance. The smaller the cloud provider is, the less you can assume and the more important due diligence becomes. Some will be very trustworthy while others will be too risky with which to engage. You will not know unless you take a close look.

Enterprise-grade solutions are rarely served by single applications. An on-premise enterprise architecture can include business applications cross-integrated with one another, authentication infrastructure, logging infrastructure, and the like. Cloud solutions are no different. It is not uncommon to engage a cloud-based SaaS provider only to discover that to get the most out of the application or to govern its use appropriately, it needs to be integrated with other business applications and technology infrastructure. Frequently, the solution is to engage more cloud providers to glue these pieces together. By the time you are fully

integrated with the cloud provider serving the initial business requirement, you may find that you have had to integrate with several additional providers to assemble a complete solution. If done correctly, a foundation of cloud solutions that integrates with and extends your enterprise architecture is created. Salesforce.com's AppExchange is just one example of such an ecosystem. The down side is that, at least initially, the cost of due diligence will be high, because you have had to assess the risk of engaging with multiple third-party service providers to meet that initial business need.

A quick look at the applications in Salesforce.com's AppExchange reminds us that the cloud is an excellent place for mobile and social applications, or any application that requires collaboration and information exchange with parties outside the enterprise. Without the cloud, you have to build an extranet to exchange information with others, leaving your enterprise to solve some of the same security architecture problems faced by cloud providers, e.g., the source IP address filtering challenges described previously. As an information security and risk management professional, the ability to easily support collaboration is one of the most compelling reasons to prefer a cloud-based solution. And, to the degree that complexity is the enemy of security, cloud solutions reduce the complexity of collaboration (or at least spread that complexity out over a wider field of resources and specialists).

And so, it is no surprise that collaboration is a key component of each of the cloud-based solutions of which I have been a part. X.509 certificate authorities need to be hosted by trusted third parties to achieve the segregation of duties central to the registration model and also must make submission of certificate requests and distribution of revocation information easier. Customer communications are pushing to mobile and social platforms. And, vendor risk management requires collaboration and information exchange between enterprises and their third parties for assessments and audits. For these activities, the cloud simply makes sense.

Just as cloud providers use their ability to specialize and their economies of scale to perfect the business solutions they provide, so too can they leverage these differentiators to secure and govern their solutions. Enterprise architects have to build computing environments that support the general-use case of multiple, disparate business applications. Each application presents unique challenges to use, operate, secure and govern. For on-premises solutions, this either leads to great expense and complexity as you customize, or it leads to increased risk acceptance as you generalize. By contrast, a security architect of cloud solutions can specialize. By securing instance after instance of a single solution, the security architect can drive a security and risk management program closer to perfection than in any other environment. That this is possible makes cloud solutions an attractive option for risk professionals. But, unfortunately, not all cloud providers make this investment. As risk professionals, our duty, as always, is clear: to understand and make transparent the unknown, thereby replacing the irrationality of fear with risk-based decisions that allow the business to correctly capitalize on good opportunities.

ENDNOTES

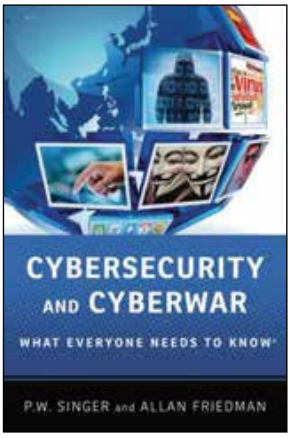
[1] Open Systems Interconnection (OSI) model is developed and maintained by the International Organization for Standardization (ISO); see ISO/IEC 7498-1.

Cybersecurity and Cyberwar: What Everyone Needs to Know

Reviewed by Larry Marks, CISA, a professional with experience in the fields of security, privacy, risk, governance and program/project management. He is based in Piscataway, New Jersey, USA, and works for IBM. He can be reached at *marksl@us.ibm.com.*

Cybersecurity and Cyberwar: What Everyone Needs to Know is one of the few books that is completely up-to-date and analyzes the importance of cybersecurity beyond the realm of the Internet. There is a growing sense of vulnerability as a result of new vectors of cyberattack. This book defines cybersecurity, discusses the basic issues of cybersecurity about which everyone should be aware and supplies the reader with tools to address these threats.

The authors, who are fellows at the Brookings Institute, do not have a specific background in IT or cybersecurity. They do not perform vulnerability assessments or teach cybersecurity or computer science courses. Rather, they wrote this book by researching and identifying key questions that a professional or layman would want answered. They scientifically validated and then narrowly fine-tuned the questions using workshops and seminars at the Brookings Institute. The result is a series of topics addressing questions readers may want answered, specifically: How does cybersecurity work? What can one do? Why does it matter?



By P. W. Singer and Allan Friedman

The book does a very good job asking and answering the questions that need to be asked such as: How can people trust in cyberspace? How come a new, more secure Internet cannot be built? How can users protect themselves (and the Internet)? With new technologies introducing new vulnerabilities, a book or reference is needed to summarize a baseline of the general information that is commonly known and what is unknown.

Cybersecurity and Cyberwar reviews the facts around the computer worm Stuxnet and how terrorists use the Internet. On a high level, it describes how the Internet works from a user-friendly and not overly technical point of view. It highlights the current issues facing corporations and government agencies: the need for more skilled resources in computer science and cybersecurity; the need for a better definition or consistent definition of cybersecurity; and the need for a greater partnership between the federal government and corporations regarding the sharing of the occurrence of data security breaches, methods of attack and the need for a common approach for remediation. For economies of scale, the authors request that corporations trust that the government will not leak their data security privacy gaps and incidents and that governments trust that corporations will disclose any incidents. Greater sharing can also result in greater prosecutions and a federal effort to strengthen the national infrastructure.

The book describes the lack of effort by the US Congress to enact legislation to strengthen the US's cybersecurity infrastructure. However, the book does not mention the reasons for this lack of effort or the initiatives to foster and elevate the need for legislation and a greater partnership. It does reference US Executive Order 13636, one of many first steps by the US government to improve the critical network infrastructure.

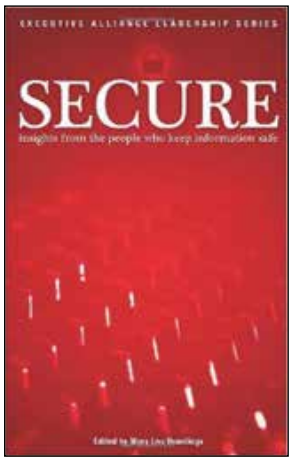
This book is recommended for anyone interested in cybersecurity because it emphasizes the necessity of understanding risk. As the authors put it: "We must accept and manage the risks of the world—both online and real—because of all that can be achieved in it. And that really is what everyone needs to know."

EDITOR'S NOTE

Cybersecurity and Cyberwar: What Everyone Needs to Know is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Secure: Insights From the People Who Keep Information Safe

Reviewed by A. Krista Kivisild, CISA, CA, who has had a diverse career in audit while working in government, private companies and public organizations. Kivisild has experience in IT audit, governance, compliance/regulatory auditing, value-for-money auditing and operational auditing. She has served as a volunteer instructor, training not-for-profit boards on board governance concepts; has worked with the Alberta (Canada) Government Board Development Program; and has served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter.



By Mary Lou Heastings

There is always a new information security issue to focus on, another area of key concern relating to IT security, data security or business continuity planning that security professionals need to be aware of to keep on top of the relevant risk. But how can security professionals determine the relevant risk to their industry? At a time when changes in technology continue to accelerate, how can anyone decide what should be the information security areas of concern to their company and the places where they should focus their team's work in the future?

Secure: Insights From the People Who Keep Information Safe is a collection of works from senior IT leaders in various industries providing what they feel are the biggest security concerns right now and for the future. In this quick, compact read, readers can gather understanding from those in the know and can consider if these experts' ideas about leadership competencies needed in the future, design security or application delivery networks are applicable to their enterprise/industry. Everyone from technical practitioners to those just beginning their IS audit, security, risk or governance careers can find value in this general management book as it keeps readers aware of the latest risk concerns.

The book's primary strength is its ability to provide the reader with valuable information on upcoming information security and technology issues, which are highlighted by the opinions of 10 IT information security leaders. The writings of each leader are engaging and succinct. As a result, readers can quickly get through a chapter and gather the information they need on a bus or train ride or between meetings. This book is ideal for anyone who does not have time to read a full book on the subject, but wants to be aware from where the next risk to IT is coming. Additionally, background on each leader and his/her company is provided, so the reader can determine if the author's industry shares the same risk factors/concerns.

The world of information security is constantly changing. The number of Internet users has grown exponentially, smartphone and mobile use is exploding, and social media web sites are used more and more to do business. Those at all levels within IS audit, risk, security and governance struggle to stay abreast of these changes and keep aware of what the real concerns are to know where to focus their efforts. While the risk is also exploding, IS professionals need to focus on the right risk: those that are growing, those that are relevant and those that are of a bigger concern.

Despite the rapidly changing nature of security and risk, this book will remain relevant for years. The majority of the leaders in this book focus on entity-level and governance risk; as a result, the insights provided in this book are at a high enough level that they will remain relevant for years to come. This book is perfect for today's IS professional who needs to learn a lot of information, but does not have much time to do so.

EDITOR'S NOTE

Secure: Insights From the People Who Keep Information Safe is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Effective Cyberthreat Management Evolution and Beyond

Seemant Sehgal, CISA, CISM, BS7799 LI, CCNA, CEH, CIW Security Analyst, SABSA, heads the security assessment services department at ING Bank, The Netherlands. He has engaged with organizations such as Capital One Bank, IBM, COMODO Security Solutions and Cisco Systems in various domains of information security.

Over the past few decades, cybersecurity has gained pivotal importance in the way businesses operate and survive in their value systems. Exponential growth in the number of users and devices connected to the Internet has led to an unprecedented expansion in the attack surface available to perpetrators in the world of cybercrime.

While attack vectors get more and more sophisticated, enterprises across the globe are confronted with a challenge to address their security concerns in an effective, yet cost-efficient way. Information security is possibly one of the most vibrant areas in the IT sector, in which technical innovation constantly paves the way to defeat emerging threats. This is not surprising, as the threat landscape itself is constantly evolving and it demands a constant revival of defense tactics.

Technology, however, is just one facet of defense strategy for any enterprise. A holistic view on people, process and technology is required in any organization to make the defense strategy successful. Ironically, the sheer size, complexity and geopolitical diversity of a modern-day enterprise acts as an inherent obstacle for its pursuit to achieve business objectives in a secured environment.

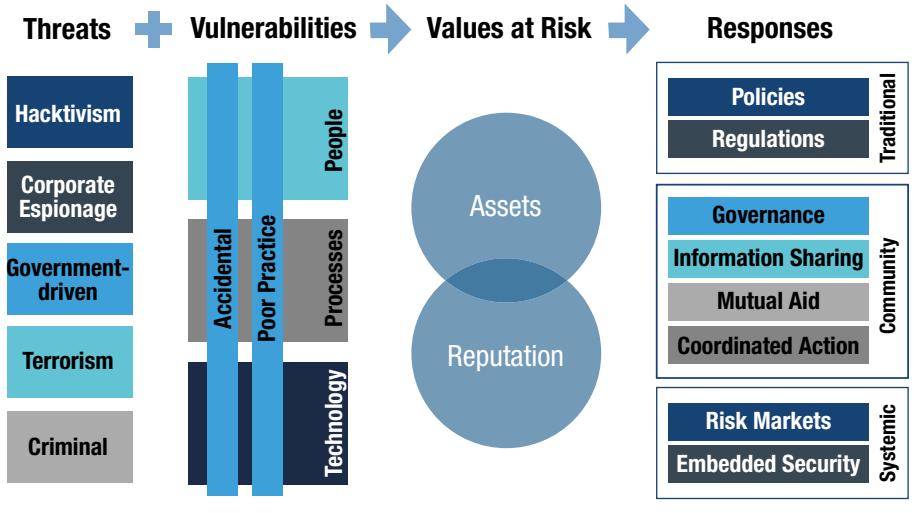
This article explores these challenges, analyzes common frameworks available to manage these challenges and deliberates on evolving possibilities that may give chief executive officers (CEOs) the agility required to cope with the cyberthreat landscape.

UNDERSTANDING THE CORE OF THE PROBLEM

One might wonder if the information security industry really understands the problem that security professionals are trying to solve. At the crux of the issue lies the paradigm of threat, vulnerabilities and value at stake for a business. An area for improvement is to solve the problem at its source.

The source of the problem is not threats themselves, but threat agents. The term "threat agent," from the Open Web Application Security Project (OWASP), is used to indicate an individual or group that can manifest a threat. So, who are these individuals or groups of individuals at the source of the problem?

Figure 1—World Economic Forum Cyber Risk Framework



Source: World Economic Forum, *www.weforum.org/*. Reprinted with permission.

Do you have something to say about this article?

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

Go directly to the article:

The answer to this question is easily visible in the overview developed from a study conducted by a task force at the World Economic Forum in 2014 (**figure 1**).[1] Irrespective of the type of threat, the threat agent takes advantage of the vulnerability and exploits it in an attempt to negatively impact the value the business has at risk. The attempt to execute the threat in combination with the vulnerability is called hacking. When this attempt is successful and the threat agent is in a position to negatively impact the value at risk, it can be concluded that the vulnerability is successfully exploited. So, essentially enterprises are trying to defend against hacking and, more important, the threat agent that is the hacker. This conclusion is supported by the facts presented in the Verizon *2014 Data Breach Investigations Report*,[2] which clearly shows hacking as the activity that resulted in the greatest number of breaches in the past decade (**figure 2**). In fact, most activities in this chart can be termed as the by-product of a hacker's mind-set.

TRADITIONAL CYBERTHREAT MANAGEMENT

While there is no one-size-fits-all framework to build and run a sustainable security defense in a generic enterprise context, the framework in **figure 3** reflects a high-level representation.

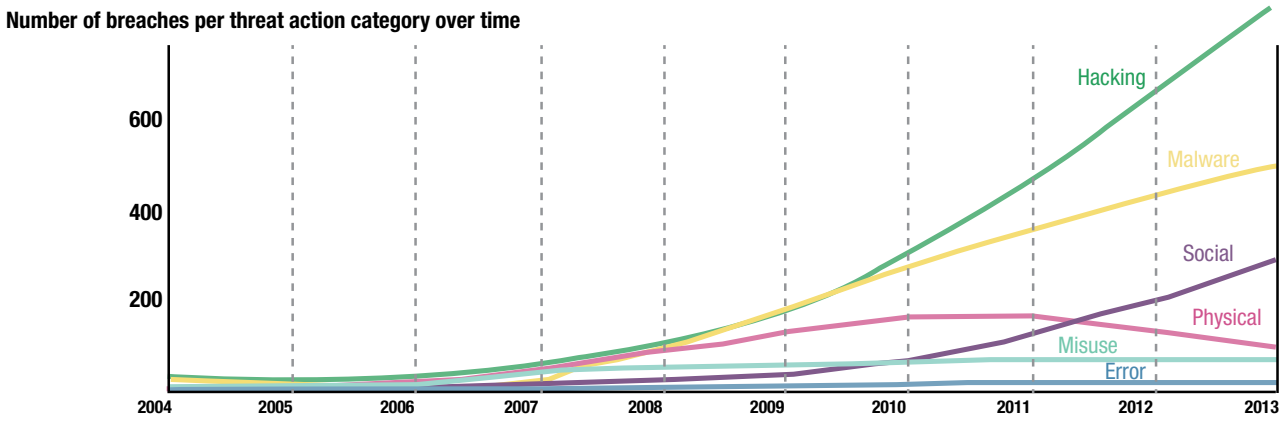
Most IT risk and security professionals would be able to identify this framework and would agree that it is a sustainable approach to managing an enterprise's security landscape. Facts prove that this is not the case. If the framework was working as intended, the number of security incidents would show a downward trend as threats would fail to manifest into incidents. They would be identified by enterprises as known security problems and dealt with in day-to-day security operations. However, recent security surveys conducted by many organizations clearly show an upward trend of rising security incidents and breaches.

The trend of rising security incidents and breaches in itself is not surprising. In 2013, 13,073 vulnerabilities were registered across vendors and technologies. That is an average of 35 new security failures each day of the year (**figure 4**).

Figure 3—IT Risk Management Framework

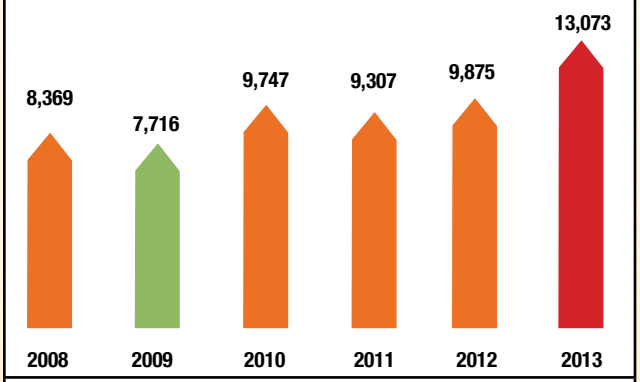
Source: Seemant Sehgal. Reprinted with permission.

Figure 2— Breaches Per Threat Action Category



Source: Verizon, *2014 Data Breach Investigations Report*, 2014, *www.verizonenterprise.com/DBIR/*. Reprinted with permission.

Figure 4—Annual Security Vulnerabilities



Source: Secunia, *www.secunia.com*. Reprinted with permission.

Couple these facts with the ease of execution and readily available exploit kits and the threat grows in both probability of exploitation and magnitude of impact. With speed and magnitude, each threat hits the security ecosystem of an enterprise and takes away its ability to deal with it in a daily operational regime. Hence, most enterprises witness a growing trend of security incidents being reported and registered.

THE EVOLVED VIEW ON ADDRESSING THE PROBLEM

Due to a sharp increase in the number of published vulnerabilities in 2013-14, many organizations had to set up emergency response teams to respond to cyberthreats and incidents. These teams are a new addition to the existing ecosystem and have two main functions: responding to security incidents and collecting internal and external security intelligence for predictive analysis.

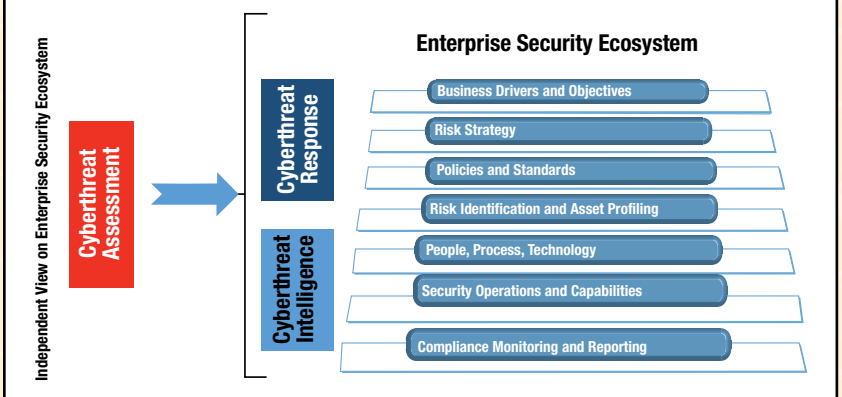
Being able to respond to security incidents via a dedicated response team boosts the capacity of the operational organization to contain and recover from the same. Responding to incidents is, in any case, a reactive approach to deal with cyberthreats. This is where cyberthreat intelligence comes into play. Threat intelligence is a more proactive means of enabling an organization to predict incidents. However, this approach also has a downside. The influx of a great deal of intelligence information may limit the prospects of making it actionable within the required time span.

Cyberthreat assessments are an effective means to add the relevance factor to this overwhelming influx of intelligence information. Cyberthreat assessment is currently recognized in the industry as red teaming, which is the practice of viewing a problem from an adversary or competitor's perspective.[3] As part of an IT security strategy, enterprises can use red teams to test the effectiveness of the security ecosystem as a whole and provide a relevance factor to the intelligence feeds on cyberthreats. This can help CEOs decide what threats are relevant and have higher exposure levels compared to others.

The evolution of cyberthreat response, cyberthreat intelligence and cyberthreat assessment (red teams) in conjunction with the existing IT risk framework is reflected in **figure 5** and can be used as an effective strategy to match the agility of evolving cyberthreats.

The cyberthreat assessment process assesses and challenges the ecosystem of enterprise security systems, including designs, operational-level controls and the overall cyberthreat response and intelligence process to ensure they are capable of defending against relevant cyberthreats.

Figure 5—Evolution of Cyberthreat Management



Source: Seemant Sehgal. Reprinted with permission.

HOW CEOS CAN ADAPT TO THE EVOLVED VIEW

While the traditional view of cyberthreat management is purely based on threat perception, the evolved view is a step ahead in terms of its relevance to the evolving threat landscape. In the past, enterprise risk and security decisions were based on theoretical risk assessment exercises only. This trend was mainly encouraged by a compliance-oriented mind-set. As cyberthreats grew in scale and complexity, the industry realized the gap between perceived threat and real threat. This led to the emergence of threat landscape monitoring and threat intelligence capabilities. Cyberthreat intelligence strengthens response capabilities by supplying the required information, which can be made actionable and help enterprises prepare for emerging threats.

Most threat intelligence solutions available in the market today are driven by external and mostly public sources of threat information. Another source of such information can be fellow organizations and competitors. The amount of data an organization receives from such shared information can be quite overwhelming. This is why it becomes important to add a relevance factor to it. This can help CEOs decide what threats are easier to combat for the threat agents and where they can afford to accommodate an evolution road map for their defense capabilities.

Cyberthreat assessment exercises can be extremely helpful to highlight the most relevant cyberthreats and quantify their potential impact. The word "adversary" in defining "red team" is a key element that emphasizes the need to independently challenge the security ecosystem from the view point of an attacker.[4] Red team exercises should be independent of the scope, asset profiling, security, and IT operations or coverage of existing security policies. Only then can enterprises bring in the attacker's perspective, measure the success of its risk strategy and see how it scores when challenged.

It is important that red team exercises look at the ecosystem as a whole and point to flaws in all components of the IT risk framework. It is a common notion that a red team exercise is a penetration test. This is not true. Use of penetration test techniques is a means to achieve the required information to replicate cyberthreats and create a controlled security incident. The technical shortfalls that are discovered as a result of this exercise are mere symptoms of gaps that may exist in the governance of people, processes and technology. Hence, to make the organization more resilient against cyberthreats, focus should be kept on addressing the root cause and not merely fixing the security flaws discovered during the exercise. Another key aspect to keep in mind is to include cyberthreat response and threat monitoring in the scope of such assessments. This demands that such exercises be executed, and partially announced, with CEO-level approval. This ensures that enterprises challenge the end-to-end capabilities of an enterprise to cope with a real-time security incident. Lessons learned can be capitalized on to improve the overall security posture of the organization.

CONCLUSION

As cyberthreats evolve, 100 percent security for an active business is impossible to achieve. Business is about making optimum use of existing resources to derive the desired value for stakeholders. Cyberdefense cannot be an exception to this rule. To achieve optimized use of security investments, CEOs should ensure that the security spending for their organization is mapped to the emerging cyberthreat landscape. Red teaming is an effective tool to challenge the *status quo* of an enterprise's security framework and derive facts about its security state. Not only can these facts be used to improve cyberthreat defense, they can also prove to be an effective mechanism to steer a higher return on cyberdefense investments.

ENDNOTES

[1] World Economic Forum, Partnering for Cyber Resilience (PCR), 2014, *www.weforum.org/issues/partnering-cyber-resilience-pcr*

[2] Verizon, *2014 Data Breach Investigations Report*, 2014, *www.verizonenterprise.com/DBIR/*

[3] Red Team Journal, "Read Team," Glossary, *http://redteamjournal.com/glossary/glossary-red-teaming/*

[4] Secunia, Vulnerability Review, 2014, *http://secunia.com/vulnerability-review/vulnerability_update_all.html*

Implementing an Information Security Continuous Monitoring Solution—A Case Study

Tieu Luu is director of research and product development for SuprTEK, where he leads the development of innovative products and services for the company, including the PanOptes Continuous Monitoring Platform.

The threats to government computer systems and networks continue to evolve and grow due to steady advances in the sophistication of attack technology, the ease of obtaining such technology, and the increasing use of these techniques by state and nonstate actors to gain intelligence and/or disrupt operations. The US Government Accountability Office (GAO) cites that from 2006 to 2012, the number of cyberincidents reported by federal agencies to the US Computer Emergency Readiness Team (US-CERT) grew from 5,503 to 48,562, an increase of 782 percent.[1]

As one of the responses to this growing threat, the executive branch of the US government has established as one of its cross agency priority (CAP) goals[2] the continuous monitoring of federal information systems to enable departments and agencies to maintain an ongoing near-real-time awareness and assessment of information security risk and rapidly respond to support organizational risk management decisions. In November 2013, the US Office of Management and Budget (OMB) issued memorandum M-14-03 requiring all federal departments and agencies to establish an information security continuous monitoring (ISCM) program.[3] The US Department of Homeland Security (DHS) has been tasked to work with all of the departments and agencies to help them implement continuous monitoring through the Continuous Diagnostics and Mitigation (CDM) program.

To help it comply with the OMB mandate, one large US government agency has contracted with SuprTEK, an IT engineering and professional services firm, to develop a continuous monitoring system that is responsible for monitoring millions of devices across a globally distributed network. The system has enabled the client to improve its processes for risk and vulnerability management, certification and accreditation (C&A), compliance and reporting, and secure configuration management, greatly improving the security posture of its systems and saving countless work hours by automating many of the previously manual processes.

DEFINING ISCM

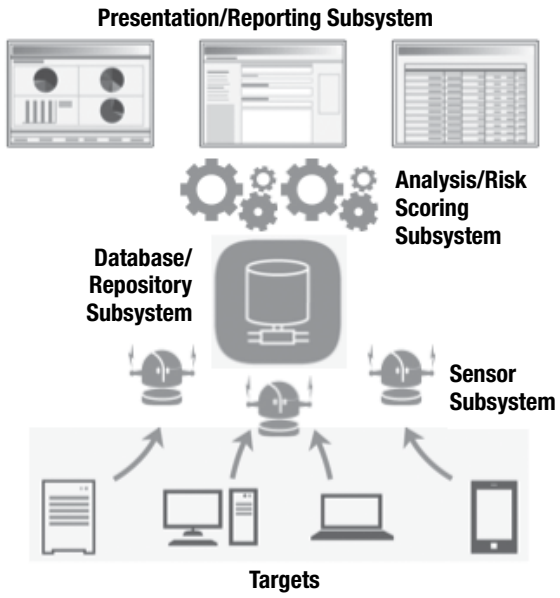
So what exactly is ISCM? "Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions."[4] This means continuously collecting information to provide a comprehensive understanding of everything that is deployed on an enterprise's networks and using this information to assess compliance against security policies and exposure to threats and vulnerabilities. This information provides IT managers with a comprehensive and up-to-date inventory of assets and how they are configured so that they understand what is on their networks and where the networks may be vulnerable. It helps system administrators properly prioritize vulnerabilities based on how pervasive they may be across the enterprise and their potential impact to the mission or business, rather than trying to patch everything and continuously play catch-up with newly discovered vulnerabilities. The information provides auditors with up-to-the-minute information on each system's security posture so that they can properly decide whether or not a system should be approved to go live on the production network or be taken offline if a critical finding is not properly remediated or mitigated. The collected information is also entered into a set of risk-scoring algorithms to quantify the security posture across the entire enterprise and identify and prioritize the worst problems to fix first so that executives can focus their scarce IT resources.

IMPLEMENTATION ARCHITECTURE

A continuous monitoring system is essentially a data analytics application, so at a high level, the architecture for a continuous monitoring system, depicted in **figure 1**, resembles that of most typical data analytics/business intelligence (BI) applications. DHS has defined a technical

reference architecture for continuous monitoring called the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) reference architecture[5] based on the work of three leading US federal agencies that have successfully implemented continuous monitoring solutions: the US Department of State (DOS), the US Internal Revenue Service (IRS) and the US Department of Justice (DOJ).

Figure 1–Continuous Monitoring System Architecture



Source: Tieu Luu. Reprinted with permission.

The CAESARS reference architecture represents the essential functional components of an ISCM and risk-scoring system, as depicted in **figure 1**. The four functional subsystems defined by CAESARS are:

- **Sensor subsystem**—Responsible for collecting data such as hardware and software inventory, configurations, compliance and vulnerabilities from the targets (i.e., assets or devices such as the computing, network and mobile devices on an enterprise's networks). The sensor subsystem may be composed of agent-based and agentless software, as well as hardware devices that scan the devices and networks and send data back to the database/repository subsystem.
- **Database/repository subsystem**—Responsible for storing the findings collected by the sensor subsystem. The database/repository subsystem is also responsible for storing and managing the technical security policies and implementation guidance that define how the targets should be configured. Targets are assessed against these baseline configurations to determine compliance and how well they are secured.
- **Analysis/risk-scoring subsystem**—Responsible for correlating, fusing, deconflicting and deduplicating the findings collected by the sensor subsystem in addition to assessing compliance of the findings against the baselines. Once the collected data have been processed by the analysis capabilities, the risk-scoring capabilities are responsible for using this information to quantify security posture and risk of the enterprise using algorithms that take into account the severity of the findings, the probability of exploit and the impact of successful exploit.
- **Presentation and reporting subsystem**—Responsible for presenting the results of the analysis and risk-scoring subsystem through various dashboards and reports to "motivate administrators to reduce risk; motivate management to support risk reduction; inspire competition; and measure and recognize improvement."[6] The subsystem has to be able to present information at an aggregate level across the enterprise as well as to be able to drill down into specific devices and findings to support remediation.

DATA INTEGRATION CHALLENGES

As with most data analytics/BI applications, data integration presents many challenges for a continuous monitoring system. Most large enterprises have multiple tools that make up the sensor subsystem, e.g., they may use a network access control (NAC) solution to detect devices, vulnerability scanners to detect vulnerabilities on devices, code analyzers and scanners to detect software flaws, and configuration scanners to assess compliance against security policies. Thus, it becomes the classic master data management (MDM) problem where the complete picture of an IT asset (e.g., hardware, operating

system, software applications, patches, configuration, vulnerabilities) has to be pieced together from disparate systems. Some of the key challenges with trying to piece together all of the required data from these types of tools are described in **figure 2**.

A data ingest capability was implemented as an asynchronous layer around the database/repository subsystem with a Secure Content Automation Protocol (SCAP)-based[7] interface to consume data from the sensor subsystem. As mentioned, the use of SCAP alleviated some integration challenges by enabling a common format, but also created other challenges due to variations in implementation by the different sensors. Ultimately, those variations were accounted for via the use of different interpreters based on version information in the data that are received by the ingester. Techniques from MDM were applied to address some of the other data integration challenges. For example, cross-referencing is a common technique in MDM where a master table is defined for an entity that contains all of the potential identifiers for that entity across the disparate systems. In this case, the cross-reference capability defined a master identifier for devices and also contained all of the other identifiers for devices used by the various sensor tools (e.g., MAC address, Internet Protocol [IP] address, host name) that were used to match the findings from the sensors to the correct device. There was no panacea to address the challenges with data completeness and quality. It required a great deal of close monitoring and validation when integrating sensor data from a new site and working with the site's administrators to correct the issues that were identified. Various system reports were used to check for completeness and quality (e.g., what sites were publishing data and what data they were publishing). To deal with issues around overlapping and conflicting findings from different sensors, a trust model that defined which sensors to trust for which types of findings (i.e., for findings of this type, trust the results from sensor A over the results from sensor B) was implemented. For example, for vulnerability assessments, the results from authenticated, agent-based scanners were considered more credible than the results from agentless, network-based scanners.

Figure 2—Examples of Key Data Integration Challenges

Challenge	Examples
Asset identification	Different tools use different ways to identify devices (e.g., MAC address, IP address, hostname, internal identifier); there needs to be a reliable way to correlate all of these identifiers to be able to aggregate and fuse together the data from all of these sources.
Incomplete and/or inaccurate data	The completeness and the quality of the data from sensors are not always reliable. For example, during the early stages of rollout of an ISCM system, many departments start by just detecting and reporting hardware inventory without running any scans for vulnerability detection, configuration and compliance assessment, so there is an incomplete picture of the asset. Inexperienced administrators may also incorrectly run scans on devices so the reported findings may be questionable (e.g., results for Microsoft Windows Domain Controller Security Technical Implementation Guidance [STIG] reported for machines that are just regular Windows boxes causing a number of false positive findings on those boxes).
Conflicting findings	There can be overlapping and/or conflicting data from multiple sensors detecting and reporting findings on the same device. For example, in a large enterprise, there are often multiple tools that perform vulnerability scanning and it is not uncommon to find that these tools report different levels of vulnerability exposure and patch compliance on the same device.
Integrating with multiple data access mechanisms and formats	Multiple tools mean multiple mechanisms for data access and multiple data formats. Some tools provide good application programming interfaces (APIs) for data access, others provide access directly to their database and others support only manual exports. Some systems send their data in batches while others send them in an event-driven model. Formats can vary greatly from log files, to comma-separated values (CSV) files, to Extensive Markup Language (XML), to only human-readable reports.
Different interpretations of standards	The NIST's SCAP is increasingly being adopted by the tools to automate assessment procedures as well as to standardize data content and formats. SCAP standards help to alleviate some of these issues, but also present their own challenges. As most developers know, the use of standards does not necessarily guarantee interoperability as a result of different interpretation of standards, support for different versions, and so forth. For example, an issue was discovered with the use of Common Platform Enumeration (CPE), a SCAP standard that is used to standardize how operating systems and application software are represented as strings. Subtle variations in how wildcard characters were used in CPE syntax caused significant differences in vulnerability and patch compliance assessment results.

Source: Tieu Luu. Reprinted with permission.

DATA ARCHITECTURE CHALLENGES

The database/repository subsystem needs a robust architecture that can support multiple interaction models—a lot of writes to ingest data from the sensor subsystem, batch and real-time processing to support the analytics, and *ad hoc* queries from users. Additionally, it needs to be able to accommodate a rich and evolving set of information that is collected about an enterprise's IT assets. For example, the initial phase of the DHS's CDM program is focused on hardware and software asset management, configuration settings, known vulnerabilities and malware. The dataset required to support these use cases includes devices, software applications, patches, configurations, vulnerabilities and operational metadata (e.g., owning/administering organizations, locations, supported systems). Subsequent phases of the program add other use cases, such as auditing, event and incident detection, privilege management, and ports/protocols/services, which greatly expand the dataset that the database/repository subsystem will have to support. Key data architecture challenges presented by these requirements are described in **figure 3**.

This system started with a single database architecture, but evolved into a three-stage data architecture to support the diverse and sometimes conflicting requirements described herein. The purpose of the first stage was to provide a warehouse or collection area to quickly write the data coming in from the sensors, assemble all the messages and reconcile them with existing records in the repository. A great deal of data transformation at the point of data ingestion could create a bottleneck, so the schema for this first stage was designed to closely resemble the data models used by Asset Reporting Format (ARF)[8] and Asset Summary Reporting (ASR).[9] Once the data were ingested, a separate set of jobs would perform the consolidation, correlation and fusion to create the complete, up-to-date profile of the asset. Next the data were extracted, transformed and loaded (ETL) into the second stage, which was a dimensional (e.g., star and snowflake schema) database that was optimized for the analytics and to support the presentation and reporting subsystem. The third stage was a set of Online Analytical Processing (OLAP) cubes that were built from the dimensional database to support the hierarchical dashboards with high-speed roll-up and drill-down analysis of the data.

ANALYTICS CHALLENGES

The main types of analytics required in a continuous monitoring solution include correlation, fusion and deconfliction of sensor findings; compliance assessment; risk scoring; historical trending; and *ad hoc* queries. In addition to helping identify the vulnerabilities that an enterprise is exposed to, along with the scope of exposure and potential

Figure 3—Examples of Key Data Architecture Challenges

Challenge	Examples
Consolidating data from multiple sources	In a large enterprise, the database/repository subsystem may be ingesting data from hundreds of sensors. In this system, the ingest capabilities were implemented to be asynchronous, idempotent and sequencing independent for efficiency and fault tolerance. As a result, the complete set of information for an asset may be distributed across multiple messages, possibly out of order and from multiple sources at different times. The database/repository subsystem needs to consolidate all of this information into a cohesive model that can be applied to analysis and risk scoring.
Conflicting data models	The database/repository subsystem needs a data model that allows the system to quickly write the rich set of information received from the sensors. In this system, the database/repository subsystem received data from the sensors in the ARF and the ASR standards. ARF is used primarily for transmitting information on hardware inventory and operational metadata. ASR is used for transmitting the actual findings discovered about those assets by the sensors. ARF is a very relational model while ASR is more denormalized. Thus, the datasets have conflicting schema design requirements.
Efficiently supporting a diverse set of analytics, dashboards and reports	The schemas for efficient ingest of the ARF and ASR messages do not necessarily make for efficient processing of the analytics nor efficiently supporting the dashboard and reporting requirements from the presentation and reporting subsystem. In addition, different portions of the analytics may require different models. For example, precomputed OLAP cubes are great for the risk-scoring dashboards that present an aggregated enterprise view of risk, as well as to provide the ability to drill down into specific departments along the organizational hierarchy or along other dimensions. However, OLAP cubes are not going to be as effective in supporting *ad hoc* queries and exploration of the data because they require *a priori* definition of the specific intersections of facts and dimensions that are desired so that they can be precomputed. This may not always be known ahead of time for exploratory use cases.

Source: Tieu Luu. Reprinted with permission.

impact, these analytics capabilities also help an enterprise assess how well it has implemented the security controls defined in its policies, e.g., the SANS Top 20 Critical Security Controls.[10] Risk scoring is applied to these assessments to quantify how well the organization is doing and prioritizes the worst problems to fix first. The risk-scoring algorithms can get quite complex when taking into consideration the different types of defects/findings, the severities of the findings, the threats and the impact on the affected assets. Additionally, the organization has to consider whether or not the findings can be remediated, mitigated and accepted, or whether the risk can be transferred to another organization. The analytics and risk scoring have to be applied at multiple levels, from the individual asset or device level, to the network enclave level, to the department level and, finally, up to the enterprise level. This enables the comparative analyses required to identify the worst areas to fix first and enables administrators to drill down into specific assets that have to be remediated. Some of the challenges that may be encountered when implementing these analytics capabilities are described in **figure 4**.

Rigorous engineering discipline combined with agile development methodologies were key to overcoming the challenges associated with the complexity of the analytics' algorithms, as well as to continuously correct and/or evolve the analytics to keep up with changes in the operational environment. Accounting for the quality and consistency issues in the sensor data published from the various sites required a combination of technical and nontechnical solutions. For example, the algorithms were implemented to be robust enough to account for missing data, but then were assigned default values that would penalize the sites for missing data and this was used to drive behavior to ensure that the organization would publish their sensor data correctly in the future. Ensuring that the data could be properly aggregated from multiple sites across the enterprise ultimately required the centralization of the definition of the taxonomies that were used to organize the assets for reporting. So while

Figure 4—Examples of Key Analytics Challenges

Challenge	Examples
Inconsistent data sets across departments	Just as data quality and completeness present a challenge to data integration, they present perhaps an even bigger challenge to implementing the analytics capabilities. Different departments may not consistently provide all of the data necessary to calculate the analytics so that equivalent comparisons can be performed across departments. For example, one of the components in the risk scoring measures was whether or not antivirus signature databases are kept up to date, but there were some departments with sensors that lacked the capability to check that on certain platforms. As a result, the scoring algorithm had to be adjusted to deal with cases of a missing date on the antivirus signature check. This had to be fixed after this particular capability was already deployed into production. In many cases, it is difficult to discover such issues until after the capability has already been deployed.
Aggregation of analytics results across multiple dimensions	The capability to apply and aggregate the analytics at multiple levels can be challenging to implement correctly. There are often multiple hierarchies that the results have to be aggregated against (e.g., active directory structure, organizational structure, IT system/program structure, locations, chain of command). In a very large enterprise with a federated deployment, these challenges can be further exacerbated with different departments and sites, independently organizing their assets using their own taxonomies. With these independent taxonomies, it becomes difficult to reliably aggregate the results together across the enterprise, thereby skewing the results of the analytics.
Accounting for timeliness of sensor findings	Different sensors may report findings for devices at different intervals that can make it challenging when trying to pull together the complete set of findings for a device. For a large enterprise with multiple sites reporting at different times, this can be exacerbated. In addition, for certain findings (e.g., software inventory), some sensors report only a snapshot in time of the current inventory without any differential information (e.g., this software was added or this software was deleted). As a result, there needs to be intelligence in the analytics to know what time window to look across to determine the most recent set of findings for a device and what findings to exclude because they have been superseded.
Evolving requirements and algorithms for analytics	Government, industry and academia are constantly defining new metrics and risk-scoring algorithms to keep pace with the emergence of new cyberthreats. For example, the DOS defined a good baseline model with iPost[11] and the DHS is expanding on that with its CDM scoring model. The risk scoring built for this client was also based on the iPost model, but has been customized for the client and has been updated and enhanced numerous times since it was first implemented. Different sectors also have their own set of metrics and models such as the US Department of Energy's (DOE) Cybersecurity Capability Maturity Model (C2M2)[12] for organizations in the energy industry. As a result, the analytics capabilities in the system have to be able to keep pace with these evolving metrics, models and algorithms.

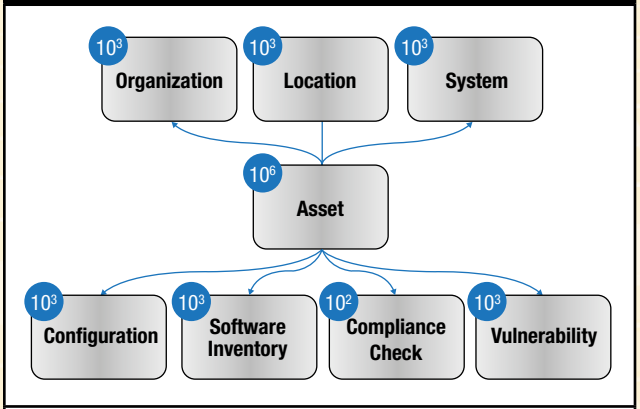
Source: Tieu Luu. Reprinted with permission.

this took away some flexibility for the sites to dynamically define their own taxonomies, the ability to correctly and reliably aggregate the data outweighed this drawback.

PERFORMANCE AND SCALABILITY CHALLENGES

While not on the same scale that large Internet companies face in their applications, in general, a continuous monitoring solution still stores and processes large amounts of data so there are performance and scalability challenges. For example, the client agency described here has somewhere between 5 million and 10 million assets with thousands of software applications and patches, thousands of compliance and configuration settings, and thousands of vulnerabilities to assess against these assets on a daily basis. **Figure 5** depicts these key datasets and the order of magnitude in the number of records that were collected.

Figure 5—Number of Records for Key Datasets Collected



Source: Tieu Luu. Reprinted with permission.

SCAP standards such as ARF, ASR and the Extensible Configuration Checklist Description Format (XCCDF) are rather verbose XML formats and can be very central processing unit (CPU)- and memory-intensive to process. This system has a fixed-time window each night for running the batch jobs that process all of the data collected from the sensors and there have been occasions when the processing duration exceeded the allotted time. These problems are not unique to continuous monitoring and there are many available solutions to address them (e.g., the use of fast-streaming XML parsers to quickly write the ARF, ASR and XCCDF data to the database and have separate jobs to do the consolidation and correlation so that no bottleneck is created at ingestion). Data are stored in multiple formats that are specifically optimized for the analytics they are supporting. Wherever possible, preprocessing is used to speed up response times (e.g., precomputed results in OLAP cubes to drive the dashboards). And then, of course, portions of the architecture have been migrated to Hadoop (e.g., HBase for the data warehouse and Map/Reduce and Pig for some of the analytics) to increase the scalability.

CONCLUSION

An ISCM solution applies many of the technologies from data analytics, business intelligence and MDM applications to the complex domain of cybersecurity. Thus, one may encounter many of the same challenges faced by these types of applications around data integration, data architecture, analytics, and performance and scalability, with additional complexities introduced by the use cases, datasets and standards that are specific to cybersecurity.

Implementing an ISCM solution across a large enterprise is a complex undertaking and there are many other challenges from the deployment, operations and governance perspectives that need to be considered. For example, the deployment approach needs to ensure that sensors are deployed in such a way that provides complete coverage of an enterprise's IT landscape. From an operations perspective, an ISCM solution has a broad set of stakeholders (e.g., chief information officers [CIOs], chief information security officers [CISOs], program managers, system administrators) and they all need to be trained to properly operate and use the capabilities provided. Executives such as CIOs and CISOs need to know how to interpret the results that are displayed in the dashboards, while the system administrators need to know how to properly scan their assets and publish findings. And perhaps most important, governance is needed to make all of this work: First, to require that all of the departments use the tool to inventory and scan their assets in accordance with enterprise security policies and, finally, to enforce the necessary mitigating or remediating actions to address the findings.

ENDNOTES

[1] Government Accountability Office, Report to Congressional Committees, "High-Risk Series: An Update," USA, February 2013, *www.gao.gov/assets/660/652133.pdf*

[2] Performance.gov, "Cross-Agency Priority Goal—Cybersecurity," *www.performance.gov/content/cybersecurity#overview*

[3] Office of Budget Management, "M-14-03. Enhancing the Security of Federal Information and Information Systems," USA, *www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf*

[4] National Institute of Standards and Technology, Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," USA, *http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf*

[5] Department of Homeland Security, "Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture Report," USA, *www.dhs.gov/xlibrary/assets/fns-caesars.pdf*

[6] *Ibid.*

[7] National Institute of Standards and Technology, "The Security Content Automation Protocol (SCAP)," USA, *http://scap.nist.gov/*

[8] National Institute of Standards and Technology, "ARF—The Asset Reporting Format," USA, *http://scap.nist.gov/specifications/arf/*

[9] National Institute of Standards and Technology, "ASR—The Asset Summary Reporting," USA, *http://scap.nist.gov/specifications/asr/*

[10] SANS Institute, "Top 20 Critical Security Controls," USA, *www.sans.org/critical-security-controls*

[11] Department of State, "iPost," USA, *www.state.gov/documents/organization/156865.pdf*

[12] Department of Energy, "Cybersecurity Capability Maturity Model (C2M2)," USA, *http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity*

User Threats Vs. User Privacy

Striking the Perfect Balance

Dimitri Vlachos is the vice president of marketing at ObserveIT. He has more than 15 years of experience as a marketing leader in both start-ups and established corporations. He has extensive experience with industry analysts in the security, network performance and application performance markets.

On the one hand, user-based attacks—whether from hackers using stolen credentials, careless third-party vendors, or negligent or even malicious insiders—represent the largest IT security threat to organizations. On the other hand, no one wants to work in an environment where their activities are constantly being monitored. So, should companies watch everything their employees are doing? Or, should they blindly trust them to safeguard company data? The answer is: Neither.

THE NATURE OF USER-BASED ATTACKS

Typically, user-based attacks come in two flavors: a disgruntled employee or a hacker using stolen credentials. These attacks are usually the fault of an employee, knowingly or unknowingly; 82 percent of data breaches are caused by employee error.[1] Regardless, these individuals are able to bypass infrastructure-level defenses with their authentic login credentials. Once inside the system, these users begin to execute on their agenda.

User-based activity monitoring solutions were designed to provide insight on these threats from the perspective of the user. This technology can track every action taken by authenticated employees, vendors and partners, regardless of how they connect or which applications they access. And, it aggregates screen captures throughout the process to collect video footage on exactly who did what and when.

As it turns out, more than 67 percent of data breaches involve stolen credentials.[2] Even those hackers who start with information from low-ranking employees or vendors are capable of finding ways around internal roadblocks, disabling firewalls, extracting data and installing malware.

Analytics are the best defense against this type of attack. Comparing user actions against their known user profiles, job descriptions, usage patterns and other intelligence helps security teams quickly sniff out anomalous, suspicious and out-of-policy behaviors. For example, companies can quickly see if an employee or trusted vendor changed a firewall setting, executed a DROP command from a database or ran a screen-sharing application while looking at CRM records. Today's solutions are extremely sophisticated; they can even notify a hospital when a nonattending physician accesses the files of a patient or flag a vendor attempting to access a point-of-sale (POS) system.

THE IMPORTANCE OF IT FORENSICS FOR INCIDENT RESPONSE AND COMPLIANCE AUDITS

One of the most difficult tasks security professionals face is reconstructing what a hacker did once inside. Many IT departments rely on system log files to provide the details. Unfortunately, this approach is both time-consuming and full of knowledge gaps. System logs were not designed to provide a full accounting of user activity. Because they were created to provide developers with much needed intelligence on software defects, it is extremely hard for the average person to distinguish meaningful user information from system details. Not every application provides log files, which means that even those companies that aggregate all their log-based data using a central security information and event management (SIEM) system will have trouble piecing together a seamless, 360-degree view of user activity.

On the other hand, user activity monitoring solutions follow authenticated users as they travel the network, access files and use applications while also recording every keystroke, preference and option they select. Forensic investigators can simply play back video footage of exactly what a user did to gain empirical evidence of illegal activity. More important, companies can quickly identify the culprit—or at least the user whose credentials were compromised—and quickly shut

Do you have something to say about this article?

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

Go directly to the article:

down the account. And, they can see exactly what was stolen, which customer records were comprised and which systems are still vulnerable. Armed with this level of information, companies can more quickly rectify the situation.

As an added benefit, user activity monitoring solutions provide irrefutable evidence as to a company's compliance with Payment Card Industry (PCI), North American Electric Reliability Corporation (NERC), US Federal Energy Regulatory Commission (FERC), and US Health Insurance Portability and Accountability Act (HIPAA) regulations, among others governing the access and use of sensitive data.

WHAT TYPES OF ACTIVITY SHOULD BE MONITORED

For the most part, companies are not concerned about the personal lives of their employees. The exception, of course, is when that personal behavior can adversely affect corporate security. For that reason, every action a user takes after authentication—and while on the corporate network—should be monitored, recorded and stored. Hackers are extremely adept at covering their tracks and maintaining a low profile once inside. If the monitoring system were to stop monitoring while users went on Facebook or only track activity across specific programs, the gaps could provide key escape hatches for obscuring illegal behaviors. Although every action is being recorded, only suspicious activities should trigger alerts.

HOW TO COMMUNICATE MONITORING POLICIES

Companies must notify employees and any third-party users that their actions are being monitored. To start, organizations need a policies and procedures document that clearly defines what the company monitors, how that information is used and what constitutes acceptable behavior. Users should fully understand that all actions, including individual keystrokes, are recorded, but only those actions with security implications are scrutinized.

All users should be given policy information along with their login credentials. Depending on the size of the organization, human resources (HR) departments can include a review of this information during the employee orientation process.

Companies should also remind users that they are being monitored. Notifications and important policy messages can be built into the monitoring software and presented at user login. Requiring users to confirm before continuing ensures that policy messages have reached their targeted users.

THE CONCEPT OF IT DETERRENCE

Informing employees, vendors, partners and other users trusted with authentic credentials that they are being monitored goes a long way toward deterring abnormal, illegal and out-of-policy behavior. After all, someone is much less likely to commit an illegal act in front of a video camera.

FINDING THE RIGHT BALANCE

When it comes to security, companies need to use every available defense to protect valuable assets and sensitive information. While user activity monitoring is the best protection against the threat within, companies need to be smart about it. The key is communicating openly with employees and trusted third parties to ensure that they fully understand corporate initiatives, policies and procedures. Such a system is best used for incident response, compliance audits and, in fact, protecting a company's users themselves from being held accountable for actions a hacker may take with their account. Employees and partners should understand that this system is not designed for monitoring their day-to-day activity, snooping on their browsing history or making them feel scrutinized. With a balanced approach to monitoring and privacy, companies can deploy user activity monitoring solutions to protect themselves and their users.

ENDNOTES

[1] Fogarty, K.; "82% of Data Breaches Due to Staff Errors; 4% of IT Trusts Users; IT Is Still to Blame," *ITWorld*, 19 April 2012, *www.itworld.com/article/2729066/security/82--of-data-breaches-due-to-staff-errors--4--of-it-trusts-users--it-is-still-to-blame.html*

[2] Verizon, *2014 Data Breach Investigations Report*, March 2014, *www.verizonenterprise.com/DBIR/*

Understanding Software Metric Use

David Henderson is assistant professor of accounting in the College of Business at the University of Mary Washington (Fredericksburg, Virginia, USA). He can be reached at *dhender3@umw.edu.*

Steven D. Sheetz is associate professor of accounting and information systems in the Department of Accounting and Information Systems in the Pamplin College of Business at Virginia Tech (Blacksburg, Virginia, USA). He can be reached at *sheetz@vt.edu.*

Linda Wallace is associate professor of accounting and information systems in the Department of Accounting and Information Systems in the Pamplin College of Business at Virginia Tech (Blacksburg, Virginia, USA). She can be reached at *wallacel@vt.edu.*

In the early 1990s, the baggage claim system at Denver International Airport (Colorado, USA) was designed to automate baggage handling by using software to direct baggage contained in unmanned carts running on a track. Unfortunately, errors in the software that controlled the baggage claim system resulted in substantial cost overruns, delayed the opening of the new airport and eventually resulted in complete abandonment of the system. The Denver baggage claim project illustrates the catastrophic impact a failed software project can have on an organization.[1]

An effective software metrics program can help prevent software project failures, such as the Denver baggage claim project, by evaluating and monitoring project progress, thereby helping to identify problems before they worsen.[2] A software metric provides a quantitative indication of some attributes of software, such as size, complexity or quality. Examples of software metrics include function points, cyclomatic complexity and source lines of code. The potential of software metrics to increase control of the software development process naturally makes the appropriate use of software metrics a concern for IS auditors.[3] Without the appropriate use of software metrics, the software development process may be loosely controlled, thereby making it difficult for IS auditors to assess and monitor risk during software development.

Although software metrics can provide greater control over the software development process, resistance to them has resulted in inappropriate use and high failure rates for software metric initiatives.[4, 5, 6, 7] More than 80 percent of software metric initiatives fail within the first 18 months.[8] Even when software metrics are used, development teams often use them inappropriately.[9] For example, despite arguments from the research community about why source lines of code (SLOC) are a poor measure of software size, development teams still commonly use them to assess productivity and provide cost and schedule estimates.[10] The improper application of a software metric, such as SLOC, can quickly lead to project failure if it produces flawed estimates.

One possible reason for resistance to software metrics is that members of a development team may not perceive the advantages of using software metrics. Development teams must perceive software metrics as useful; otherwise, they may use them reluctantly and inappropriately.[11, 12]

Another potential reason for resistance to software metrics is that different groups involved in software metrics initiatives (managers, developers and metrics coordinators) use software metrics for different reasons, implying that they have different perceptions about software metrics. When groups have varying perspectives of a technology, organizations may experience difficulty developing, implementing and using the technology.[13] These differences in perception among different stakeholders on a software metrics initiative could lead to communication problems and, ultimately, resistance to use.

Resistance to software metrics initiatives should concern IS auditors. Strong opposition to software metrics can result in inappropriate or unenthusiastic use or even deliberate obstruction of software metrics initiatives. Inappropriate or unenthusiastic use, in turn, may result in a less-controlled and riskier software development process. Since software metrics mitigate risk and increase control of the software development process, IS auditors should ensure that development teams use software metrics appropriately and determine whether groups within development teams perceive the benefits of software metrics differently.

Motivated by these issues, 126 managers, developers and metrics coordinators were surveyed to determine whether they understand the benefits of using software metrics and whether they perceive the benefits of software metrics differently. The results suggest managers, developers and metrics coordinators may not fully appreciate the benefits of software metrics and also indicate that these three groups perceive the benefits of software metrics differently.

IS AUDITORS AND SOFTWARE METRICS

Software development is fraught with risk, including variations in project scope, time overruns, cost overruns and inappropriate

resourcing/staffing model management. Software metrics can help mitigate the risk by serving as effective monitoring tools, thereby helping to mitigate risk and increase control of the software development process. For example, software metrics, such as function points, can help management plan software development projects, allocate resources, monitor software project progress, and watch for schedule and cost overruns.[14] Other software metrics, such as tracking defects per line of code, can help development teams ensure high software quality.[15]

The potential of software metrics to mitigate risk during the software development process, coupled with the IS auditor's responsibility to ensure that the development process is timely and cost-effective, makes the appropriate use of software metrics a concern for IS auditors. If development teams fail to use metrics appropriately, either because they fail to appreciate the benefits of metrics or because groups within the development team perceive the benefits of metrics differently, the development process may be loosely controlled. Accordingly, IS auditors should ensure that key software metrics have been established to measure the performance of the project team and the project and then take steps to ensure that metrics are used appropriately throughout the project.[16, 17] Furthermore, IS auditors should review service level agreements (SLAs) to determine if they utilize metrics that are monitored and measured.[18]

SURVEY DESIGN

To develop a framework for understanding whether managers, developers and metrics coordinators understand the benefits of using software metrics, prior research was reviewed to uncover the characteristics (i.e., the desirable properties) of effective software metrics. **Figure 1** lists the desirable properties of software metrics.[19]

This list of desirable properties formed the basis for the web-based survey. When completing the survey, respondents were asked to identify a software metric with which they were familiar and then respond to the questions developed from the desirable properties about that software metric. Survey

Figure 1—Desirable Properties of Software Metrics

Desirable Properties of Software Metrics	Definition	No. of Questions
Automatibility	The degree to which the collection of data for the metric and the metric's calculation are computerized	4
Calculation ease	The degree to which the value of the metric is easy to calculate	3
Data availability	The degree to which the data required to calculate the metric are readily available given the products and processes currently used	3
Intuitiveness	The degree to which the metric's behavior conforms to intuition	1
Language independence	The degree to which computation of the metric does not depend on the programming language used	3
Life cycle applicability	The degree to which the metric can be applied throughout the SDLC	4
Normativeness	The degree to which there is a standard, typical or normal range of "acceptable" values for the metric	3
Predictiveness	The ability of the software metric to estimate an important attribute to be realized in the future; for management metrics, the ability of the metric to provide accurate software size and effort estimates; for quality metrics, the ability of the metric to predict software quality	1
Prescriptiveness	The ability of the software metric to not only diagnose problems, but suggest solutions; for management metrics, the ability of the metric to help diagnose problems in the software development process and make changes accordingly (e.g., increase resources to improve schedule performance); for quality metrics, the ability of the metric to help diagnose problems in software quality and recommend solutions accordingly	4
Sensitivity	The degree to which the metric is sensitive to changes in the attribute(s) measured	1
Timeliness	The degree to which the metric provides feedback in time to affect the outcome	1
Understandability	The degree to which the metric is easy to understand; the degree to which the metric is free of mental effort	2
Validity	The degree to which the software metric assesses the attributes it purports to measure; the degree to which it has been empirically tested and supported	4

question responses were measured on a five-point rating scale ranging from one to five, in which one equaled strongly disagree, three equaled undecided and five equaled strongly agree. **Figure 2** lists the survey items.

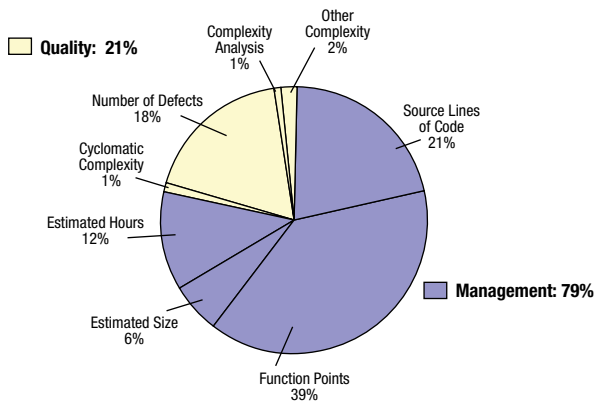
Data were collected from three different sources over a six-month period. The first source consisted of members of a computer software metric Usenet group. The second source included members of the Information Systems Special Interest Group of the Project Management Institute (PMI-ISSIG). Additional participants were employees of a large IT consulting company. The final sample consisted of 126 managers, developers and metrics coordinators.

Figure 2— Survey Items

Desirable Property	Survey Item
Automatibility	The data required to calculate the measure can be automatically collected.
Automatibility	The measure can be calculated by a computer program.
Automatibility	A computer program can interpret the measure.
Automatibility	Data collection and calculation of the measure can be automated.
Calculation ease	The calculation of the measure is straightforward.
Calculation ease	The measure is easy to calculate.
Calculation ease*	Calculating the measure is often frustrating.
Data availability	The data required to calculate the measure are readily available in the current software development environment.
Data availability	Analysis of the measure can be performed using data from the existing software development process.
Data availability	The measure can be calculated without having to collect additional data.
Intuitiveness	The measure behaves according to intuition.
Language independence	The measure is programming-language-independent.
Language independence	The choice of programming language does not affect the ability to calculate the measure.
Language independence	The calculation of the measure is not affected by the differences in programming languages.
Life cycle applicability	The measure can readily be used throughout the entire development process.
Life cycle applicability	The measure can easily be used repeatedly throughout a development process.
Life cycle applicability	The measure can support development in early and later stages.
Life cycle applicability	The measure can be easily applied to designs, specifications and software.
Normativeness	The measure has a well-known range of acceptable values.
Normativeness	The measure has established standards that can be used to interpret measured values.
Normativeness	A standard range of values for the measure is known.
Predictiveness	The measure improves the ability to predict success.
Prescriptiveness	The measure improves the ability to identify problems with the software.
Prescriptiveness	The measure makes it easier to identify methods for improving the software.
Prescriptiveness	The measure increases the ability to identify new procedures that should be followed.
Prescriptiveness	It is easier to solve problems when using the measure.
Sensitivity	The measure is highly sensitive to changes in the software.
Timeliness	The measure can be used in time to improve the software.
Understandability	The measure is easy to understand.
Understandability	The use of the measure requires little mental effort.
Validity	The measure has been rigorously tested in the field.
Validity	The measure has been extensively empirically validated.
Validity	The measure is highly credible.
Validity	The scale of the measure is appropriate.
*Denotes reverse-coded item	

The software metrics identified by the respondents were categorized as either management or quality metrics, and the data analysis was conducted along those dimensions. Software metrics typically used to control the software development process, such as function points and SLOC, were classified as management metrics. Software metrics used to monitor software quality, such as cyclomatic complexity and number of defects, were classified as quality metrics. **Figure 3** shows the software metrics identified by the participants, their respective categorization as quality or management, and the percentage of respondents who identified each software metric.

Figure 3—Software Metrics Identified by Type



After categorizing the metrics identified by the survey respondents as quality or management, the job codes provided by each participant as manager, developer or metrics coordinator were classified. **Figure 4** shows position titles identified by the respondents and their subsequent mapping to the manager, developer and metric coordinator categories, along with the percentage of respondents they represent. The average respondent was 44 years old with 19 years of experience in the software industry and had used software metrics for 5.8 years. Of the 126 participants, 62 were managers, 45 were developers and 19 were metrics coordinators. Managers, developers and metrics coordinators had approximately the same amount of experience and were similar in age.

RESULTS

The average scores for each desirable property for each metric were then analyzed. **Figure 5** presents the average scores for each question for quality metrics. **Figure 6** presents the average scores for each desirable property for management metrics.

As indicated by the scores in **figure 5**, the average scores for all groups for all desirable properties except one (intuitiveness) are slightly higher than three (undecided), suggesting that while metrics coordinators, developers and managers generally perceive the value of quality metrics, they do not overwhelmingly believe in the value of quality metrics. Metrics coordinators generally have the most favorable perceptions

Figure 4—Mapping of Job Categories to Manager, Developer and Metric Coordinator Groups

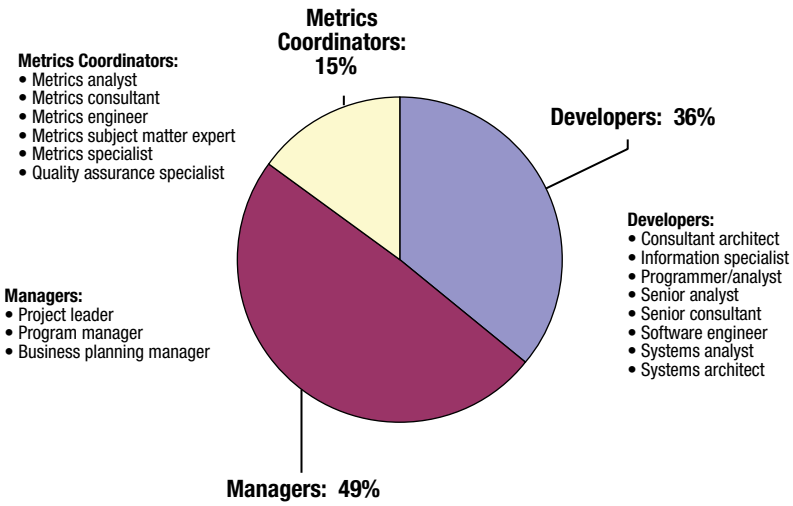


Figure 5—Average Scores by Desirable Property for Quality Metrics				
Property	**All Job Codes**	**Metrics Coordinators**	**Developers**	**Managers**
Automatibility	3.80	4.00	3.81	3.72
Calculation ease	3.91	4.27	3.70	3.92
Data availability	3.80	4.00	3.81	3.72
Intuitiveness	**2.89**	**2.92**	**2.89**	**2.92**
Language independence	4.11	4.53	3.93	4.08
Life cycle applicability	4.13	4.50	4.19	3.94
Normativeness	**3.49**	3.93	3.52	**3.31**
Predictiveness	4.15	4.00	4.11	4.23
Prescriptiveness	3.99	4.15	4.08	3.87
Sensitivity	3.67	4.40	**3.33**	3.62
Timeliness	4.22	4.60	4.11	4.15
Understandability	3.67	3.60	3.61	3.73
Validity	3.83	4.15	3.75	3.77
Average	3.82	4.08	3.76	3.77
Bold=below 3.5				

Figure 6—Average Scores by Desirable Property for Management Metrics				
Property	**All Job Codes**	**Metrics Coordinators**	**Developers**	**Managers**
Automatibility	**3.21**	**3.34**	**2.98**	**3.35**
Calculation ease	3.52	3.90	**3.48**	**3.44**
Data availability	3.68	4.19	3.63	3.56
Intuitiveness	**2.96**	**3.07**	**3.08**	**2.84**
Language independence	3.53	**3.24**	4.08	**3.21**
Life cycle applicability	3.99	4.32	4.16	3.78
Normativeness	3.65	3.86	3.62	3.62
Predictiveness	3.79	4.14	3.97	3.55
Prescriptiveness	**3.23**	**3.25**	**3.38**	**3.12**
Sensitivity	3.55	4.36	**3.11**	3.63
Timeliness	3.62	3.86	3.75	**3.45**
Understandability	**3.32**	3.79	**3.18**	**3.29**
Validity	3.91	4.23	3.92	3.81
Average	3.54	3.81	3.57	**3.43**
Bold=below 3.5				

of quality metrics, as they have the highest average scores for every desirable property, except for understandability and predictiveness. It is surprising that developers did not perceive quality metrics more favorably, given that these metrics are used to monitor software quality. All three groups indicated that quality metrics are not intuitive (average is less than three), suggesting that training programs may be needed in the beginning of a software metrics implementation.

As shown in **figure 6**, no scores for any desirable property for all job codes exceeded four (agree), indicating that these groups, as a whole, do not completely appreciate the benefits of management metrics. Similar to the findings for quality metrics, metrics coordinators typically have more favorable views of management metrics than managers. Unlike the findings for quality metrics, developers perceive higher value of management metrics than managers. This result is counterintuitive given

that managers should be more reliant on management metrics than developers, as these metrics are used for monitoring productivity. The average scores for management metrics for the prescriptiveness desirable property are slightly higher than three (undecided) for all groups. This finding is surprising given that management metrics should be useful for diagnosing problems in the software development process (e.g., increase resources to improve schedule performance); thus, prescriptiveness should be a main reason for using management metrics. Furthermore, management metrics are not perceived as intuitive, suggesting that additional training on management metrics may be useful.

IMPLICATIONS AND RECOMMENDATIONS FOR IS AUDITORS

These results indicate that managers, developers and metrics coordinators may not fully understand the benefits of management metrics. Management metrics, such as function points, should help managers, developers and metrics coordinators recognize problem areas in the software and suggest solutions accordingly. Thus, it would be expected that all three groups would use management metrics for their prescriptiveness. Interestingly, however, all three groups were undecided about the prescriptiveness of management metrics. This finding should be a concern for IS auditors as it suggests that managers, developers and metrics coordinators may not fully appreciate the benefits of using management metrics, which, in turn, may cause inappropriate use of software metrics.[20, 21] Furthermore, all three groups seem to perceive quality metrics more favorably than management metrics. Given that management metrics, such as function points, should be established to monitor and control the systems development process,[22] IS auditors should, therefore, ensure that members of a development team appreciate the value of software metrics. IS auditors can accomplish this task via observation, inquiries, and taking an active, yet independent, role in the systems development process.[23]

Previous studies on software metrics have found that managers perceive software metrics as more useful than developers.[24] On the contrary, this survey found that developers and metrics coordinators better understand the benefits of management metrics, more so than managers. Given that managers use management software metrics, such as function points to provide software size estimates, it would be expected that managers, more so than developers, use management metrics to predict level of effort and software size. Results, however, indicate that managers do not use management metrics for their predictiveness or prescriptiveness. This finding is a concern for IS auditors as it suggests that managers may not understand the value of management metrics, which could lead them to use software metrics inappropriately. Using software metrics inappropriately, in turn, can hinder the ability to control the software development process and mitigate risk. IS auditors should, therefore, ensure, via observation and interviewing techniques, that management understands the value of software metrics and is using the appropriate software metrics.

Survey results also show that managers, developers and metrics coordinators perceive the benefits of software metrics differently. As mentioned previously, metrics coordinators and developers appear to have more favorable perceptions of software metrics than managers. IS auditors should be aware that these groups perceive software metrics differently and that these differences in perceptions can lead to opposition against software metrics. IS auditors should monitor the perceptual differences between these groups and ensure that these differences in perception do not result in inappropriate use. Accordingly, IS auditors should take an active role in the software development process and ensure that effective communication between different groups on the development team is occurring and that each group appreciates the values of the other groups.

CONCLUSION

To raise awareness of the benefits of software metric use and potentially improve communication among managers, developers and software metrics coordinators during software metrics initiatives, organizations should develop integrated and comprehensive education and training programs. Education and training efforts should include an overview of the potential benefits to all groups, followed by a focus on those characteristics of using software metrics tailored to each group. For example, metrics coordinators do not use management metrics for a range of issues important to managers and developers, including predictiveness; thus, metrics coordinators could, instead, be instructed on the predictiveness benefits of management metrics. Additionally, members of all three groups may benefit from training in communication techniques that emphasize understanding the views of others and communicating using the target audience's concepts and terminology. IS auditors can play a

role in these education and training efforts by ensuring that metrics coordinators, developers and managers have received adequate training on the benefits of using software metrics.

Another strategy for increasing the effectiveness of software metrics initiatives is to use a dedicated metrics team to facilitate the implementation of software metrics programs.[25, 26] These survey results indicate that metrics coordinators perceive the value of metrics more than managers and developers. Metrics coordinators, who serve as liaisons between managers and developers during software metrics initiatives, are particularly well positioned within the organization to fill this role and, hence, can help managers and developers better understand the benefits of software metrics. Further, IS auditors should ensure that the organization has a dedicated metrics team to assist with the implementation of software metrics initiatives.

Although implementing education and communication programs may improve awareness of the benefits of software metrics and potentially increase use, it may be that more effective software metrics are needed with clearly defined goals. This survey indicates that quality metrics are not used for their ability to identify problems with software quality, potentially implying that managers, developers and metrics coordinators believe prescriptive quality metrics simply do not exist. Perhaps efforts should not only be directed toward education and training, but also toward developing software metrics that more practitioners perceive as predictive and prescriptive.

ENDNOTES

1 Calleam Consulting, "Case Study—Denver International Airport Baggage Handling System—An Illustration of Ineffectual Decision Making," 2008, *http://calleam.com/WTPF/?page_id=2086*

2 Ewusi-Mensah, K.; "Critical Issues in Abandoned Information Systems Development Projects," *Communications of the ACM*, vol. 40, iss. 9, 1997, p. 74-80

3 ISACA, *CISA Review Manual 2014*, USA, 2013, *www.isaca.org/bookstore*

4 Rubin, H.; "Measure for Measure," *Computerworld*, vol. 25, 15 April 1991, p. 77-78

5 Roche, J.; M. Jackson; M. Shepperd; "Software Measurement Methods: An Evaluation and Perspective," 3rd Symposium on Assessment of Quality Software Development Tools, Washington DC, USA, June 1994

6 Jones, C.; *Applied Software Measurement: Assuring Productivity and Quality*, McGraw-Hill, 1991

7 Gopal, A.; M. S.Krishnan; T. Mukhopadhyay; D. R.Goldenson; "Measurement Programs in Software Development: Determinants of Success," *IEEE Transactions on Software Engineering*, vol. 28, iss. 9, 2002, p. 863-75

8 *Op cit*, Rubin

9 *Ibid.*

10 Fenton, N. E.; Martin Neil; "Software Metrics: Successes, Failures and New Directions," *Journal of Systems and Software*, vol. 47, iss. 2 and 3, 1999, p. 149-57

11 Hall, T.; Neil Fenton; "Implementing Effective Software Metrics Programs," *IEEE Software*, vol. 14, iss. 2, 1997, p. 55-65

12 Grady, R. B.; *Practical Software Metrics for Project Management and Process Improvement*, Prentice Hall, 1992

13 Orlikowski, W.; Debra Gash; "Technological Frames: Making Sense of Information Technology in Organizations," *ACM Transactions on Information Systems (TOIS)*, vol. 12, iss. 2, April 1994, p. 174-207

14 *Op cit*, ISACA, 2013

15 *Ibid*.

16 *Ibid*.

17 ISACA, *Systems Development and Project Management Audit/Assurance Program*, 2009, *www.isaca.org/auditprograms*

18 *Ibid*.

19 Henderson-Sellers, B.; *Object-Oriented Metrics: Measures of Complexity*, Prentice-Hall, 1996

20 *Op cit*, Hall and Fenton

21 *Op cit*, Grady

22 *Op cit*, ISACA, 2009

23 Henderson, D.; "Issues With Auditing the Systems Development Process," *ISACA Journal*, vol. 6, 2008, p. 42, *www.isaca.org/journal*

24 Sheetz, S. D.; D. Henderson; L. Wallace; "Understanding Developer and Manager Perceptions of Function Points and Source Lines of Code," *The Journal of Systems & Software*, vol. 82, iss. 9, 2009, p. 1540-9

25 *Op cit*, Hall and Fenton

26 *Op cit*, Grady

Auditing SQL Server Databases Using CAATs

Ian Cooke, CISA, CGEIT, CRISC, COBIT Foundation, CFE, CPTS, DipFM, ITIL-F, Six Sigma Green Belt, is an IT audit manager based in Dublin, Ireland, with more than 25 years of experience in all aspects of information systems. A member of ISACA's Communities Committee, he is also the topic leader for the Oracle Databases, SQL Server Databases and OS/400 discussions in the ISACA Knowledge Center. Cooke welcomes comments or suggestions at *ian.j.cooke@gmail.com* or on the SQL server topic in the ISACA Knowledge Center.

There are a variety of commercial security tools[1] available to audit Microsoft (MS) SQL Server databases. However, there can be instances when their application is not practical, including:

- For smaller companies in which the cost may be prohibitive
- For larger holding companies or geographically dispersed companies that do not have full network connectivity between the centre and its subsidiaries
- For consultancies performing external reviews that are not given permission to install or run tools that require full database administrator privileges and, hence, the administrator password. Furthermore, the audited entity has no oversight of what the tool does or what effect it is likely to have on mission-critical databases.

The following approach to auditing MS SQL Server databases using computer-assisted audit techniques (CAATs) in conjunction with information taken directly from the MS SQL Server database offers a solution to the issues identified. It describes a cost-effective solution for auditing MS SQL Server databases to a company's own standards using tools already available in the enterprise.

SQL SERVER DATABASES

All MS SQL Server installations contain information about the installed databases. To retrieve the information, one must understand how it is stored and the tools available to extract it.

- **SQL server catalog views**—MS SQL Server databases contain information about data known as catalog metadata. This provides details about the database's configuration options, users, objects and more. Catalogue metadata are accessed through catalog views. Catalogue views provide an organised view of the catalog metadata. The views are grouped into categories, one of which is security. A full list of the catalog views along with more detailed explanations may be found on Microsoft's Developer Network.[2]
- **SQL Server Management Studio**—This is a tool for accessing, configuring, managing, administering and developing SQL server databases. It also allows users to query the database using SQL, formatting the output as desired and writing the results to file (if required).
- **SQL server structure**—Each instance of the MS SQL Server has four system databases (master, model, tempdb and msdb) and one or more user databases.[3] Security is built around the master/server level (server roles) and the user database level (database roles).

OUTPUTTING SQL SERVER CATALOG VIEWS

Figure 1 offers an example of an MS SQL Server script (a full script can be downloaded from the ISACA® Knowledge Center[4]). Once generated, these scripts can be transferred to the database administrator to be run over the required database(s). One comma-separated values (CSV) file is produced for each server-level view. A CSV file is also produced for each database-level view, but it contains separate output for all installed databases (the required setup, formatting and configuration options are described in **figure 2**).

ANALYSING SQL SERVER CATALOG VIEWS

The files can then be imported into CAATs tools for analysis and comparison. Examples of MS SQL Server catalog views include:

- **Configurations**—The entity being audited should have a policy on how its MS SQL Server databases are configured. Much of the configuration is reflected in the MS SQL Server parameters, which can be retrieved from the sys.configurations catalog view. Examples of parameters include those for enabling the command shell or allowing client applications on remote computers to use an administrator connection (a full list of SQL server configuration options exists on Microsoft's Developer Network[5]).

Figure 1—SQL Script Output to CSV Text Files

```
-- Be sure you are in SQL Command Mode
-- Replace the output destination "C:\SQLAUDIT\" as required

set nocount on

-- (a) SQL Server Configuration, output to SYS_Configuration.txt
:OUT C:\SQLAUDIT\SYS_Configuration.TXT
SELECT * FROM SYS.CONFIGURATIONS

GO

-- (b) Authenticated Users / roles, output to SYS_SERVER_PRINCIPALS.txt
:OUT C:\SQLAUDIT\SYS_Server_principals.TXT
SELECT * FROM SYS.SERVER_PRINCIPALS

GO

-- (c) SQL Logins, output to SYS_SQL_LOGINS.txt
:OUT C:\SQLAUDIT\SYS_SQL_Logins.TXT
SELECT * FROM SYS.SQL_LOGINS

GO

-- (d)Server Role Members (links with principals above), output to SYS_SERVER_ROLE_MEMBERS.txt
:OUT C:\SQLAUDIT\SYS_Server_role_members.TXT

SLECT a.role_principal_id, b.name as role_principal_name, a.member_principal_id, c.name as member_principal_name
FROM (sys.server_role_members a INNER JOIN sys.server_principals b ON
a.role_principal_id = b.principal_id)
INNER JOIN sys.server_principals c ON
a.member_principal_id = c.principal_id;

GO

-- All other databases -------------------------------------

-- (e) Database principals, output to DATABASE_PRINCIPALS.txt
:OUT C:\SQLAUDIT\DATABASE_PRINCIPALS.TXT
EXEC sp_MSforeachdb 'USE ? SELECT ''?'' as database_name, * FROM SYS.DATABASE_PRINCIPALS'

GO

-- (f) Database Role Members (links with principals above), output to MASTER_DATABASE_ROLE_MEMBERS.txt
:OUT C:\SQLAUDIT\DATABASE_ROLE_MEMBERS.TXT
EXEC sp_MSforeachdb 'USE ? SELECT ''?'' as database_name, a.role_principal_id, b.name as role_principal_name,
a.member_principal_id, c.name
FROM (sys.database_role_members a INNER JOIN sys.database_principals b ON
a.role_principal_id = b.principal_id)
INNER JOIN sys.database_principals c ON
a.member_principal_id = c.principal_id'

GO
```

Source: Ian Cooke. Reprinted with permission.

Figure 2—Formatting and Configuration Requirements

Component	Description
SQL server command mode	By using the Database Engine Query Editor in MS SQL Server Management Studio, one can write and edit queries as SQLCMD scripts. Use SQLCMD scripts when it is necessary to process Windows system commands and Transact-SQL statements in the same script.[6] Here it is used to output to selected file(s). Ensure that SQLCMD Mode is selected.
Output to text file	Right click on the SQLCMD line (:OUT) in SQLCMD mode and choose query options, 'select text'. Select output format 'comma delimited', and check 'include column headers in the result set' (see **figure 3**).
sp_MSForEachDB	The undocumented stored procedure 'For Each Database' comes with the MS SQL Server and can be found in the master database. It is used to process a single SQL query against all installed databases. In this instance, a query over a database catalog view is run over all databases.

Source: Ian Cooke. Reprinted with permission.

As noted, this catalogue view can be output to a CSV file. A sample output from the configuration's CSV file can be seen in **figure 3**. The first line shows the MS SQL Server field names. The field name relates to the defined layout for the configurations catalogue view.[7] (The layout for all SQL server catalogue views are available on Microsoft's Developer Network.[8])

All common CAATs tools (as well as Microsoft Excel and Microsoft Access) allow for the importation of CSV files. Once the configurations are imported to the CAATs tool, they can be analysed for compliance to the entity's standards. These standards could be based upon any source of assurance for an MS SQL Server database,[9] e.g., the Center for Internet Security Benchmarks,[10] or a document developed by the entity. (ISACA's *Microsoft SQL Server Database Audit/Assurance Program*[11] does not use catalogue views, although the items could be tested by referencing them.)

Once one database is analysed and known to be compliant to required standards, it can be used as a 'master configuration' using the CAATs tool to compare the configurations of interest across all of the organisation's MS SQL Server databases. This can be done by joining the field configuration_id displaying all records where the value is not equal. In this manner, noncompliant configurations are quickly flagged for follow-up and review.

If required, the review of the configurations can be repeated periodically. This would allow changes to be tracked and used as part of a continuous monitoring audit programme.

- **Server principals**—An MS SQL Server provides two methods of authenticating to the database: Windows authentication or mixed mode.[12] Windows authentication uses MS Windows security to validate all of the database accounts and passwords against the Windows operating system. It is the mode recommended by Microsoft.[13] Mixed mode allows for both Windows authentication and MS SQL Server authentication. With MS SQL Server authentication, an explicit user account and password are required to access the database.

  The entity being audited should have a policy on how these passwords are configured. For Windows authentication, these will be as per the Windows server. From Windows Server 2003 onwards, mixed mode can be configured to validate the password against the Windows server.[14] In a mixed mode environment, the mode in use for a given user can be seen in the sys.server_principals catalogue view (**figure 1** [b]). The field 'type' will be 'S' for an SQL login or 'U' for a Windows login.

  From SQL Server 2005 onwards, the password hashes for SQL login users are stored in the view sys.sql_logins catalogue view.[15] To audit the passwords, one must request that the MS SQL Server database administrator output the contents of the view (**figure 1** [c]) to a CSV file, as discussed. Once one has the password hashes, these can be validated by running them through a password cracking tool, e.g., Hashcat.[16]

  In an MS SQL Server, anything that can be granted a right to perform an activity is called a principal. So, fundamentally, principals include logins, users and roles, for example. Principals can also be separated into server principals and database principals.[17]

Figure 3—(Modified) Configurations Sample Output

```
URATION_ID,NAME,VALUE,MINIMUM,MAXIMUM,VALUE_IN_USE,DESCRIPTION,IS_DYNAMIC,IS_ADVANCED
allow updates                ,0,0,1,0,   Allow updates to system tables
remote access                ,1,0,1,1,   Allow remote access
remote admin connections     ,0,0,1,0,   Dedicated Admin Connections are allowed from remote clients
Agent XPs                    ,1,0,1,1,   Enable or disable Agent XPs
SQL Mail XPs                 ,0,0,1,0,   Enable or disable SQL Mail XPs
Database Mail XPs            ,0,0,1,0,   Enable or disable Database Mail XPs
SMO and DMO XPs              ,1,0,1,1,   Enable or disable SMO and DMO XPs
Ole Automation Procedures    ,0,0,1,0,   Enable or disable Ole Automation Procedures
Web Assistant Procedures     ,0,0,1,0,   Enable or disable Web Assistant Procedures
xp_cmdshell                  ,0,0,1,0,   Enable or disable command shell
Ad Hoc Distributed Queries   ,0,0,1,0,   Enable or disable Ad Hoc Distributed Queries
Replication XPs              ,0,0,1,0,   Enable or disable Replication XPs
```

Source: Ian Cooke. Reprinted with permission.

Permissions are what allow principals to perform activities in an MS SQL Server. Depending on the scope, the permission granted is either a server permission or a database permission.

Roles are used to group together permissions or other roles. They are a means of facilitating the granting of multiple permissions or roles to users. An MS SQL Server provides some predefined roles to help in database administration. Fixed server roles[18] are defined at the server level and have server-level permissions.[19] They cannot be added, removed or changed. Each member of a fixed server role can add other users to the role. Since MS SQL Server 2012, one can also create user-defined server roles.[20]

Fixed server roles can also be seen in the sys.server_principals view (the field 'type' is 'R'), while the users who have been allocated the fixed server roles can be seen in the sys.server_role_members view (**figure 1** [d]). These should be reviewed for appropriateness and separation of duties.

- **Database principals**—Fixed database roles[21] are defined at the database level and exist in each database. Members of the db_owner and db_securityadmin database roles can manage fixed database role membership; however, only members of the db_owner database role can add members to the db_owner fixed database role.[22]

User-defined (or flexible) database roles allow one to create one's own roles. After a role is created, one can configure the database permissions of the role by using grant, deny and revoke, for example.

Using the sys.database_principals view via the sp_MSforeachdb stored procedure (**figure 1** [e]), one can obtain a list of the database roles in use for each database. The users allocated these roles can be retrieved from sys.database_role_members (**figure 1** [f]). These should also be reviewed for appropriateness and separation of duties.

As there are many MS SQL Server catalog views, it is not possible to discuss them all in this article. Those mentioned previously are for illustration purposes. The views used depend on the purpose of the audit, but could also include:

- **Sys.databases**, which lists all the installed databases. This could be used to ensure that all databases are required, in use, and secured, and that there is a separation between test and live databases.
- **Sys.server_permissions**, which lists all the permissions that have been defined at the server level. This could be reviewed to ensure that the server permissions are appropriate.

- **Database_permissions**, which lists all the permissions that have been defined at the database level. This could be reviewed to ensure that the database permissions are appropriate.
- **Database_objects**, which lists all the objects for a given database. This could be cross-checked with permissions to ensure that the database permissions are appropriate.

A full list of MS SQL Server catalog views, including those for auditing and encryption, along with more detailed explanations can be found on Microsoft's Developer Network.[23]

The key point is that any of the views may be output to CSV files and imported into a CAATs tool. These may then be:

- Compared to other SQL server databases, including a master that one knows to be compliant to one's standards
- Compared to development, test or QA versions of the production database (useful for change control)
- Compared to other sources of data, including data from internal or external entities

BENEFITS OF CAATS FOR SQL SERVER DATABASES

Benefits of the proposed CAATs solution for auditing MS SQL Server databases include cost, as many organisations are already using CAATs software. The approach also allows for total transparency as the database administrator of the audited entity can review the SQL that is being run over the database to ensure that it will have no adverse effects on the production environment. Furthermore, the approach allows external consultants and geographically dispersed companies to request that the queries are run by the local database administrator without the need to compromise security (the administrator password) or install any additional software. Once the queries have been run,

they can be securely transferred for analysis. Query results can be compared against other databases from the audited entity or known compliant (master) databases to highlight areas of audit concern. Query results can also be compared against preproduction databases and other sources of data, such as the company payroll. Finally, the entire process can be repeated, reconfigured (if required) and used as part of a continuous monitoring and/or audit.

ENDNOTES

[1] TechTarget, SQL Server security test checklist, *http://searchsqlserver.techtarget.com/feature/SQL-Server-security-test-checklist*

[2] Microsoft Developer Network, 'Catalog Views (Transact-SQL)', *http://msdn.microsoft.com/en-us/library/ms174365(v=sql.100).aspx*

[3] Microsoft TechNet, Database Architecture, *http://technet.microsoft.com/en-us/library/aa214422(v=sql.80).aspx*

[4] ISACA, Knowledge Center, Outputs SQL Server Files CSV, 2013, *www.isaca.org/Groups/Professional-English/sql-servers/GroupDocuments/SQL%20Server%20Script%20New.SQL*

[5] Microsoft Developer Network, 'Setting Server Configuration Option's', *http://msdn.microsoft.com/en-us/library/ms189631(v=sql.100).aspx*

[6] Microsoft Developer Network, 'Edit SQLCMD Scripts With Query Editor', *http://msdn.microsoft.com/en-us/library/ms174187.aspx*

[7] Microsoft Developer Network, 'sys.configurations (Transact-SQL)', *http://msdn.microsoft.com/en-us/library/ms188345(v=sql.100).aspx*

[8] *Op cit*, Microsoft Developer Network, Catalog Views (Transact-SQL)

[9] ISACA, Knowledge Center, 'Sources of Assurance for a SQL Server Database', *www.isaca.org/Groups/Professional-English/sql-servers/GroupDocuments/Sources_of_Assurance_for_a_SQL_Server_Database_Update_2.pdf*

[10] Center for Internet Security, 'Security Benchmarks, Microsoft SQL Server 2008 R2 Database', 2012, *https://benchmarks.cisecurity.org/tools2/sqlserver/CIS_Microsoft_SQL_Server_2008_R2_Database_Engine_Benchmark_v1.0.0.pdf*

[11] ISACA, *Microsoft SQL Server Database Audit/Assurance Program*, 2011, *www.isaca.org/auditprograms*

[12] MSSQLTips.com, 'How to Check SQL Server Authentication Mode Using T SQL and SSMS', *www.mssqltips.com/sqlservertip/2191/how-to-check-sql-server-authentication-mode-using-t-sql-and-ssms/*

[13] Microsoft TechNet, 'Choosing an Authentication Mode', *http://technet.microsoft.com/en-us/library/ms144284(v=sql.100).aspx*

[14] MSSQLTips.com, 'SQL Server Login Properties to Enforce Password Policies and Expiration', *www.mssqltips.com/sqlservertip/1088/sql-server-login-properties-to-enforce-password-policies-and-expiration/*

[15] Microsoft Developer Network, 'Sys.sql_logins (Transact-SQL)', *http://msdn.microsoft.com/en-us/library/ms174355(v=sql.100).aspx*

[16] Hashcat.net, *http://hashcat.net/hashcat/*

[17] Microsoft Developer Network, 'Principals (Database Engine)', *http://msdn.microsoft.com/en-us/library/ms181127(v=sql.100).aspx*

[18] Microsoft Developer Network, 'Permissions of Fixed Server Roles (Database Engine)', *http://msdn.microsoft.com/en-us/library/ms175892(v=sql.100)*

[19] MSSQLTips.com, 'Understanding SQL Server Fixed Server Roles', *www.mssqltips.com/sqlservertip/1887/understanding-sql-server-fixed-server-roles/*

[20] Microsoft TechNet Magazine, 'SQL Server: User-defined Roles', *http://technet.microsoft.com/en-us/magazine/hh641407.aspx*

[21] Microsoft Developer Network, 'Permissions of Fixed Database Roles (Database Engine)', *http://msdn.microsoft.com/en-us/library/ms189612(v=sql.100)*

[22] MSSQLTips.com, 'Understanding SQL Server Fixed Database Roles', *www.mssqltips.com/sqlservertip/1900/understanding-sql-server-fixed-database-roles/*

[23] *Op cit*, Microsoft Developer Network, 'Catalog Views (Transact-SQL)'

Audit Accounting Data Using Excel Pivot Tables

An Aging of Accounts Receivable Example

Joshua J. Filzen, Ph.D., CPA, is an assistant professor of accounting in the College of Business at the University of Nevada (USA). He can be reached at *jfilzen@unr.edu.*

Mark G. Simkin, Ph.D., is a professor of information systems in the College of Business at the University of Nevada (USA). He can be reached at *markgsimkin@yahoo.com.*

Microsoft Excel's pivot table options provide powerful tools for aggregating and analyzing accounting data, but so does alternate software such as ACL. So why use pivot tables?

- **Convenience**—The data to analyze may already reside in a spreadsheet, the required analytical tools are already there, and no additional software is required.
- **Flexibility**—Pivot tables allow for an almost unlimited number of cross-tabulations in one, two or three dimensions, and this may be sufficient for the auditing tasks at hand.
- **Documentation**—The fact that, unless deleted, any pivot tables created become a permanent part of the same Excel workbook as the data on which it is based.
- **Many formatting options**—Auditors are not limited to a single prescribed format, but instead can present their analyses in a wide variety of designs and graphics.

The following examples demonstrate three variations of a common accounting task that is easily performed using pivot tables—creating an aging analysis of accounts receivable. The steps discussed apply equally to Excel 2010 and Excel 2013.

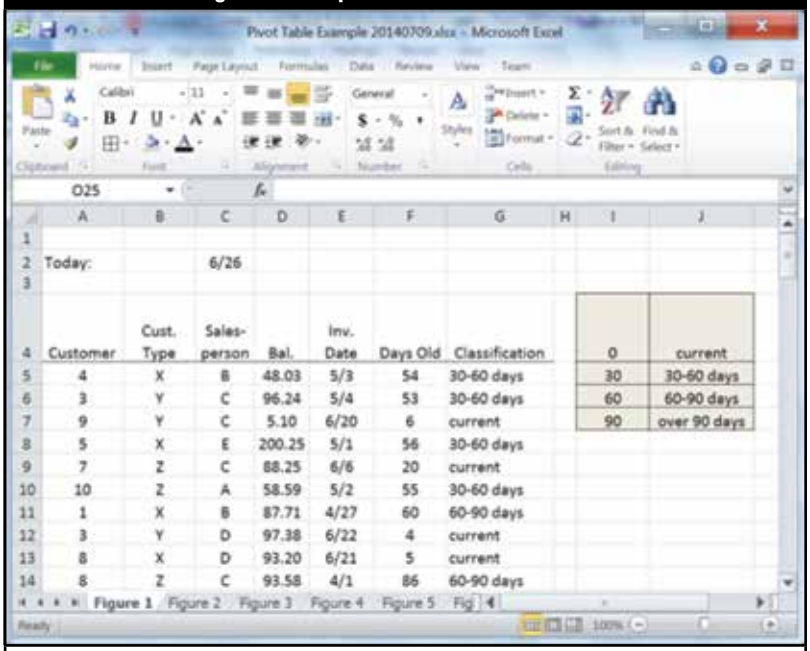
TASK 1: CREATING A ONE-DIMENSION AGING ANALYSIS

The (simplified) spreadsheet in **figure 1** contains the purchase records for 100 fictitious unpaid invoices, the first few of which are displayed. Each record includes information such as customer number, customer type, assigned salesperson, account balance (i.e., Bal.) and an invoice date (i.e., Inv. Date). What a manager or auditor might desire is an aging report that summarizes these data in order to assess the collectability of customer accounts.

At first, the data might not include computations for determining the age of the invoices (columm F in **figure 1**), but the spreadsheet can easily compute them as the difference between today's date (in cell C2) and the invoice date, formatted to a number format. For example, the formula for cell F5 is: = $C$2 - E5. This formula uses an absolute cell reference for cell C2, so that it can be copied to the other cells in column F.

To classify the customer records into standard categories such as "current," "30-60 days" and so forth, the spreadsheet uses the data in cells I4:J7, which it treats as a VLookUp table.[1] To illustrate, the formula for cell G5 (for the first customer) is: =VLOOKUP(F5,$I$4:$J$7,2). In this formula, F5 is the value to look up; $I$4:$J$7 is the range of cells containing the VLookUp table; and the last value of "2" is the column

Figure 1—Sample Accounts Receivable Data



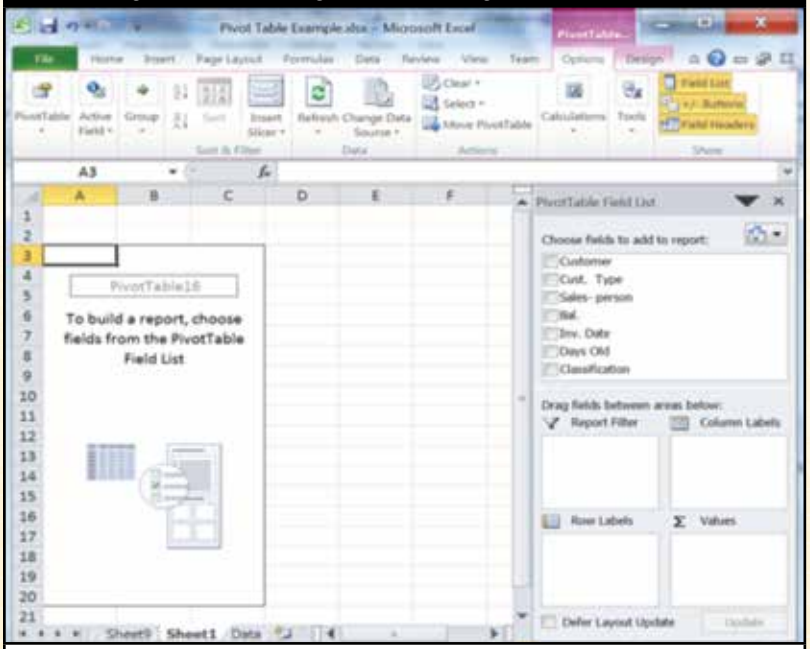
Source: Filzen and Simkin. Reprinted with permission.

Do you have something to say about this article?

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

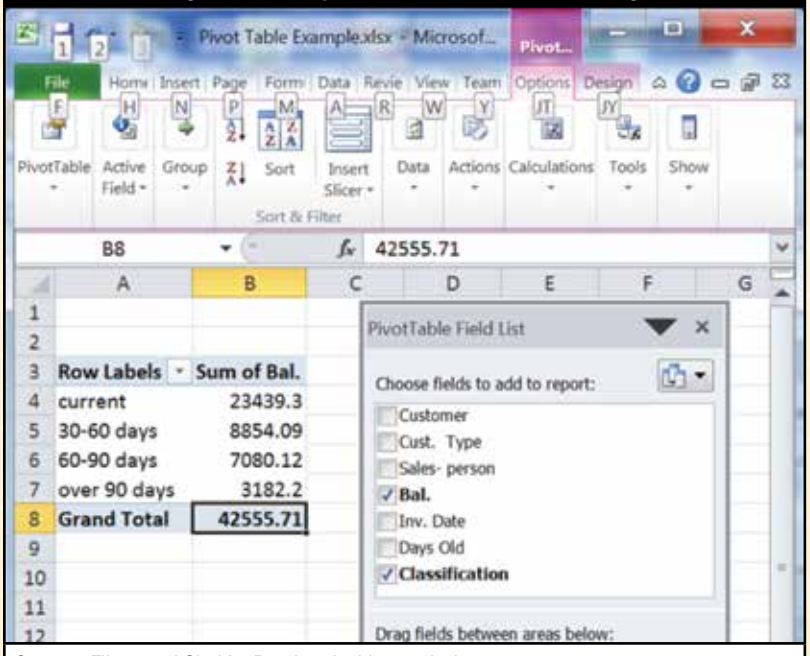
Go directly to the article:

Figure 2—The Starting Point for Creating a Pivot Table in Excel



Source: Filzen and Simkin. Reprinted with permission.

Figure 3—A Simple Pivot Table Without Formatting



Source: Filzen and Simkin. Reprinted with permission.

offset (i.e., the reference to the second column of the lookup table). To display conventional labels in the subsequent pivot table, the entries in the VLookUp table use the words "current," "30-60 days" and so forth, as shown in **figure 1**.

Because the coordinates of the lookup table are absolute cell addresses, the VLookUp formula can be copied to the other cells in column G. **Figure 1** shows the results. For example, because the age for first record is 54 days, its classification is "30-60 days," as desired. Similar computations produce similar results for the other cells in column G.

A pivot table is a perfect tool with which to compute the desired aging analysis. To do so:

1. Highlight the entire set of data (i.e., the range A4:G104 for the spreadsheet in **figure 1**).
2. Include the column titles in row 4, which Excel will use to identify the various data for the pivot table.
3. Select the menu choices Insert/Pivot Table/Pivot Table for Excel 2010 (or Insert/Pivot Table for Excel 2013) starting from Excel's main menu. The resulting dialog box (not shown) enables the spreadsheet designer to verify the data range selected and also to decide whether or not to use a separate worksheet for the results.

Figure 2 illustrates the results of this work, mostly a blank worksheet that includes the Pivot Table Field List on the right side of the worksheet.

To create an aging analysis, the spreadsheet designer must first indicate which columns of data to use. He/she does this by checking the checkboxes for the "Classification" data and for the "Bal." (balance) data in the Pivot Table Field List. Alternatively, the designer can drag the name of the data field item, whether checked or not, into one of the four boxes in the lower portion of the Pivot Table Field List.[2] **Figure 3** displays the desired settings, with the classification in the Row Labels box and the sum of balance in the Values box. Field names can also be dragged from box to box if necessary. Finally, Excel assumes that

the designer wants the sum of the balances, but this can be changed. **Figure 3** displays the results of this work.[3]

To format the numbers in the pivot table of **figure 3**, click on the ▼ symbol next to the "Sum of Bal." entry in the Values box in the lower-right corner of the Pivot Table Field List and select "Value Field Settings." This produces the dialog box shown in **figure 4**. In this box, the designer can click on the Number Format button in the lower left portion, and then select any desired numerical format from the subsequent dialog box that Excel provides (not shown).

The auditor may also want values other than (or in addition to) the sum of the amounts owing for each category in an aging analysis. For example, suppose that the auditor wants to examine (1) the sum of the transaction amounts for each aging category, (2) a count of the number of transactions, (3) the average of the transaction balances for each aging category and (4) the maximum transaction amount for each category. This is easily accomplished by adding new items to the Values box in the lower right corner of the pivot table dialog box of **figure 3**.

To perform this task, click and drag the balance field from the Pivot Table Fields List (top right portion of **figure 3**) to the Values box, and then repeat this step twice more. The results will roughly resemble those in **figure 5**, except that Excel will again show the sum of balance entries instead of the desired counts, averages and maximums. To have Excel display these desired values, click on the ▼ symbol next to each of these fields in the Values box and then select "Count," "Average" or "Max" from the Field Settings dialog box in **figure 4**.

The results, when formatted, will resemble those in **figure 5**. Here, the first column shows the aging categories, the second column displays the sum of receivables for each category, the third column displays the number of transactions for each category, the fourth column displays the average transaction amount for each category and the fifth column displays the largest transaction in each category. The designer can display additional columns, such as the minimum transaction amount for each category, by repeating these same steps for each value desired.

TASK 2: CREATING A TWO-DIMENSION AGING ANALYSIS

When performing audits of accounts receivable data, it may also be useful to create a two-dimensional table that displays account balances classified by both transaction age and customer. Pivot tables perform such tasks easily. **Figure 6** displays the desired analysis.

Figure 4—The Value Field Settings Dialog Box

Source: Filzen and Simkin. Reprinted with permission.

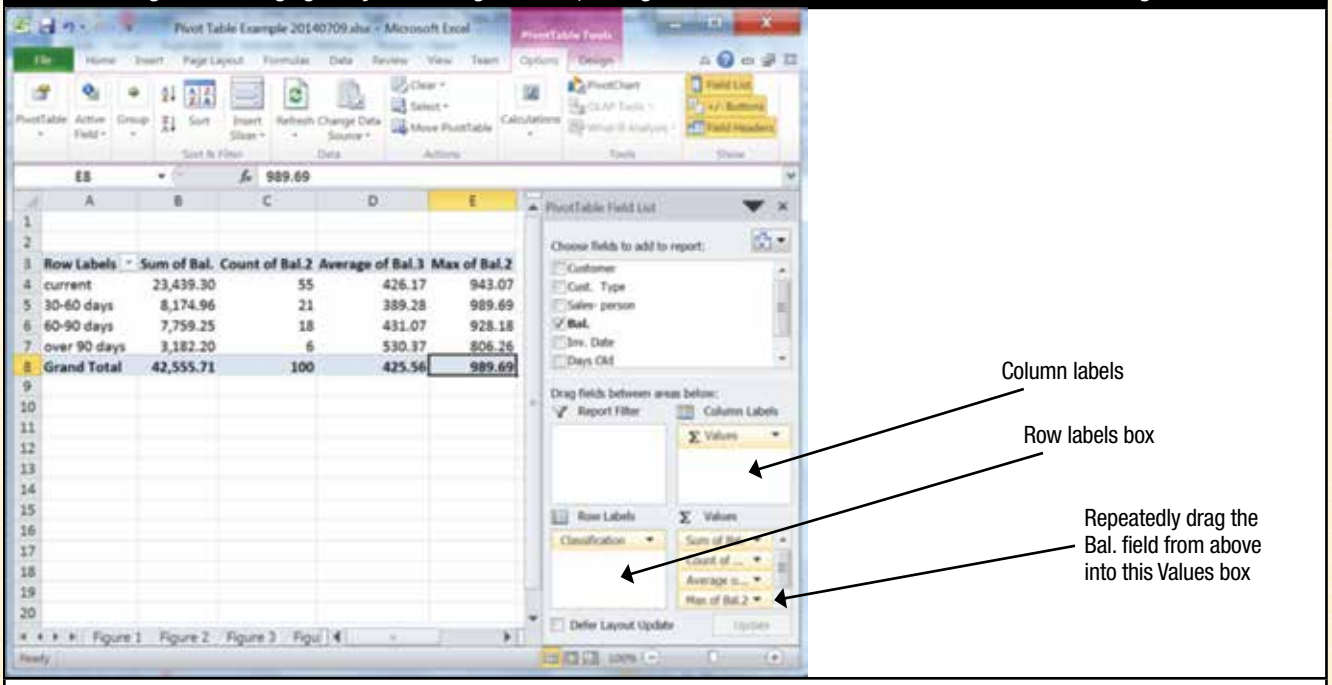
The following are the steps to create the two-dimensional pivot table shown in **figure 6**:

1. Start with the original data from **figure 1**.
2. Highlight the entire dataset.
3. Select the menu choices Insert/Pivot Table/Pivot Table to create a new pivot table in a new worksheet.
4. Next, select the "Customer," "Bal.," and "Classification" data fields and make sure that the "Classification" field is in the Column Labels box of the Pivot Table Field List, the "Customer" field is in the Row Labels box of the field list, and the "Bal." field is in the Values box of the field list.
5. If any data field is not in its correct box, simply drag it from whatever box in which it does appear and drop in into the appropriate area.

The results, when formatted, should resemble those in **figure 6**.

With the data for the pivot table properly specified and formatted, it is now easy to make some observations about this set of transactions. For example, in this illustration, it is clear that some customers are completely current

Figure 5—An Aging Analysis Showing the Sums, Averages and Counts of Account Balances for the Data in Figure 1



Source: Filzen and Simkin. Reprinted with permission.

(e.g., customers 7 and 9), while others have transactions that are seriously in arrears (e.g., customers 2, 6 and 8).

In practice, it is likely that a company would have hundreds of customers. To select only a few of them for viewing, the analyst can click on the drop-down button in cell A4 of the pivot table to select specific customers for viewing. Similarly, to limit the pivot table to show only one or two specific aging categories (e.g., only the "60–90 days" and "over 90 days" columns in the pivot table), the analyst can click on the drop-down button in cell B3.

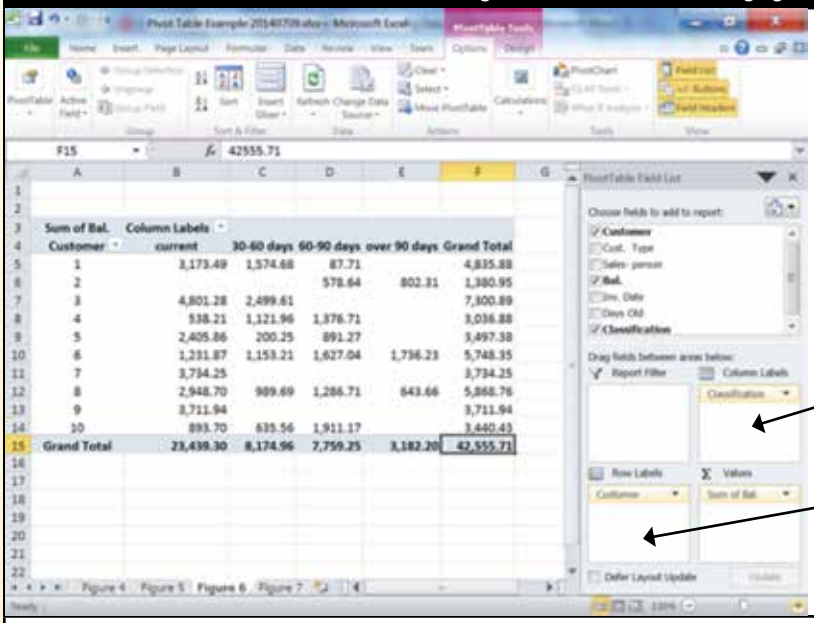
TASK 3: CREATING A THREE-DIMENSION AGING ANALYSIS

If an auditor wishes to classify receivables in some way other than by Customer and Aging Category, he/she need only create a new pivot table using alternate data fields in the Pivot Table Field List. To illustrate, perhaps the auditor wishes to tabulate the amounts by both age classification and customer type.[4] In the initial dataset of **figure 1**, for example, there are three types of customers with codes X, Y and Z. Do the aged accounts receivables differ by customer type?

To find out, an auditor can create the pivot table in the left portion of **figure 7**. Here, the aging categories form one dimension of the table and the customer codes form the second dimension. This table was created using the tools described previously for task 2. The only difference is that the column variable is now "Cust.Type." The lower portion of the Pivot Table Field List on the right side of **figure 7** shows the specific settings required.

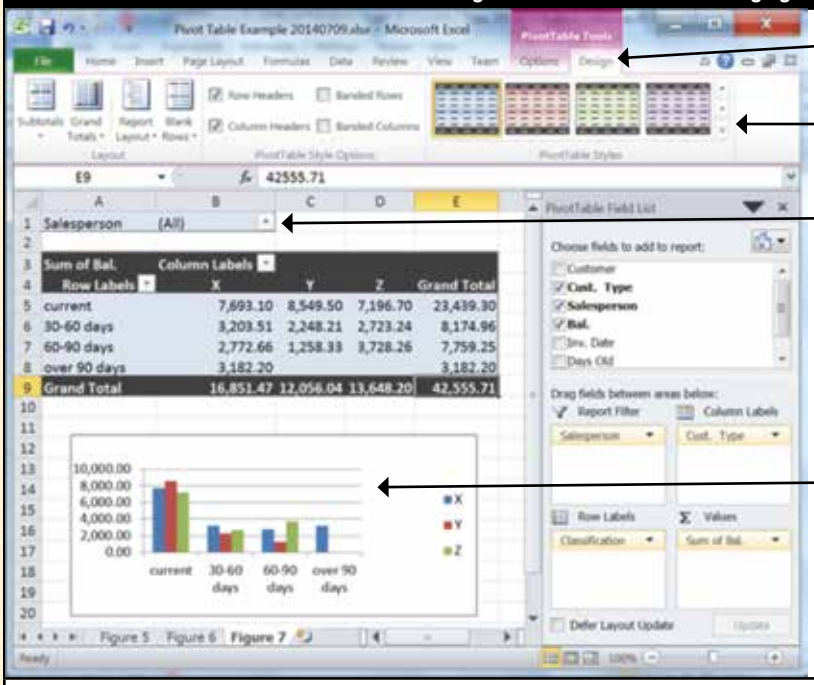
In Excel, it is also possible to add a third dimension, called a "filter," for a pivot table. **Figure 7** illustrates an example—an aging analysis that shows the sum of the transaction amounts owing by (1) age, (2) customer type and (3) salesperson. To create such a table, first create the two-dimensional table using the tools described earlier for task 2. Then, add the final variable ("Salesperson") and, if necessary, drag this variable to the Report Filter box in the Pivot Table Field List box, as shown in **figure 7**. Excel will then add the filter to the pivot table, as shown in cells A1 and B1 of **figure 7**. Now by clicking on the arrow in cell B1, an auditor can ask Excel to display the aging analysis for a specific salesperson. This allows the auditor to examine how average account balances vary by age category (the variable on the left), by customer type (the variable across the top row) and by salesperson (the selection in the filter).

Figure 6—A Two-Dimension Aging Analysis



Source: Filzen and Simkin. Reprinted with permission.

Figure 7—A Three-Dimension Aging Analysis



Source: Filzen and Simkin. Reprinted with permission.

SELECTING ALTERNATE DISPLAY OPTIONS

After creating a pivot table, the auditor can reformat it as desired. For example, as suggested by **figure 7**, Excel provides a number of different design options for pivot tables. To select an alternate, perhaps more colorful, style for the pivot table, the auditor can click on the Design tab for a pivot table and then click on the More button to see other design options (see **figure 7**). Excel classifies its design options as light, medium and heavy, but spreadsheet designers can also create their own custom designs, if desired.

As illustrated in **figure 7**, designers can also create pivot charts from pivot tables. In fact, if the user selects "Insert/Pivot Chart" instead of "Insert/Pivot Table," Excel can generate both the chart and the table at the same time. However, a pivot chart can always be added by selecting "Pivot Chart" from the Analyze tab (in Excel 2013) or the Options tab (in Excel 2010) under Pivot Table Tools. The designer can format each item separately once they have been created.

A final programming note is that Excel does not automatically update a pivot table if a spreadsheet designer alters any of the underlying data. But, this inconvenience is easily overcome by manually refreshing the table. To do so, the auditor can use the Pivot Table tabs in the top menu portion of **figure 7** and select Options/Refresh for this task.

CONCLUSION

Microsoft Excel's pivot table options provide powerful tools for aggregating and analyzing accounting data. While the example here focused on analyzing accounts receivable, similar analyses are possible for accounts payable, cash sales, inventory or payroll applications, as well. The data do not even have to be numeric—pivot tables can also count occurrences of alphabetic data if frequency distributions are required. Further, although the example presented here used a small set of data, much larger data sets are easily handled in the same manner. For these reasons, the ability to use pivot tables should be a natural part of the skill set of external and internal auditors wishing to perform cross-tabulation analyses of accounting data.

ENDNOTES

[1] Technically, the categories are "current," "30-59 days," "60-89 days," and "90 days or more." The VLookup table used here performs exactly this classification.

[2] All pivot table tools as well as the Pivot Table Fields List are visible only when the spreadsheet cursor is located in one of the cells of the pivot table itself.

[3] The default row label order is alphabetical; however, custom sorting orders are available by clicking the ▼ symbol next to "Row Labels."

[4] For example, the term "customer type" could designate geographic sales region, credit rating or type of account.

Bill Hargenrader, CISM, CEH, CISSP, is a senior lead technologist at Booz Allen Hamilton, where he is developing a next-generation cybersecurity workflow management software solution. He is working on his doctorate degree in information technology, focusing on the intersection of cybersecurity and innovation.

Information Security Continuous Monitoring

The Promise and the Challenge

Combining an organization-applicable risk framework with an all-encompassing control set and an information security continuous monitoring (ISCM) methodology provides for a holistic approach to compliance and risk management by providing controls across a wide array of areas with a high level of detail and guidance on tailoring.[1] An enterprise could apply this approach to risk management by assessing the organization, integrating the risk management framework and establishing a security baseline based on the security control standards. When the controls are continually monitored, assessed and addressed, the organization has taken a big step toward reducing its security risk potential.

There is an ongoing movement toward adopting ISCM at the federal level, as well as within the US Department of Defense (DoD), due to US Federal Information Security Management Act (FISMA) compliance requirements. Though the compliance issues are federal in nature, there are lessons to be learned and technology improvements that can be implemented in any industry, such as finance, utilities and health care. In 2013, the US Department of Homeland Security (DHS) presented all federal agencies with a blanket purchase agreement worth up to US $6 billion for reduced-cost continuous monitoring software.[2] The US Office of Management and Budget (OMB) has offered guidance on how continuous monitoring will be able to replace the current three-year accreditation cycles.[3]

Disponible également en français
www.isaca.org/currentissue

ISCM has the promise of being the next best thing for cybersecurity and risk management, but there are still some immaturities and challenges that exist in the methodologies and software. In this regard, three areas should be examined relating to ISCM. Those three areas are manual vs. automated logging, current technology available, and control sampling frequency.

BACKGROUND INFORMATION ON ISCM

The primary literature studied for this research on ISCM was developed by the US National Institute of Standards and Technology (NIST). "NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems."[4] NIST provides detailed guidance on implementing a risk management framework.[5] It also provides a detailed and broad control set for federal agencies to adopt—though any organization can adopt the controls as standards. A combination of the risk management framework, control set and the continuous monitoring implementation guidance can be used to set up a federally accepted continuous monitoring plan. Three key NIST Special Publications are described in **figure 1**.

Figure 1—Key NIST Special Publications Related to ISCM

Special Publication Title	Subject Matter
NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems	Guidance for applying enterprise-level risk management to an organization
NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	A multitiered approach to risk management through control compliance. This approach includes security control structure, security control baseline and security control designations.
NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	A holistic, enterprise-level approach to setting a continuous monitoring strategy, implementing a program and executing the activities of the program

Do you have something to say about this article?

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

Go directly to the article:

Some of the gaps in the research dealing with continuous monitoring are that the vast array of studies undertaken have been conducted in the area of audit, energy, medical and sensor network. This opens the possibility of transferring a technology or algorithm from a disparate field. For instance, the implementation of continuous auditing and decision processes to be included in the early design stages of emergency response processes[6] would have a strong correlation to designing continuous monitoring into a system from the start. Some advances could be orchestrated and pose the potential to leap ahead in the area of ISCM by modeling these other areas.

EVALUATION OF CONTINUOUS MONITORING RISK MANAGEMENT COMPLIANCE FRAMEWORK

Continuous monitoring is one of six steps in the Risk Management Framework (RMF).[7] When properly selecting a framework, it is critical to choose one that will effectively support operations as well as the controls that the organization uses for compliance.[8] The selection can be viewed across four areas of security, service, operations and governance. Information assurance (IA) exists in all of these areas as well, because the aim is to ensure that the mission can be completed and these four areas all play a role in a mission's effectiveness. There have been many updates on how to address risk management, but among the more prominent is NIST SP 800-37 combined with the NIST SP 800-53 and NIST SP 800-137. Together these documents thoroughly address the IA area of risk management and compliance, and do so in continuous fashion.

RISK MANAGEMENT FRAMEWORK REFERENCE

NIST SP 800-37 provides guidance for applying a risk management program to an organization. As the types of sophisticated, well-organized attacks have increased, the potential for higher levels of damage to national security has increased as well.[9] For organizations to understand their chances of becoming compromised and the damage done from that compromise, a system of continuous assessment of vulnerabilities, impacts, mitigations and residual risk acceptance should be adopted. Without a comprehensive system in place, an organization is essentially leaving itself open to chance. SP 800-37 provides for that system and a means of implementing it, but it is up to the organization to tailor and implement it effectively.

The process involves the following steps: Categorize information systems, select security controls, implement security controls, assess security controls, authorize information systems and monitor security controls. SP 800-37 revolves heavily around control assessment to determine the level of risk an organization is facing. The level of compliance or completeness with the established security controls can give leadership an idea of the overall risk level of the organization, as well as provide guidance on what areas should be improved through policy, technology or personnel.

SECURITY CONTROLS REFERENCE

Critical to the risk management framework are the controls that fit into that framework. SP 800-53 uses a multitiered approach to risk management through control compliance. This approach includes security control structures, a security control baseline and security control designations.[10] SP 800-53 works hand in hand with SP 800-37 in that the controls are overlayed on top of the risk management framework for an organization. The controls are selected based on the criticality and sensitivity of information owned by the system and are applied in a suggested order with identified higher priority controls first. The controls include identification and authentication, contingency planning, incident response, maintenance, risk assessment, and media protection, among many others.

INFORMATION SECURITY CONTINUOUS MONITORING REFERENCE

Continuous monitoring can be a ubiquitous term as it means different things to different professions. NIST SP 800-137 sets forth a standard to follow when applying the principle in the risk management framework utilizing the NIST control set. The primary process for implementing ISCM is to:[11]

- Define the ISCM strategy
- Establish an ISCM program

- Implement an ISCM program
- Analyze data and report findings
- Respond to findings
- Review and update the monitoring program and strategy

Factored into this is the use of manual and automated checks to provide continuous updates and feedback to the system as a whole.

Though these three NIST Special Publications form a solid foundation for continuous security monitoring, risk management and compliance, there are some areas that need to be addressed and reviewed for effectiveness. Automated technology drives the push for continuous monitoring and has been the focus of ISCM efforts;[12] however, only so many controls can be tracked via an automated process, which presents a potential gap in the control set for activities that are performed manually. There is also the matter of technology available. One of the largest federal ISCM projects has issued a suite of automated tools to provide this function. The question with these tools is how many controls they cover. And, there is the matter of control sampling frequency. NIST SP 800-137 offers guidance, but not specifics.

THE ADVANTAGES AND DISADVANTAGES OF THE MODEL: MANUAL VS. AUTOMATED PROCESSES

One of the advantages of the ISCM model is that it captures aggregate data from already-existing systems in automated fashion. This automated process provides for real-time, up-to-the-minute information to be collected and reviewed by leadership. One of the disadvantages of the model is that not all activities take place in an automated or networked fashion. It may not be easy to capture and log automatically, for example, when planning for acquisitions took place or that a policy was updated. In addition, there is no volume of federal guidance on manual logging. In NIST SP 800-137, manual checks and procedures are called out as needing to comply with the same level as automated checks.

One potential solution would be to provide a manual logging mechanism for actions completed. This could be a login interface to communicate when someone has finished backing up a server or performed a security sweep of a remote location server room. Sign-in sheets for access to controlled areas could also be automated, perhaps by signing in on a tablet that logs times and names and identifies unusual patterns of behavior, such as entry at a late hour that is against the norm. The review of advantages and disadvantages of physical vs. automated solutions can be complemented by a survey of current continuous monitoring solutions.

COMPARISON OF CONTINUOUS MONITORING SOFTWARE SOLUTIONS

Guidance from the OMB states that, "The continuous monitoring phase must include monitoring all management, operational, and technical controls implemented within the information system and environment in which the system operates including controls over physical access to systems and information."[13] In this regard, a table was created that lists all the DHS applications that are being offered to federal systems, as noted previously.[14] The software was reviewed online and categorized against the NIST control category and control type (**figure 2**).

After the data were collected and reviewed, a comparison table was created to show how many control types were used and how many were not used. A high-level estimate was made from these data of the effectiveness at total coverage of the currently offered automated solution.

CONTINUOUS MONITORING SOFTWARE ANALYSIS

Of the 21 control families, eight are covered by the DHS continuous monitoring software offerings. Additionally, there are numerous specific controls under the control types that are not covered. From a very high-level view, only 38 percent of control types are affected by software offering. This leaves room for future improvements. There are software solutions not on this list that cover some of the control categories. In addition, there currently is not a system that integrates the data feeds from each of these individual software packages.

FREQUENCY OF CONTROL ASSESSMENT

Sampling frequency factors that should be taken into consideration are risk level, changes in the control item (often intermittent), and whether the control is in an open or incomplete state.[15] Risk level is how much of an impact there would be if a vulnerability related to the control were exploited. The thresholds and timing have to be set by the organization's leadership and by that of the overarching governing agency body.

A public web server may have a higher risk level than a file server on the domain located securely within the enclave; the chances are lower of it being attacked, and there would be less impact if it were taken offline. In this way, public servers may

Figure 2—NIST SP 800-53 Control Count Cross-reference by Family			
Count 1	**Control Family Not Covered by DHS Applications**	**Count 2**	**Control Family Covered by DHS Applications**
1	Planning	1	System and information integrity
2	System and service acquisition	2	Risk assessment
3	Security assessment authorization	3	Incident response
4	Program management	4	Asset management
5	Personnel security	5	Audit and accountability
6	Physical and environmental	6	Configuration management
7	Contingency planning	7	Malware detection
8	Maintenance	8	Identity access
9	Media protection		
10	Awareness and training		
11	Identification and authentication		
12	Audit and accountability		
13	System and communications protection		

be chosen to be sampled more frequently. The sensitivity of the data would have to be taken into consideration as well. If the file server contains US Social Security numbers, it could require a higher sampling frequency than the public web server.

Certain controls, such as reauthorizing user access annually, may have to be sampled only twice a year for a particular program if that process occurs only once a year. It would be a waste of resources, computing power and storage to sample that control every minute, day or week. The spectrum for controls most likely ranges from a scale of annually, to every second year. Developing a road map for an organization, or a standard best practices timeline, would save time and energy. It will also facilitate buy-in from the user community. If they are being asked to report something more frequently than they know they have to, the whole concept of continuous monitoring could gain a bad reputation in the organization.

CONCLUSION

ISCM has a major positive impact on improving risk management and compliance across many industries and bodies, including the US federal government, the DoD, and commercial and financial organizations. The technology available today goes a long way toward improving security, though temperance should be used when conveying what problems this solves as there are some glaring holes in what is currently available. Future research could include looking for a solution to fill the gaps in control coverage, such as a physical logging mechanism, to input workflow activities into an automated system for aggregation. Establishing best practices for the control sampling frequency provides the necessary timing for the manual logging. One final proposed change to the model would be to connect both the continuous monitoring solution to a single dashboard for managing overall risk. Working from this model would be able to show organizations which areas are being continuously monitored and which areas still need to be tracked the traditional way. Though the promise of ISCM is great, there are many challenges to overcome to realize complete implementation. The only way to overcome those challenges is to get started on implementing ISCM and to share the lessons learned with the cybersecurity community.

ENDNOTES

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

[2] Bennett, C.; "With $6 Billion Continuous Monitoring Contract, DHS Takes 'Next Leap' in Cybersecurity," Fedscoop, 2013, *http://fedscoop.com/with-6-billion-continuous-monitoring-contract-dhs-takes-next-leap-in-cybersecurity/*

[3] Zients, J. D.; "Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," Office of Management and Budget, 2012, *www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf*

[4] National Institute of Standards and Technology, Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," USA, 2011, p. 3, *http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf*

[5] National Institute of Standards and Technology, Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," USA, 2010, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

[6] Chumer, M.; R. Hiltz; R. Klashner; M. Turoff; "Assuring Homeland Security: Continuous Monitoring, Control & Assurance of Emergency Preparedness," *Journal of Information Technology Theory and Application*, 2004, vol. 6(3), p. 1-24, *http://search.proquest.com.library.capella.edu/docview/200008540?accountid=27965*

[7] *Op cit*, NIST 2010

[8] Schlarman, S.; "Selecting an IT Control Framework," *Information Systems Security*, 2007, 16(3), p. 147-151

[9] *Op cit*, NIST 2010

[10] *Op cit*, NIST 2013

[11] *Op cit*, NIST 2011

[12] US Department of Homeland Security, "Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)," Federal Network Security Branch, 2010, *https://www.dhs.gov/continuous-asset-evaluation-situational-awareness-and-risk-scoring-reference-architecture-report*

[13] *Op cit*, Zients, p. 11

[14] US Department of Homeland Security, "BPA Awardees and Tool Suites," *Federal Times*, 2013, *http://apps.federaltimes.com/projects/files/bpa_awardees.pdf*

[15] *Op cit*, NIST 2011

HelpSource Q&A

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

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

Ganapathi Subramaniam is director, information security, at Flipkart, an online marketplace entity. Previously, he worked with Microsoft India and Accenture, as well as PricewaterhouseCoopers, Ernst & Young and a UK-based mortgage institution while living in the UK. Subramaniam is an international conference speaker and columnist.

Q Privacy is one area that has never been audited in my enterprise. Please provide your point of view on how privacy compliance can be assessed?

A Though some standard security controls can ensure protection of sensitive information, including those that can be deemed as private, security and privacy are not synonymous. Privacy requirements vary from country to country, depending on national and regional laws and regulations. However, there are some common principles on privacy based on which such laws/regulations are created. Examples of such principles include, but are not limited to, the following:

> "Security and privacy are not synonymous."

- Notice
- Choice
- Purpose specification
- Collection limitation
- Access and rectification
- Retention
- Disclosure to third parties

Depending on the country/continent, there are multiple data protection models such as:

- Comprehensive laws of the European Union
- Sector-specific laws in the US
- Co-regulatory model, found in Australia and Canada
- Self-regulatory model, found in US, Japan and Singapore

Compliance with regulations is mandatory and nonnegotiable.

This is an indicative list to outline the assessment approach; only a lawyer can provide legal advice.

The privacy policy of your enterprise (assuming one exists) must serve as the basis of your audit. The privacy policy must be reviewed for its comprehensiveness. Operationalizing such principles is essential so that the policy is adopted both in letter and in spirit:

- Adequate notice must be provided to the consumers whose data get collected.
- The notice given must explicitly state how the information collected will be processed.
- Choice must be provided to the consumers. In other words, does the enterprise provide for the consumers to either opt in or opt out?
- The purpose for which data are collected must be disclosed to the consumers at the point of collection. Any change in purpose must also be disclosed.
- The data collected must not be unlimited information. It must be clearly predefined, limited information.
- Personal information (PI) collected must be protected against threats such as unauthorized access, modification impacting the integrity of the data and deletion.
- Consent must be obtained from the data subjects or the consumers from whom the data are collected.
- Consumers whose data are collected must be given the facility to view the information held about them. In addition, they must be given the facility to amend or delete information that is not complete, relevant or accurate.
- An identified individual must be designated to be accountable for ensuring compliance toward the above principles.
- What constitutes a breach must be clearly identified. Processes and controls to handle any breach must be defined and must be in place. In some cases, notification has to be done to external regulators and the data subjects/consumers whose data have been compromised. Disclosure as stipulated by laws and regulations will not constitute a breach.

Do you have something to say about this article?

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

Go directly to the article:

- Transfer of data outside the EU, for example, for processing purposes can be done subject to certain conditions. If your enterprise were to transfer data from the EU to the US, it must ensure that the conditions laid out by regulations are clearly met.

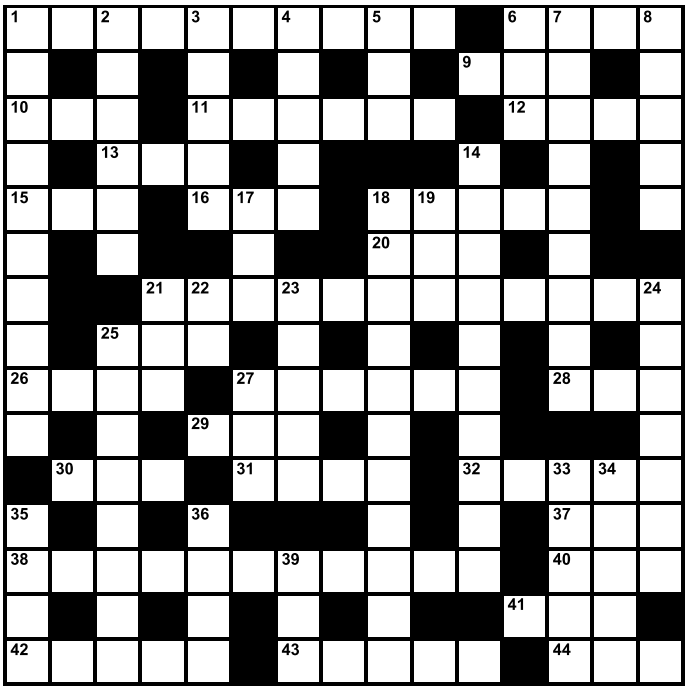
Figure 1 provides a comparative analysis of the various privacy principles as elucidated in various laws/regulations.

Figure 1— Privacy Principles Comparison

Asia Pacific Economic Cooperation (APEC)	EU Data Protection Act	US Federal Trade Commission Fair Information Practice Principles
• Preventing harm • Notice • Collection limitation • Choice • Usage • Access controls and correction • Accountability	• Purpose specification • Collection limitation • Security controls • Usage • Accountability • Participation by individuals	• Notice • Choice and consent • Access to participate • Security controls to ensure accuracy of data • Enforcement

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. Bug recently found in Bash
6. Important certification for IS auditors
9. Computer link
10. ____ files: they don't provide a full accounting of user activity
11. Means of hacking attack
12. Software code problems
13. Make sure of, as a victory
15. ___ Microsystems, acquired by Oracle
16. Bathroom scale meas.
18. It enables connection with remote servers used for data storage
20. ___ command
21. Cybersecurity weakness that was attacked in Target and Home Depot (2 words)
25. Yank
26. Central component
27. _____ effect
28. Government department concerned with cyberwarfare
29. Sign, as a contract
30. Important position in the audit profession, abbr.
31. _____ Red, 90s supercomputer
32. Problem
37. ___ flash (2 words)
38. Transferring, of a file
40. World-wide web inventor, Berners-Lee
41. All in place
42. Internet phone company acquired by Microsoft
43. Tier
44. Fast plane, for short

DOWN

1. World's number one customer relationship management application
2. A program that performs a core or essential function for other programs
3. Security tier
4. Breaks into another's system
5. Key executive, for short
6. Urban transport
7. Overwhelmed
8. It's on the plus side of the ledger
14. Essential component of internal controls
17. Communication system that transfers data between computers
18. The essential asset for any auditor
19. Wheel fastener
21. Signal
22. Silver's symbol
23. Enticements
24. View a problem from an adversary or competitor's viewpoint (2 words)
25. 1985 Commission on fraudulent financial reporting
27. Modern means of ID
33. www locations
34. Modules
35. Actuary's concern
36. Tooth color (technologically speaking)
39. Soup to nuts

(Answers on page 58)

CPE Quiz

Prepared by Sally Chan, CGEIT, CPA, CMA, ACIS

Take the quiz online:

QUIZ #158

Based on Volume 5, 2014—Mobile Devices

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

TRUE OR FALSE

RAVAL ARTICLE

1. Broadly, machine ethics is a discipline that attempts to address the ethics of artificial intelligence (AI). Attempts to articulate moral dimensions are relatively recent. This leap from computer ethics to machine ethics is necessary due to the elevated status of computers from mere enablers to intelligent collaborators with humans.
2. Mobile computing cannot be seen as an agent with ethical impact. It does not make decisions and is not responsible for the moral dimensions of human behavior.

GELBSTEIN ARTICLE

3. Application (app) development is a regulated market. The degree of app quality assurance does not depend on who provides them.
4. IT and information security practitioners agree that the four pillars that enable sustainable success are governance, process, technology and people. People should be considered the weakest link and the existence of the great digital uninformed (GDU) makes success hard to achieve.
5. The characteristics of GDU behavior that are easy to change include: the shifting boundaries between work and home life, autonomy and independence, and device owners with information security and data protection responsibilities and a lack of personal engagement.

YU ARTICLE

6. A purely white-list style validation allows for false negatives to fall through the cracks in some scenarios. A combination of black-list and whitelist styles in production is generally not used.
7. Input/output (I/O) validation goes a long way toward adding a very useful layer of security by ensuring that only well-defined data move across the code. Some of the most notorious security vulnerabilities, such as buffer overflows and injection loopholes, are made exploitable with missing and insufficient validation.
8. It is important to pick well-used and vetted code bases, particularly for cryptography. A well-reputed code base will have an army of people looking for problems with it and an army of people using it who have the incentive to fix it.

CHAUDHARY ARTICLE

9. A Harris Interactive survey sponsored by Fiberlink found that nearly 82 percent of employees are concerned about employers viewing private information on their personal device. Some of the user BYOD privacy concerns include locking, disabling and data wiping, as well as GPS and location information.
10. ISACA's *BYOD Audit/Assurance Program* is a tool and template to be used as a road map for the completion of a specific assurance process. The BYOD program focuses on risk management, managing device configuration and security, human resources, and training users. BYOD assurance based on the COBIT framework can be part of an organization's overall assurance program by including BYOD and privacy in the scope.

FU ARTICLE

11. The Association of Certified Fraud Examiners (ACFE) has estimated that about 80 percent of all companies around the world experienced some type of fraud in 2012, with total global losses due to fraud exceeding US $3 trillion annually.
12. The goal of a current-state analysis and assessment is to understand the overall fraud capability and health of the organization. The current-state analysis should cover the entire spectrum for the life cycle of fraud prevention—from awareness, understanding, adoption, implementation, operations and enforcement of fraud-relevant policy and procedures, to fraud data analysis, investigation, process improvement, and reporting and development.
13. The IBM capability maturity model is a balanced assessment approach across the critical domains of the enterprise fraud risk management program and processes. It allows organizations to dive into their specific capabilities and further evaluate and determine their current state of fraud prevention as compared to industry best practices.

MASIKA ARTICLE

14. Kotter's eight steps to leading change do not have to be worked through in sequence. Skipping one or more steps to try and accelerate the process would not cause problems.
15. Information security managers need to create a vision and information security strategy to guide information security operations. They must empower all stakeholders to play their role and act on the information security vision.
16. One of the key information security initiatives to establishing a sense of urgency is to nominate information security champions who have the energy and time to champion information security as focus groups in each business unit and all branches.

ISACA Journal
CPE Quiz
Based on Volume 5, 2014—Mobile Devices

Quiz #158 Answer Form

(Please print or type)

Name _____

_____

Address_____

_____

_____

CISA, CISM, CGEIT or CRISC #_____

Quiz #158

True or False

RAVAL ARTICLE

1._____

2._____

CHAUDHARY ARTICLE

9._____

10._____

GELBSTEIN ARTICLE

3._____

4._____

5._____

FU ARTICLE

11._____

12._____

13._____

YU ARTICLE

6._____

7._____

8._____

MASIKA ARTICLE

14._____

15._____

16._____

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

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

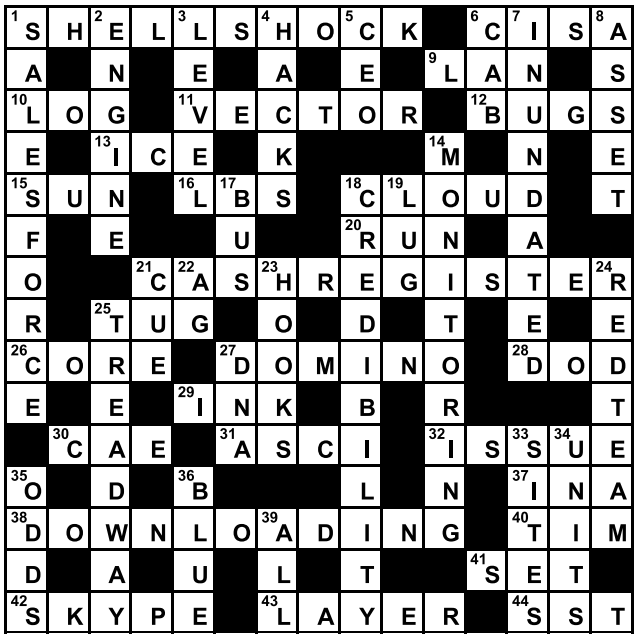
Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

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

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

Answers—Crossword by Myles Mellor

See page 56 for the puzzle.



ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

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

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

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

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

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

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

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

IS Audit and Assurance Standards

The titles of issued standards documents are listed as follows:

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

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

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

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

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

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

Reporting
2401 Reporting
2402 Follow-up Activities

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

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

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

Advertisers/Web Sites

Leaders and Supporters

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

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

ISSN 1944-1967

ISACA®
Trust in, and value from, information systems

BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

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

NEW PRODUCTS

CISA Review Questions, Answers & Explanations – 12 month web-based subscription

Available on the web – **XMXCA15-12M**
Member: $185.00 Nonmember: $225.00

FISMA Compliance Handbook, Second Edition

Available in print – **15SYN**
Member: $55.00 Nonmember: $65.00

Fraud Prevention and Detection: Warning Signs and the Red Flag Systems

Available in print – **61CRC**
Member: $56.00 Nonmember: $66.00

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

Available in print – **22ITG**
Member: $35.00 Nonmember: $45.00

Implementing the NIST Cybersecurity Framework*

Complimentary eBook available to Members only.
Available in print – **CSNIST** and eBook **WCSNIST**
Member: $35.00 Nonmember: $60.00

FEATURED PRODUCTS

Auditing Social Media—A Governance and Risk Guide

Available in print – **110WAS**
Member: $31.00 Nonmember: $41.00

CISA Review Manual 2015

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

CISM Review Questions, Answers & Explanations – 12 month web-based subscription

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

Cyber Threat! How to Manage the Growing Risk of Cyber Attacks

Available in print – **108WCT**
Member: $33.00 Nonmember: $43.00

CSX Cybersecurity Fundamentals Study Guide*

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

Risk Scenarios: Using COBIT 5 for Risk

Complimentary eBook available to Members only.
Available in print – **CB5RS** and eBook **WCB5RS**
Member : $35.00 Nonmember: $60.00

* Published by ISACA

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

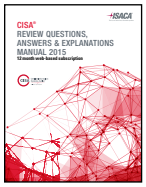
All prices are listed in US Dollars and are subject to change

We are constantly expanding. Check out our new books and eBooks!
https://www.isaca.org/bookstore/Pages/New-Arrivals.aspx

New/Featured Products

NEW PRODUCTS

CISA Review Questions, Answers & Explanations – 12 month web-based subscription*



by ISACA

The CISA Practice Question Database - w12 Month Subscription is a comprehensive 1200-question pool of items that combine the questions from the *CISA Review Questions, Answers & Explanations Manual 2013* with those from the *2014* and *2015* editions of the *CISA Review Questions, Answers & Explanations Manual Supplement*. The database is available via the web, allowing our CISA Candidates to log in at home, at work or anywhere they have Internet connectivity.

Available on the web – **XMXCA15-12M**
Member: $185.00 Nonmember: $225.00

FISMA Compliance Handbook, Second Edition

by L. Taylor

This comprehensive book instructs IT managers to adhere to federally mandated compliance requirements. *FISMA Compliance Handbook Second Edition* explains what the requirements are for FISMA compliance and why FISMA compliance is mandated by federal law. The evolution of Certification and Accreditation is discussed.

Available in print – **15SYN**
Member: $55.00 Nonmember: $65.00

Fraud Prevention and Detection: Warning Signs and the Red Flag Systems

by Rodney T. Stamler, Hans J. Marschdorf, Mario Possamai

Lessons can be learned from major fraud cases. Whether the victim is a company, public agency, nonprofit, foundation, or charity, there is a high likelihood that many of these frauds could have been prevented or detected sooner if early Red Flag warning signs had been identified and acted upon. This book will enable officers and directors, internal and external stakeholders, as well as outside analysts to protect themselves and their organizations against fraud by effectively detecting, analyzing, and acting on early Red Flag warning signs. Based on an empirically tested strategy, the Red Flag System reflects the authors' more than 100 years combined experience in the investigation of fraud in high-profile, global cases in North America, Africa, Europe, and the Far East.

Available in print – **61CRC**
Member: $56.00 Nonmember: $66.00

Governance of Enterprise IT based on COBIT 5

by Geoff Harmer

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

Available in print – **22ITG**
Member: $35.00 Nonmember: $45.00

* Published by ISACA

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

New/Featured Products

Implementing the NIST Cybersecurity Framework*

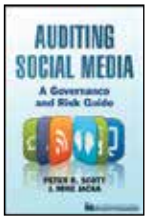
by ISACA

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

Complimentary eBook available to Members only.
Available in print – **CSNIST** and eBook **WCSNIST**
Member: $35.00 Nonmember: $60.00

FEATURED PRODUCTS

Auditing Social Media – A Governance and Risk Guide



by Peter R. Scott, J. Mike Jacka

Packed with useful web links, popular social media tools, platforms, and monitoring tools, *Auditing Social Media* shows you how to leverage the power of social media for instant business benefits while assessing the risks involved. Your organization sees the value in social media and wants to reach new markets, yet there are risks and compliance issues that must be considered. Auditing Social Media equips you to successfully partner with your business in achieving its social media goals and track it through strong metrics.

Available in print – **110WAS**
Member: $31.00 Nonmember: $41.00

CISA Review Manual 2015*

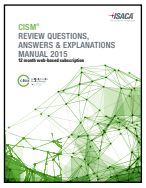
by ISACA

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

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

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

CISM Review Questions, Answers & Explanations – 12 month web-based subscription*



by ISACA

The CISM Practice Question Database – 12 Month Subscription is a comprehensive 1015-question pool of items that combine the questions from the *CISM Review Questions, Answers & Explanations Manual 2014* with those from the *2014* and *2015* editions of the *CISM Review Questions, Answers & Explanations Manual Supplement*. The database is available via the web, allowing our CISM Candidates to log in at home, at work or anywhere they have Internet connectivity.

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

* Published by ISACA

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

New/Featured Products

FEATURED PRODUCTS *(cont.)*

CSX Cybersecurity Fundamentals Study Guide*

by ISACA

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

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

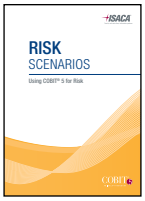
Cyber Threat! How to Manage the Growing Risk of Cyber Attacks

by MacDonnell Ulsch

Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information.

Available in print – **108WCT**
Member: $33.00 Nonmember: $43.00

Risk Scenarios: Using COBIT 5 for Risk*



by ISACA

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

Complimentary eBook available to Members only.
Available in print – **CB5RS** and eBook **WCB5RS**
Member : $35.00 Nonmember: $60.00

* Published by ISACA

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

CELEBRATING 20 YEARS

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

infosecurity EUROPE

02-04 JUNE 2015 | OLYMPIA | LONDON | UK

Securing the connected enterprise

Collect **CPE/CPD** credits

WHY YOU CANNOT MISS INFOSECURITY EUROPE 2015?

98.1% of visitors attending Infosecurity Europe in 2014, were satisfied to completely satisfied

96.6% of visitors are likely, or more than likely to attend in 2015, of which 81% are more than likely to return

84.1% of visitors are very likely to recommend participating in Infosecurity Europe to a colleague

97.2% of exhibitors were satisfied in 2014 and 80% have already rebooked to participate in 2015

ROI £447,528,560 of future orders expected to be placed with exhibitors as a direct result of Infosecurity Europe 2014

REGISTER YOUR INTEREST NOW

www.infosec.co.uk

Part of infosecurity GROUP

Organised by Reed Exhibitions

GAIN MORE ASSURANCE WITH A MASTER'S

Be an expert in data security and prevent the misuse of data and cyber attacks with Regis University's graduate programs in information assurance (IA). Classes within the master's degree and graduate certificates can be taken online, on-campus or a combination of the two.

Graduate-Level Programs

- M.S. in Information Assurance: IA Policy Management and Cyber Security specializations
- Cyber Security Programs
- IA Policy Management Certificate

A Cutting-Edge Curriculum

Designated a Center of Academic Excellence in Information Assurance Education by the National Security Agency, Regis University's IA curriculums reflect the guidelines and recommendations of:

- CNSS
- (ISC)^2
- ISACA
- NIST

The curriculum also provides you with the foundational knowledge needed to sit for multiple industry certification exams, including:

CISA | CISM | CISSP | SSCP | CCNP | CEH

REGIS UNIVERSITY

LEARN MORE TODAY
informationassurance.regis.edu/ISACA
877.820.0581