Volume 6, 2017

ISACA Journal

TRANSFORMING DATA

06

Digital Identity—Will the New Oil Create Fuel or Fire in Today's Economy?
Governance, Risk, Compliance and a Big Data Case Study
Auditing Big Data in Enterprises

www.isaca.org

ISACA®

SEE WHAT'S NEXT, NOW

GET CERTIFIED. GET AHEAD.

CISA® CRISC™ CISM® CGEIT®

FAST-TRACK YOUR FUTURE WITH ISACA'S GLOBALLY RECOGNIZED CERTIFICATIONS.

No matter your role in IS/IT—audit, security, cyber security, risk, privacy or governance, these credentials are designed for forward-thinking professionals across a variety of industries. ISACA® certifications are not just any certification, they are the ones that can get you ahead!

Obtain certifications that bring value to your career now, and in the future.
Choose your certification and get started today to secure your spot for the 1 November – 31 December exams!

Registration for the certification exams in 2018 opens in December!
Once open, you may register for the upcoming exam period that starts 1 February 2018.

Register now for a 2017 exam at www.isaca.org/GetCertified-Jv6.

SAVE
THE DATE... *or*
—REGISTER—
NOW

6th Annual

European Compliance & Ethics Institute

25–28 March 2018 | *Frankfurt, Germany*

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

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

ISACA Journal

FEATURES

PLUS

Online-Exclusive Features

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

Online Features
The following is a sample of the upcoming features planned for November and December 2017.

Assurance Across the Three Lines
Ability Takuva, CISA

Creating and Defining a Culture of Security
Pedro Alexandre de Freitas Pereira, CCNA

An IoT Control Audit Methodology
Marcin Jekot, CISSO, ISO 27001 LA, SSP and Yiannis Pavlosoglou, Ph.D., CISSP

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

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

Read more from these *Journal* authors...

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

ISACA®
Trust in, and value from, information systems

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

Information Security in Context

I do not believe in information security.

I support information security. I exhort organizations to implement and maintain information security. I have built my career around information security. But I do not believe in it. Belief is black or white. It admits no shades of grey. Security is not an absolute.

Beliefs and Causes

I do have beliefs—religious, moral and political—which I have absolutely no intention of addressing in this *Journal* or any other public forum. In fact, they are not suited to discussion because, as beliefs, they are not subject to argument. One set of beliefs can only be confronted by another, not proven right or wrong. In the past, and even in the present, people have died for what they believe. I would like to think that I have the strength of character to die for my beliefs, but I am surely *not* prepared to die for the sake of secure information in any corporation or government agency.

I bring this up because I encounter many security professionals who act as though securing information is, for them, a holy endeavor. Unlike typical belief systems, security has no contradictory beliefs. No one is against security. (Of course, that is not literally true. There are some really bad people who are against security or, more precisely, they are against *your* security, but not their own.) In the absence of a counterargument, some security professionals I have met treat information security as a Cause, not as an attribute of information systems.

So what? Why is this bad? What is wrong with a little professional fervor? My concern is that such zeal leads to intransigence. It not only isolates the person, but also creates an atmosphere that runs counter to the establishment of an effective security culture within organizations. If security is portrayed as the One True Way, its proponents lose sight of the fact that others have different incentives, such as cost reduction, mission achievement and profit. It is not that security is inimical to these, but close-mindedness crowds out the ability to understand what drives other people. Thus, security receives resistance rather than an understanding that could lead people to accommodate security along with their own motivators.

Context

This is not an argument in favor of compromise of the basic principles of information security. I prefer to think that it is recognition that security must be placed in context. The requirements for security differ in all sorts of organizations based on size, risk, resources and mission. So, for example, a company that makes household products simply does not have security needs as stringent as those of, for example, a large bank with billions that might be lost or a hospital where lives are at stake.

Moreover, information security is not a monolith. Data privacy is a major concern for those in health care or insurance, but less so for manufacturers, for whom trade secrets are a paramount issue. Fraud prevention is a focus of financial institutions, but less so for restauranteurs. So, someone pressing for across-the-board security can only be seen as foolish if he or she presses too hard.

This applies even in this age of cyberattacks. Much as I disdain those who dismiss this threat as not applying to their organizations,[1] it is true that some industries are more tempting targets than others. A small company that makes, say, plastic toys[2] is less likely to be attacked than a giant global brokerage firm. Once again, it is all a matter of context.

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

http://bit.ly/2xmXwoM

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

Enjoying this article?

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

Persuasion, Not Proselytizing

In all organizations, information security needs advocates, not fanatics. No one in any information security department is going to achieve his/her goals acting alone. Security must be achieved through all the technicians and users in an organization. This calls for persuasion, not proselytizing. Security must be conveyed as a way of doing business that is beneficial for the organization, to be sure, but also for the individual. The inherent goodness of secure information resources must be demonstrated, not just presented as revealed truth. Information security professionals must be salespeople, teachers, leaders and exponents. I do not think the role of clergy fits very well.

I have heard too many security professionals complain that their management just does not "get it." Rarely have I heard someone say, "I did not do a good enough job explaining to them the benefits security would bring to them." I suggest that the cause of management recalcitrance is not opposition to security, but an ability to see a certain *degree* of security as acceptable. A *belief* in information security does not allow degrees; less than 100 percent means that there is a hole, which means that security is incomplete, which means that there is no security at all. Effectiveness arises from comprehension that security is a variable, not an absolute.

Conferences and seminars are wonderful for learning, but they are not ideal venues for listening to different perspectives about security. If everyone in the room is a fellow professional, there are not likely to be some more strongly in favor of secure information resources and others less so. There are shared assumptions and a common vocabulary that reinforce existing parochialisms. The presentations made are about how to make security better, not good enough. It is easy to see how context could be lost and zeal could take over. If that mind-set is carried back to the office, those not similarly passionate are more likely to be turned off than to be swept up in the resulting enthusiasm.

We who are in this profession "do" security all day. It is the reason why we come to work and many of us also take it home with us, in our heads if not our briefcases. Our objective is, or should be, not to get other people to do what we do, but rather to incorporate appropriate security into what they do all day long. They should make sales securely, balance the books securely, hire and fire securely. At best, we want them to influence others to work securely as well. But we will not get them to be fellow members of a campaign because it is not their fight.

"Our objective is, or should be, not to get other people to do what we do, but rather to incorporate appropriate security into what they do all day long."

I have discussed the matter of security as a belief with colleagues and have drawn two reactions. Some treat me as an apostate for even raising the question. How could I abandon "the faith"? Others say that I am raising a straw man, that no one approaches information security as a religion or cause. In either case, I evidently have not explained my position well enough. By all means, be an advocate for information security. Be creative and influential in the communities of which you are a part. But temper the message so that information security is perceived as beneficial to the individual and the enterprise, not an unalloyed virtue unto itself.

Endnotes

1 Ross, S.; "Bear Acceptance," *ISACA® Journal*, vol. 4, 2014, *www.isaca.org/Journal/Pages/default.aspx*

2 Gurtke, C.; "No Business Too Small to Be Hacked," *The New York Times*, 3 January 2016, *www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0*. The example was not chosen idly. In 2015, Rokenbok Education, a toymaker with seven employees, was the victim of not one, but two cyberattacks.

CSX
CYBERSECURITY NEXUS

CYBER SECURITY TRAINING JUST GOT REAL

NOW YOUR STAFF CAN COMBAT REAL THREATS IN REAL TIME TO BUILD REAL TECHNICAL SKILLS.

Yesterday's lecture-based cyber security training won't protect your organization against tomorrow's advanced cyberthreats. That's why ISACA's new Cybersecurity Nexus™ (CSX) Enterprise Training Platform offers your security team:

- **On-demand access to 200+ hours of training for less than the cost of one typical course**
- **Practical, hands-on training labs performed in a live, dynamic network environment**
- **Continually updated content based on the latest real-world threats and scenarios**
- **Performance-based assessment of current and prospective employees' technical skills**

SCHEDULE A DEMO OF THE CSX TRAINING PLATFORM AT WWW.ISACA.ORG/CSXCYBERTRAINING

ISACA

Auditing Mobile Devices

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

http://bit.ly/2gimJq5

By the time this article is published, it will have been about 20 months since the US Federal Bureau of Investigation (FBI) unlocked the iPhone of the San Bernardino, California, gunman who killed 14 people.[1] The request by the FBI for Apple to build new software to unlock the mobile device resulted in strongly held opinions on encryption and backdoors on both sides[2] that have yet to be resolved. I have sympathy for all involved, but, as a technologist, I passionately believe that backdoors should not be developed. This conviction has been strengthened by the recent WannaCry[3] and Petya[4] attacks, which were developed using the leaked Shadow Brokers exploit, EternalBlue, which is generally believed to have been developed by the US National Security Agency (NSA).

Although a critical issue, this is not the focus of this column, nor is it something that we, as IT auditors, can influence on a day-to-day basis. However, an aspect of this case that received little or no coverage was the fact that San Bernardino County owned mobile device management (MDM) software that was not installed on the device.[5] This would have allowed its IT department to remotely unlock the phone and, in my opinion, save the reputation of the organization in question. This is a risk that IT auditors can and should influence. So how can practitioners audit to help mitigate this and other mobile device risk scenarios?

In a previous column,[6] I advocated the use of an ISACA® paper on creating audit programs.[7] This process can be applied to build an audit program for mobile devices for an organization.

Determine Audit Subject

The first thing to establish is the audit subject. What does a mobile device mean in the enterprise? If there are distinct types of mobiles devices in use, they should probably be recorded as separate audit universe items. ISACA categorized mobile devices (**figure 1**) in a 2012 white paper[8] while an earlier white paper[9] listed the type of mobile devices:

- Full-featured mobile phones with personal computer-like functionality, or smartphones
- Laptops and netbooks
- Tablet computers
- Portable digital assistants (PDAs)
- Portable Universal Serial Bus (USB) devices for storage (such as thumb drives and MP3 devices)
- Connectivity (such as Wi-Fi, Bluetooth and HSDPA/UMTS/EDGE/GPRS modem cards)
- Digital cameras
- Radio frequency identification (RFID) and mobile RFID (M-RFID) devices for data storage, identification and asset management
- Infrared-enabled (IrDA) devices such as printers and smart cards

In 2017, wearables, including smart watches, can certainly be added to that list. The key is to use the guidance to consider mobile devices in use at an enterprise and determine the audit subject(s). One needs to answer the key question: What is being audited?

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

Define Audit Objective

Once what is being audited has been determined, the objective of the audit needs to be established. Why is it being audited? From an auditor's perspective, it is advisable to adopt a risk-based view and define the objectives accordingly.[10]

- Identify the risk associated with the devices (**figure 2**).

Figure 1—Mobile Device Categories

Category	Devices	Examples
1	Data storage (limited), basic telephony and messaging services, proprietary operating system (OS) (limited), no data processing capability	• Traditional cell phones
2	Data storage (including external) and data processing capabilities, standardized OS (configurable), extended services	• Smartphones • Early pocket PC devices
3	Data storage, processing and transmission capabilities via alternative channels, broadband Internet connectivity, standardized OS (configurable), PC-like capabilities	• Advanced smartphones • Tablet PCs

Source: ISACA, *Securing Mobile Devices*, USA, 2012

Figure 2—Mobile Device Vulnerabilities, Threats and Risk

Vulnerability	Threat	Risk
Information travels across wireless networks, which are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, damage to enterprise reputation, nonadherence to regulation, legal action
Mobility provides users with the opportunity to leave enterprise boundaries and, thereby, eliminates many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network.	Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data
Bluetooth technology is convenient for many users to have hands-free conversations; however, it is often left on and then is discoverable.	Hackers can discover the device and launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information
Unencrypted information is stored on the device.	In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable.	Exposure of sensitive data, resulting in damage to the enterprise, customers or employees
Lost data may affect employee productivity.	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.	Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices and data that are not backed up
The device has no authentication requirements applied.	In the event that the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the enterprise and liability and regulation issues
The enterprise is not managing the device.	If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with email or store sensitive documents.	Data leakage, malware propagation, unknown data loss in the case of device loss or theft
The device allows for installation of unsigned third-party applications.	Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.	Malware propagation, data leakage, intrusion on the enterprise network

Source: ISACA, *Securing Mobile Devices*, USA, 2012

- Define objectives for each category or type of selected device; refer to information value and information risk. This is key.
- Focus on a limited number of audit objectives for a reasonable scope.

It is worth noting that although ISACA's *Securing Mobile Devices* white paper considered the vulnerability of the enterprise not managing the device, it did not consider a San Bernardino County scenario. The lesson? Spend some time considering emerging risk scenarios.

Audit objectives should also correspond to security and protection goals as defined by the enterprise (**figure 3**).[11]

Set Audit Scope

When the objectives of the audit have been defined, the scoping process should identify the actual mobile devices that need to be audited. In other words, what are the limits to the audit? This could include devices in a specific country, region or division; devices that are used for a specific purpose; or devices that contain especially sensitive data. Again, this should be risk based. Also, consider if personally owned devices (bring your own device [BYOD]) should be included.

> **"When the objectives of the audit have been defined, the scoping process should identify the actual mobile devices that need to be audited."**

Perform Pre-Audit Planning

Now that the risk has been identified (**figure 2**), it should be evaluated to determine its significance.

Figure 3—Organizational Security Goals and Audit Objectives

Security Goal	Audit Objective
Mobile device security policies and procedures are adequate and effective.	Obtain assurance over mobile device security policies and related controls at the entity level, general level and detailed control level.
Access control and encryption for mobile devices are adequate and comprehensive.	Review mobile device access controls and encryption controls in line with data and information risk as well as information classification.
Data and information segregation in brought-in devices is complete and effective.	Review concepts, methods and implementation of data and information segregation for all devices owned by and brought in by end users.
Mobile device security incident management is fully implemented and effective.	Review mobile device incident management processes and controls, and obtain assurance over the effective functioning of incident management.

Source: ISACA, *Securing Mobile Devices*, USA, 2012

Conducting a risk assessment is critical in setting the final scope of a risk-based audit.[12] The more significant the risk, the greater the need for assurance. Assurance considerations for mobile devices include:[13]

- **Policy**—Does a security policy exist for mobile devices? Does it include rules for appropriate physical and logical handling? The enterprise should have a policy addressing mobile device use and specifying the type of information and kinds of devices and information services that may be accessible through the devices.
- **Antivirus updates**—Auditors should verify that the enterprise updates the mobile device antivirus software to prevent perpetuation of malware.
- **Encryption**—Auditors should verify that any data labeled as sensitive are properly secured while in transit or at rest.
- **Secure transmission**—Auditors should determine whether mobile device users are connecting to the enterprise network via a secure connection. VPN, IP Security (IPsec) or Secure Sockets Layer (SSL) can offer some levels of assurance.
- **Device management**—Auditors should determine whether there is an asset management process in place for tracking mobile devices. This asset management program should also detail procedures for lost and stolen devices as well as procedures for employees who have been terminated or have resigned from the enterprise.
- **Access control**—Auditors should verify that data synchronization of mobile devices is not set to receive access to shared files or network drives that contain data that are prohibited for mobile use by the policy.
- **Awareness training**—The auditor should verify that the enterprise has an awareness program in place that addresses the importance of securing the mobile devices physically and logically. The training should also make clear the types of information that can and cannot be stored on such devices.
- **Risk**—Mobile devices have the capability to store large amounts of data and present a high risk of data leakage and loss. As such, mobile device policies should be created and enforced to ensure that information assets are not exposed.

The use of any mobile device encompasses several legal relationships and obligations that must be considered when auditing or reviewing devices. In partial or full BYOD scenarios, further legal obligations may arise from the fact that parts of the mobile device (and information) are considered beyond the control of the enterprise.[14] Furthermore, when the device is used for private purposes—even to a very small extent—questions of personal data protection and privacy will inevitably arise. In most jurisdictions, privacy is protected by law and additional regulations.[15] If any doubt exists, it is prudent to seek legal advice in the relevant jurisdiction.

> **“Audit programs should be considered a starting point and adjusted based upon risk and criteria that are relevant to the organization that is being audited.”**

Finally, the auditee should be interviewed to inquire about activities or areas of concern that should be included in the scope of the engagement. Once the subject, objective and scope are defined, the audit team can identify the resources needed to perform the audit work.[16]

Determine Audit Procedures and Steps for Data Gathering

At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program.[17] There is enough information to decide what documents are expected to be seen, what laws and regulations apply, the criteria and whom the audit team is going to interview. However, the testing steps do need to be defined.

In August 2017, ISACA released an updated version of its *Mobile Computing Audit/Assurance Program,*[18] which defines testing steps for mobile devices. Some readers may have just thought,

Enjoying this article?

- Read *Mobile Computing Audit/ Assurance Program.* *www.isaca.org/ auditprograms*
- Learn more about, discuss and collaborate on mobile computing in the Knowledge Center. *www.isaca.org/ mobile-computing*

"Why did he not just state this at the beginning of the article?" I refer those readers back to this author's first column.[19] Audit programs should be considered a starting point and adjusted based upon risk and criteria that are relevant to the organization that is being audited. Failure to do so can result in a checklist approach, which can lead to the auditor recommending controls that are not applicable to the organization. This, in turn, can damage the auditor's reputation with the auditee and, ultimately, with senior management.[20] It is worth spending the time considering the risk and the resulting need for assurance (**figure 4**).

Figure 4—Assurance Consideration to Audit Program Mapping

Assurance Consideration	Audit Program Process Sub-Area
Policy	Mobile computing policy
Antivirus updates	Anti-malware protection
Encryption	Device protections
Secure transmission	Wireless access points
Device management	Removable media/remote storage solutions/data recovery/asset management
Access control	Secure access/identification and authentication
Awareness training	User training
Risk	Risk management

Key testing steps in the audit program include password controls and the configuration of the selected MDM solution (if one is in place). Excellent guidance is provided on these and other aspects of mobility by the US Department of Defense (DoD) information systems Security Technical Implementation Guides (STIGs).[21]

Conclusion

As the uses, storage capabilities, power and proliferation of mobile devices have increased, so has the risk they pose to an enterprise. As a leading advocate for managing this risk, ISACA has produced several white papers in this area. Each of these documents is worth consulting to develop an audit/assurance program that is tailored to the individual enterprise. Failure to do so can result in a checklist approach, which can lead to a failure to mitigate key and emerging risk.

"As the uses, storage capabilities, power and proliferation of mobile devices have increased, so has the risk they pose to an enterprise."

Endnotes

1 Burgess, M.; "FBI Unlocks Shooter's iPhone Without Apple's Help," *Wired*, 29 March 2016, *www.wired.co.uk/article/apple-fbi-unlock-iphone-5c-court-order-dropped*

2 Elmer-DeWitt, P.; "Apple vs. FBI: What the Polls Are Saying—Updated," *Fortune*, 23 February 2016, *http://fortune.com/2016/02/23/apple-fbi-poll-pew/*

3 Symantec Security Response, "What You Need to Know About the WannaCry Ransomware," 12 May 2017, *https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware*

4 Symantec Security Response, "Petya Ransomware Outbreak: Here's What You Need to Know," 27 June 2017, *https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know*

5 Finkel, J.; "Exclusive: Common Mobile Software Could Have Opened San Bernardino Shooter's iPhone," Reuters, 19 February 2016, *www.reuters.com/article/us-apple-encryption-software-exclusive-idUSKCN0VS2QK*

6 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *www.isaca.org/Journal/archives/Pages/default.aspx*
7 ISACA, "Information Systems Auditing: Tools and Techniques, Creating Audit Programs," USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF*
8 ISACA, *Securing Mobile Devices*, USA, 2012, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security.aspx*
9 ISACA, *Securing Mobile Devices*, USA, 2010, *www.isaca.org/Knowledge-Center/Research/Documents/SecureMobileDevices_whp_Eng_0710.pdf*
10 *Op cit*, ISACA, 2012, p. 89
11 *Ibid*.
12 ISACA, *Audit Plan Activities: Step-By-Step*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/Audit-Plan-Activities_res_eng_0316.pdf*
13 *Op cit,* ISACA, 2010, p. 9
14 *Ibid*., p. 91
15 *Ibid*., p. 94
16 *Op cit,* ISACA, 2016
17 *Ibid*.
18 ISACA, *Mobile Computing Audit/Assurance Program*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Mobile-Computing-Audit-Assurance-Program.aspx*
19 *Op cit,* Cooke
20 *Ibid*.
21 Department of Defense, Security Technical Implementation Guides (STIGs), USA, *http://iase.disa.mil/stigs/mobility/Pages/index.aspx*

Sarah Orton, CISA
Is IT audit director at AstraZeneca. She has more than 20 years of IT assurance and advisory experience spanning financial services, utilities, professional services, central government and pharmaceuticals. She has worked in leadership roles during her time in professional services and, more recently, in central government and pharmaceuticals. Her expertise is in building strong relationships with key stakeholders both from a business development context and in building credibility when engaging with senior stakeholders in a business context. Orton also has the knowledge and experience to challenge businesses on complex technical issues as well as explain technology in simple terms that can be understood by all. She is a member of the ISACA Northern England Chapter board and she leads the ISACA UK and Ireland chapterwide initiative for SheLeadsTech. She also serves on the ISACA global Women's Leadership Advisory Council.

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

http://bit.ly/2gimWcR

Q: How do you think the role of IS auditor is changing or has changed?

A: The role is changing from that of technical IS auditor to that of IS controls advisory consultant, and for that, the IS auditor needs to both consolidate technical skills, but also develop their interpersonal skills and broader business knowledge to be able to provide value-added insights. With the advent of data analytics and continuous monitoring, the IS controls advisory consultant needs to recognize the value of leveraging the messaging that is contained in the data.

Q: What would be your best advice for IS auditors as they plan their career paths and look at the future of IS auditing?

A: Look for a good mentor as you start out on your journey and, while acquiring and developing technical skills, ensure that you also start to build a network to support you through your career. Joining ISACA is a great idea! ISACA chapters provide a forum for updating your technical knowledge, but also for networking and meeting some great people who are experiencing similar challenges.

Since joining AstraZeneca, I managed to connect with a great mentor. She is a woman who is outside of my line of business who I meet with on a bimonthly basis. We discuss actions I have taken in the previous month to develop my career and she offers real gems of information for me to either transform the level of my engagement or to confront issues that may be perceived barriers to my progression. I really value my bimonthly discussions with her.

Q: What leadership skills do you feel are critical for a woman to be successful in technology fields?

A: Key differentiators for a woman to be successful in technology fields are to be both credible in her subject matter (have the credentials needed to be recognized as competent) and to have good knowledge of the business. The ability to be able to translate technical risk issues into a relevant business context is highly valued by organizations. One cannot underestimate the value of emotional intelligence as a leadership tool, too. Being able to "read between the lines" of what is going on and sense the mood is vital to creating and sustaining an environment where people do their best work. Also, irrespective of gender, a vital leadership trait is to be authentic and true. These are critical to establishing the key relationships to support women in developing themselves as credible leaders of technology.

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

A: Network, network and network. If you do not feel this is something that comes naturally to you, then engage a mentor or support who can both coach you and introduce you to others so the environment does not feel so alien.

the network

She Leads IT

As mentioned earlier, ISACA provides a perfect, safe forum for you to start to build your confidence in networking.

As part of my SheLeadsTech role, I encourage women to engage with the local ISACA chapter, offering myself as a contact point for them initially until they build their confidence to engage more broadly with the group. A recent new female member attended the local ISACA chapter Annual General Meeting with the aim of building her profile by increasing her contacts in the local market. When she arrived, she was surprised to already know so many people in the room and was very comfortable networking with new people. Her confidence has grown so much that this month she is going to be a panelist for the inaugural meeting of SheLeadsTech in Manchester, UK, as a cyber security specialist in her field. I am absolutely delighted for her.

Q: What do you think are the most effective ways to address the lack of women in the technology workspace?

A: Women who are already successful in the technology workspace need to sponsor and support qualified women coming through and be role models for them. Where the environment is predominantly male, male advocates can act as mentors and support women in leadership roles to address the underrepresentation of women in the technology workspace.

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

A: Currently, cyberrisk is a key strategic risk for organizations and allows the IS auditor to broaden their role more into the business area due to it being an issue that is broader than IS. Businesses need a cross-organizational response, i.e., an organizationwide security culture and awareness campaign supported by security monitoring and reporting tailored to the business with cyber risk being reported at the highest levels within the organization.

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

A: On numerous occasions, I have worked with others in internal audit departments who have tended to have very different personality types and styles than mine. Over time this has required a "chameleon-style" approach to ensure that my opinions are received in a way that is valued and allows me to influence others to deliver the right outcomes for the business.

It is important as a leader to recognize the value of learning lessons from any mistakes made and adapt behavior, and to understand that "one size does not fit all."

www.sheleadsit.org

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

The EU General Data Protection Regulation (GDPR).

2 What are your three goals for 2018?

Build my profile, explore the next opportunity and be happy.

3 What is on your desk right now?

A5 pads with different information relating to the different subject matter I work on throughout the day, in addition to two mobile phones, a Costa cup, a small handbag and, of course, the laptop on which I am typing this.

4 What are your favorite benefits of your ISACA® membership?

The ability to keep up to date with IS audit hot topics and current and relevant methodologies, the opportunity to network with great people globally, and being able to give back to the profession that has served me so well over the years.

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

Be bold and strong and use your network to support any gaps you feel you have.

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

I am a mother, a yogini and a traveler.

Challenges of Security Log Management

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

http://bit.ly/2xYShsK

In the world of information systems, data have gained the most influential position. Data are about entities—resource, agent or event—and among these, event data are probably the most pervasive group. Even in a short period of time, a business may generate millions of data points about events, for the business thrives on creating value through events such as marketing, sales, services and client support. Interestingly, wherever events occur, there is room for logging the events. Logs are the lifeline of the information systems value chain. Financial and managerial accounting, for example, depend on logging all economic events of the entity and, in the process, creating audit trails to provide support for assurance of such events and their consequences.

Some businesses, such as Fitbit, thrive on events in the life of their customers. The Fitbit wearer generates continuous data in very large measure. Of course, the Fitbit user is not interested in individual event data, but rather the aggregate information, such as the number of steps walked in a day, or trends. For this, Fitbit logs each event—literally each step walked by the user—and processes data into information useful to the user.

As businesses capture and store high volumes of data in their operational logs every day, they also create a challenge for themselves: ensuring that the data are accurate, the common data types are standardized across all logs and the logs are protected. For Fitbit, this becomes a question of protecting the privacy of users by securing personally identifiable information (PII) in the best possible manner. Thus, the operations and resulting operational data create the need for filtering data that warrant information security measures.

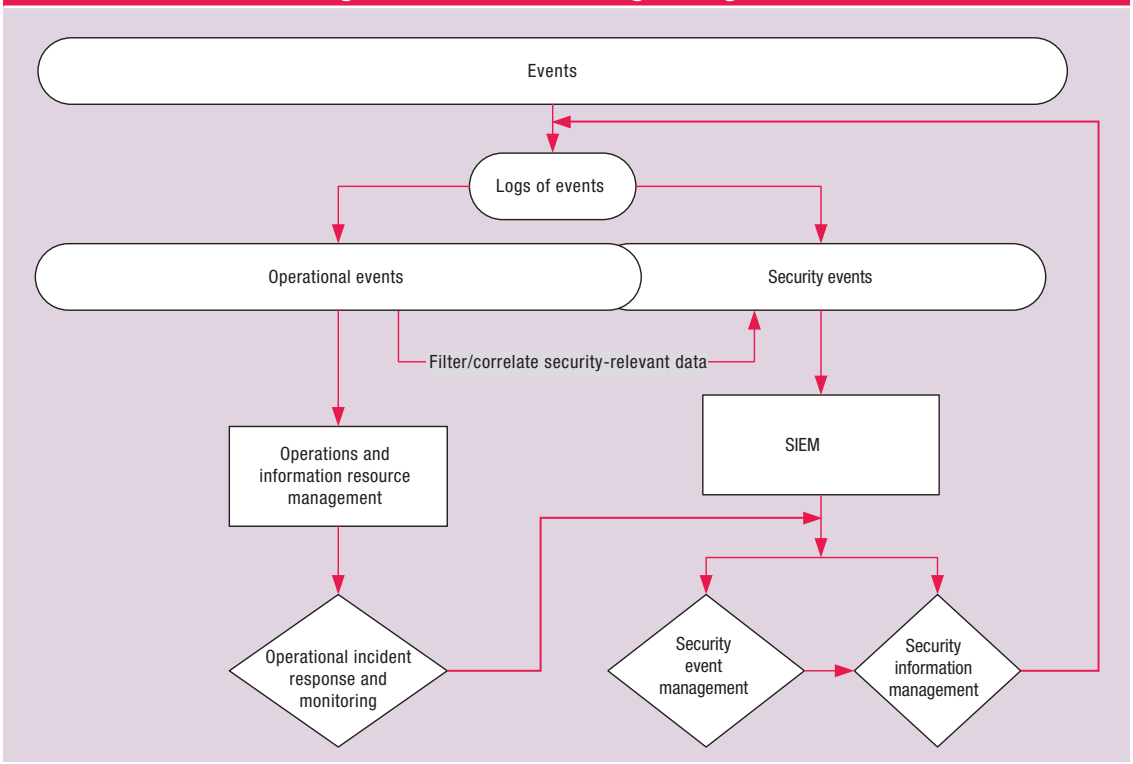
It is important to differentiate between operational data and security-related data. Fitbit creates value through operational data and, in the process, has to have information protection measures, for example, to guard the privacy of its customers. In contrast to value creation using operational data, businesses could create value by protecting clients from various information-related risk. LifeLock is an example of such a business where the company scans and monitors sensitive client identification data, provides alerts and, where necessary, helps restore the client's compromised identity.

Most businesses have both operational data and security-related data, sometimes integrated into the same database. To manage security-related data within the operational logs and data in dedicated security logs, a sophisticated technology called security information and event management (SIEM) has emerged. SIEM attempts to fulfill two separate needs: real-time monitoring, correlation and processing of security events (called security event management [SEM]) and the historical analysis of log file information (called security information management [SIM]), for example, to support forensic investigations. SEM is closely related to incident response management when the incident may concern information security. SEM represents a continuous, ongoing effort while SIM is undertaken only as needed.[1] A high-level overview of a log management scenario is presented in **figure 1**.

Vasant Raval, DBA, CISA, ACMA
Is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and corporate governance. He can be reached at vraval@creighton.edu.

Saloni Verma, CISA, CEH
Has experience in cyber security strategies, information security implementations, audits and compliance. She has worked in India for advisory services at EY, PricewaterhouseCoopers, BDO and for multinational banks. She can be reached at saloni.raghav@gmail.com.

Figure 1—Overview of Log Management



It is important to recognize that logs of operational events, while only incidentally involved in information security initiatives, may be of value to the organization. For example, a real-time monitoring of disk space utilization may be programmed to send an alert once the disk space is 80 percent full. Operational event logs should also be filtered for security-relevant data. An audit of operational logs to identify any deviations from the compliance of security log management policy should prove helpful in proactively addressing any emerging issues. An example can be seen in Uber's experience.

Organizations that do not value the importance of logging and monitoring may have to face issues in case of a breach or incident due to absence of records and evidence, or lax data management practices. This may also lead to legal, contractual or regulatory noncompliance. For example, Uber used a program called "God View," which allowed employees to monitor the locations of riders. The US Federal Trade Commission (FTC) alleged that this was an improper business practice. In a settlement with the FTC, Uber declared that, for a similar application now in use at Uber, it has limited access only to those with a critical need to access such data. As part of the settlement, Uber agreed that it will undergo third-party audits every two years for the next 20 years to seek assurance that it meets or exceeds the FTC requirements for privacy protections.[2]

> **"Organizations that do not value the importance of logging and monitoring may have to face issues in case of a breach or incident due to absence of records and evidence, or lax data management practices."**

From Technology to Solution

SIEM is a technology, not a solution. A technology can provide the backbone, or infrastructure, to develop a solution, but by itself, it will not create an optimal security log management for the business. So, the success of security log management in a large, complex enterprise depends on two related decisions:

1. Policy and strategy should drive the security log management program. Top-down risk analysis should guide decisions regarding what data to collect, how to correlate them, and how to produce and distribute information intelligence created from such logs. Staff should be competent and motivated, and challenged to continuously innovate in an area that may be perceived as static and docile.
2. Invest the appropriate amount of resources to develop an SIEM infrastructure that meets the needs of the organization. Proper selection of the SIEM technology and its customized, risk-relevant implementation within the organization is important to achieve security log management objectives.

Visa Europe, within the context of Payment Card Industry Data Security Standard (PCI DSS) data, has suggested the following steps for designing and deploying a logging solution:[3]

1. Understand the drivers.
   - Prepare for log analysis.
   - Analyze business drivers and compliance requirements.
2. Develop policy and process.
   - Scope the solution and logging strategy.
   - Develop log analysis policy.
3. Select and implement a solution.
   - Develop solution evaluation criteria.
   - Evaluate the options.
   - Develop a proof of concept.
   - Deploy log analysis.
4. Maintain and utilize the logging solution.
   - Review and refine log solution deployment.

> **“For security log management to work effectively, the staff should be experienced in the business processes of the company and be cognizant of the nature and sources of risk.”**

Challenges

There are several challenges in creating value from log management initiatives. Whether value creation involves minimizing risk, improving efficiency of operations or increasing the information supply chain effectiveness, significant challenges remain along the way. First, the task of log management may not be considered by tech-savvy staff as exciting or helpful in career building. This perception may hinder the cause of attracting talent to the task. For security log management to work effectively,

the staff should be experienced in the business processes of the company and be cognizant of the nature and sources of risk. Insights from this experience could lead to major risk-related decisions impacting what to log, how to correlate logged data, what to aggregate and how often to review the intelligence produced. This has a direct bearing on the effectiveness of the security log management policy.

Because SIEM includes SEM, it is particularly important that the incident response staff embrace SIEM and work within its scope to leverage the incident reporting activities. Without the buy-in of the incident response teams, SIEM may fail to yield the best possible results from an SIEM infrastructure. The support of an established incident response program is a necessary element of an effective SIEM solution.[4]

A second challenge rests in "balancing a limited quantity of log management resources with a continuous supply of log data."[5] Clearly, the volume, variety and complexity of data sources have increased. With limited resources, what logs to select and how to optimize the security log management function can prove to be difficult, especially at a time when there are more and more significant changes that impact data sources. Examples of such changes include the Internet of Things (IoT), device proliferation (bring your own device [BYOD]) and cloud sourcing. Sure enough, the eyes should be set on where the risk is; however, this itself remains a moving target in a dynamic, technology-leveraged organization. Under these circumstances, proving value received from security log management could be a formidable challenge.

A security log management program, by its nature, depends on filtering and correlating log data. Log data sources must support business use cases; otherwise, they will be of little value. "Sending too much data to a SIEM system will burden it with correlating and processing data unnecessarily, thus leading to poor performance."[6] Inasmuch as there is the risk of collecting too much log data, there is also the risk of not collecting enough risk-relevant data. This may be particularly critical in the life of a business where technology-induced changes are frequent and impactful. The log management team should be aware of the business processes of the organization to effectively understand the technology and business risk. With proper business knowledge, the team will be able to identify the type of necessary logs to be collected, determine the log aggregation criteria with respect to the business process, determine the threats related to the business, and efficiently store and analyze logs organizationwide.

"A security log management program, by its nature, depends on filtering and correlating log data."

In 2016, hackers stole US $81 million from a Bangladesh bank by hacking into SWIFT. The incident remained undetected for months as the logs of the fraudulent activities were being cleared by the malware.[7] Recently, hackers leaked upcoming episodes of the popular US television series *Games of Thrones* and hacked the show's network, HBO. The breach included employees' personal data and emails. Hackers have demanded US $6 million as ransomware.[8] If such attacks had been identified at the right time, HBO would not have to face these reputational and financial loss issues. Visa Europe[9] suggests that in many cases organizations are operating completely unaware of a compromise because of:

- Disabled logging
- Loss of trigger events due to overwritten logs
- Failure to monitor logs
- Lack of awareness of events being logged

Enjoying this article?

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

In the current state of information technology deployment, it is even more crucial to return the priority to security logging. However, it must be done correctly to yield benefits from the significant effort involved and the other resources it would take to implement and maintain an effective security log management program.

Endnotes

1 ISACA®, *Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives*, USA, 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Information-and-Event-Management-Business-Benefits-and-Security-Governance-and-Assurance-Perspective.aspx*

2 Bensinger, G.; "Uber Agrees to Decades of Audits to End FTC Probe," *The Wall Street Journal*, 16 August 2017

3 Visa Europe, "Planning for and Implementing Security Logging," fact sheet, *www.visaeurope.com/media/images/security_logging_factsheet-73-18417.pdf*

4 *Op cit,* ISACA, p. 8

5 Kent, K.; M. Souppaya; *Guide to Computer Security Log Management*, National Institute of Standards and Technology Special Publication SP 800-92, USA, 2006

6 Frye, D.; *Effective Use Case Modeling for Security Information and Event Management*, SANS Institute Reading Room, 21 September 2009, p. 7, *www.sans.org/reading-room/whitepapers/bestprac/effective-case-modeling-security-information-event-management-33319*

7 Smith, M.; "Bangladesh Bank Cyber-Heist Hackers Used Custom Malware to Steal $81 Million," CSO, 25 April 2016, *www.csoonline.com/article/3060798/security/bangladesh-bank-cyber-heist-hackers-used-custom-malware-to-steal-81-million.html*

8 Associated Press, "Hackers Leak More Game of Thrones Scripts and HBO Emails in Demand for Millions in Ransom Money," *The Telegraph,* 8 August 2017, *www.telegraph.co.uk/technology/2017/08/08/hackers-leak-game-thrones-scripts-hbo-emails-demand-millions/*

9 *Op cit,* Visa Europe

Digital Identity—Will the New Oil Create Fuel or Fire in Today's Economy?

亦有中文简体译本
www.isaca.org/currentissue

Digital identity has the power to propel your enterprise forward…or it can cause you to crash and burn. How you govern and manage it will make all the difference.

Think about your current state. Most in-place identity and access management (IAM) deployments are outdated and do not scale to current volumes of people, data and things—much less what is coming. Few organizations have yet adapted to emerging regulatory risk and privacy issues in the global environment. However, those that optimize their IAM architectures now can improve operational effectiveness and reduce risk. They can leverage transformative mobile, cloud, Internet of Things (IoT) and machine learning trends into innovative, identity-enabled capabilities for competitive advantage.

The New Oil

To repurpose an old quote,[1] personal data is the new oil. Historically, companies have harvested that value by launching new online customer offerings and marketing campaigns with few constraints. But tightening privacy regulations are forcing global companies to obtain and document consent in a manner compliant with jurisdiction-specific standards when leveraging personal data.

Like oil, personal data can be toxic when spilled. Studies based on industry data show the costs of a breach in the US can easily run into the 10s of millions of US dollars.[2] Even higher consequences will arrive for companies storing European Union (EU) citizens' data once the General Data Protection Regulation (GDPR)[3] comes into effect in May 2018.

Why so much friction in the brave new world of digital identity? Facing disruptive change to business practices and technologies, people and practices evolve more slowly than technology. Citizen and consumer angst are behind the privacy-related risk. Human error is often the root cause of data spills.

IAM Innovation Is About Relationship Management

Organizations use IAM for internal control, to achieve operational efficiencies and to launch new customer-facing products. Over the years, they have extended IAM to business-to-business (B2B) partners and suppliers as well as individuals or consumers.

> **"Like oil, personal data can be toxic when spilled."**

Today, IAM must cover relationships of people, mobile devices, consumer devices, cloud services, service providers and manufacturers. Privacy compliance and consent management must operate across all domains. Handled safely, a business may claim a success story like one

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

http://bit.ly/2yvidiN

Dan Blum, CISSP
Is a principal consultant with Security Architects Partners. As an internationally-recognized expert in security, privacy, cloud computing and identity management, he leads and delivers consulting projects spanning multiple industries. Formerly a Golden Quill award-winning vice president and distinguished analyst at Gartner, he has led or contributed to projects such as cloud security and privacy assessments, security program assessments, risk management framework reviews, and identity management architectures. He has provided technical security consulting engagements in all areas of data protection domains including encryption/key management, data loss prevention, privileged access management and enterprise authorization. Blum has participated in industry groups such as ISACA, the CSA, Kantara Initiative, OASIS and others.

international airport that has leveraged identity in cloud delivery models to scale operations for more than 40 million passengers annually amidst exacting security requirements.[4]

Call to Action

Handled unsafely, personal data breaches can put a company on a wall of shame.[5] On the flip side, even avoiding breaches and complying with regulations does not guarantee profits. According to Ctrl-Shift's Liz Brandt, a purely compliance-driven approach to GDPR could deliver a Pyrrhic victory, resulting in compliance with 20 percent fewer customers and loss of permission to market to a further 60 percecnt.[6] To avoid this:

- Modernize the architecture
- Adopt privacy principles
- Take an identity and privacy engineering approach

Modernize the Architecture (Federate, Do Not Aggregate)

The rise of local area networks (LANs) and the commercial Internet in the '90s spawned waves of innovation that brought us Lightweight Directory Access Protocol (LDAP) and enterprise identity-provisioning products designed to consolidate identity information into services such as Microsoft's Active Directory. Centralized directories became a mainstay of internal control. Now, with data sovereignty regulations spreading globally, centralized directories are going away.

Without them, what is next? In the second golden age of identity,[7] directories will move into the cloud and become much more distributed, virtualized and abstracted. OAuth, Open ID Connect and other standards provide a "federated identity" capability that supersedes LDAP by enabling cross-domain single sign-on, attribute management, and access control.

Successful businesses are integrating IAM with applications via application programming interfaces (APIs) leveraging OAuth and related standards. Internally, organizations should be integrating IAM with human resources (HR), awareness/training, supplier relationship management and security analytics. Externally, they should be building consistent customer relationship management processes across their various business units. Identity as a Service (IDaaS) solutions are gaining favor by making it easier to integrate identity across diverse IT ecosystems including Software as a Service (SaaS) environments.

Adopt Privacy Principles Into the Business Process

Australia, Canada, the European Union and many other jurisdictions mandate strong privacy rights that consider individuals to be the owners of personal data. In addition to compliance, companies have other incentives to get privacy right. Adopting privacy-friendly principles and communicating them clearly may encourage customers to share information they would otherwise hold back.

What principles? We can summarize GDPR principles[8] as an example:

- Provide fair, lawful and transparent processing of personal data.
- Limit use to declared purposes.
- Limit collection.
- Ensure data quality.
- Limit retention periods.
- Allow persons to delete or remove records where possible or legally required.
- Provide data security.
- Demonstrate compliance.

Take an Identity and Privacy Engineering Approach

Companies that successfully "talk the talk" with privacy principles should also "walk the walk" by giving customers easy-to-use tools to control their own data in ways appropriate to the service provided. Winning hearts and minds on privacy may win share amidst the coming GDPR churn.

The next challenge is to securely extend identity and privacy functionality across global partner ecosystems. Online retail is converging with

brick-and-mortar retail, and both are converging with media, mobile, financial services and business services. Using modernized federated architectures, innovative IAM architectures can provide customers with a convenient experience across these domains without the Yet Another User Password (YAUP) drag. They can maintain brand consistency and trust in the process.

Few have mastered the multidomain customer experience challenge to date. Either the front-end customer authentication is too weak to be so widely trusted, trusted brokers are not available to transfer attributes needed for authorization, or back-end business processes are not integrated across domains. Further adoption of multifactor authentication and standards from groups such as FIDO Alliance[9] for online authentication will help. But organizations also need to develop or subscribe to sophisticated identity provider (IDP) hub architectures and interconnect them via APIs.

> **"To fuel the business in the second golden age of identity, we must all be innovators."**

Unfortunately, regulations such as GDPR will increase the risk to companies interconnecting their online ecosystems and brands. The YAUP will not go away easily. But there are opportunities to add privacy and consent machinery to the federated identity environment. For example, new standards such as User Managed Access (UMA)[10] and the Consent Receipt Specification[11] are emerging that will make it easier to either put customers in control of personal data and their usage and/or implement explicit consent processes.

To fuel the business in the second golden age of identity, we must all be innovators.

Endnotes

1 Rotella, P.; "Is Data the New Oil?," Forbes.com, 2 April 2012, *https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#64ee40a57db3*

2 Blum, D.; "Security Business Case for Breach Risk Reduction (Part 1)," Security Architects Partners, 13 April 2016, *http://security-architect.com/security-business-case-part1/*

3 Karczewska, J.; "COBIT 5 and the GDPR," *COBIT Focus*, 19 May 2017, *www.okta.com/customers/gatwick-airport*

4 Okta, Gatwick Airport Takes Flight With Okta, *https://www.okta.com/customers/gatwick-airport/*

5 Information Is Beautiful, World's Biggest Data Breaches, 5 January 2017, *www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*

6 Brandt, L.; "GDPR: Spend It and Sink It or Spend It and Grow It," LinkedIn, 23 February 2017, *https://www.linkedin.com/pulse/gdpr-spend-sink-grow-liz-brandt-nee-brown-*

7 Blum, D.; "The Second Golden Age of Identity," Security Architects Partners, 22 November 2016, *http://security-architect.com/second-golden-age-identity/*

8 Gabel, D.; Hickman, T.; "Chapter 6: Data Protection Principles—Unlocking the EU General Data Protection Regulation," White & Case, 22 July 2016, *https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection*

9 FIDO Alliance, https://fidoalliance.org/

10 Kantara Initiative, UMA, 14 March 2017, *https://kantarainitiative.org/confluence/display/uma/Home*

11 Kantara Initiative, Consent Receipt Specification, 8 May 2017, *https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification*

Governance, Risk, Compliance and a Big Data Case Study

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

http://bit.ly/2hSTf5I

By showing what would have changed if a previously successful big data analytics project was performed given today's governance, risk and compliance (GRC) imperatives, this article highlights the GRC considerations that should be incorporated by design into any new big data project.

This project did not begin with the intention of being based on big data at the outset. Rather, big data was found to be incidental to helping solve a business problem for a Forbes Global Top 1000 bank. It is only in retrospect that the bank found it had met the definition of big data as part of its solution to achieve data-driven customercentricity.[1]

Guy Pearce
Has served on five boards of directors and two management boards in banking, financial services and retail over the last decade. He also served as chief executive officer of a multinational retail credit business that served 100,000 customers in three countries, where he led the organization's 700 staff to profitability soon after the 2008 global financial meltdown. He has published numerous articles on cyberrisk, big data and various aspects of governance, and he currently consults in strategy, risk, governance, IT, big data and analytics.

Defining Governance, Risk, Compliance and Big Data

To ensure this article is interpreted as intended, the following definitions are provided:

- **Governance**—"[S]tructures and processes that are designed to ensure accountability, transparency, responsiveness, rule of law, [and] stability…"[2]
- **Risk**—"The effect of uncertainty on [business] objectives."[3]
- **Compliance**—Acting in accordance with a wish or command.[4]
- **Big Data**—High-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.[5]

A Business Summary of the Big Data Case Study

The market share of the bank was under pressure due to increasing competition. Data-driven customercentricity proved to be an effective solution to the problem, putting the bank on track to regain market share. The bank regained market share through the creation of US $94.95 million in incremental value for the bank within six months. The way the value was created for both the bank and its customers provided a peek into the power of a customercentric paradigm.

As part of the process of understanding the business problem, the outcome of multiple focus group sessions with a representative sample of customers showed that the bank was not meeting its customers' expectations, a finding in parallel with the bank's own market research (**figure 1**).

Figure 1—Parallels Between the Market Research Findings and Customer Expectations (Extract Shown)

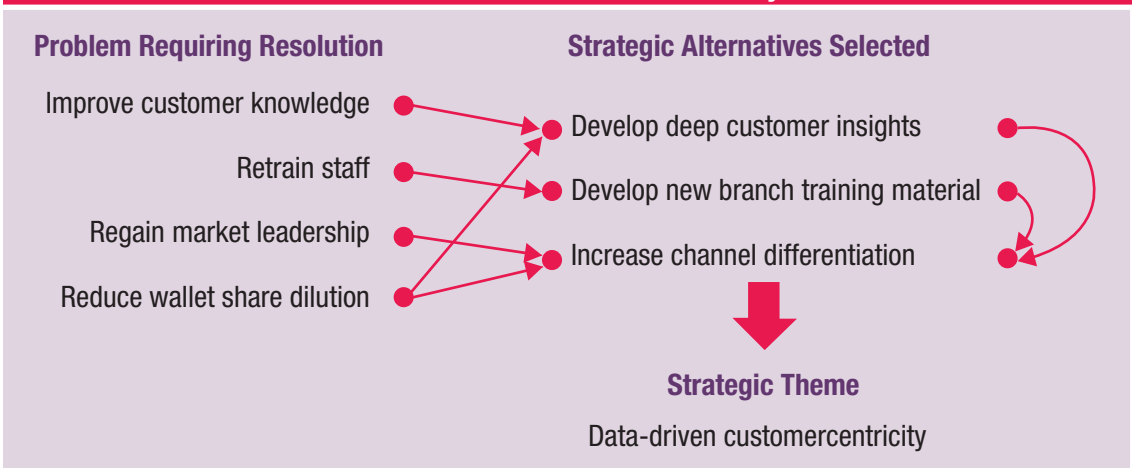
What the Market Research Showed	What the Bank's Customers Wanted
The bank was second to its major competitor for having competent and knowledgeable staff and for understanding its own products and services.	Bank staff with good knowledge of the bank's products and services
The bank was third to its two major competitors for understanding its customers' needs.	Staff that understand them

Corrective actions were then identified and prioritized according to their urgency and impact, and prospective solutions were filtered based on their risk-adjusted business cases and their ease of implementation.

The deep customer insights raised in **figure 2** were categorized as products and services, product utilization, channel utilization, wallet dilution, economic insights, industry insights, and regional insights. The data needed as inputs for these insights—made up of both internal and external, and structured and unstructured data—were identified. However, not knowing the quality and, therefore, the eventual usability of the analytics posed a considerable business risk. Processes were thus created and executed to determine the completeness, uniqueness, validity and accuracy dimensions of data quality for the data elements identified. In one case, the findings of the data quality assessments were such that enterprisewide data restitution was performed to increase the completeness attribute of a key data element.

After resolving data access, data integration, data quality, data cleansing and data fusion (structured with unstructured, and internal with external) issues, a portfolio of descriptive, behavioral and predictive analytics initiatives were performed on the consolidated data source.

Figure 2—The Path From the High-Priority Solution Requirements to Data-Driven Customercentricity



Enjoying this article?

- Read ***Big Data: Impacts and Benefits.*** *www.isaca.org/big-data-wp*
- **Learn more about, discuss and collaborate on big data in the Knowledge Center.** *www.isaca.org/big-data*

The point of deployment gets tougher given the growth in privacy legislation today. While few laws were applicable to leveraging data when the case study was performed, two observations are useful at this point. First, the bank already had working business relationships with their clients, implying consent in today's terms. Second, data-driven customercentricity was not just a phrase. It meant the creation of two-way value. Value was created for the bank because real value was created for customers. The results bear this out.

Once prototyping proved that data-driven customercentricity could address the business problem, senior approval was given for enterprise deployment. This involved distributing periodically generated analytics-derived customer insights to 1,300 branches using a customer relationship management (CRM) tool. Customer-facing bank staff now had access to key insights on each of their customers and could consequently strategize about how to have more meaningful and mutually beneficial conversations with them.

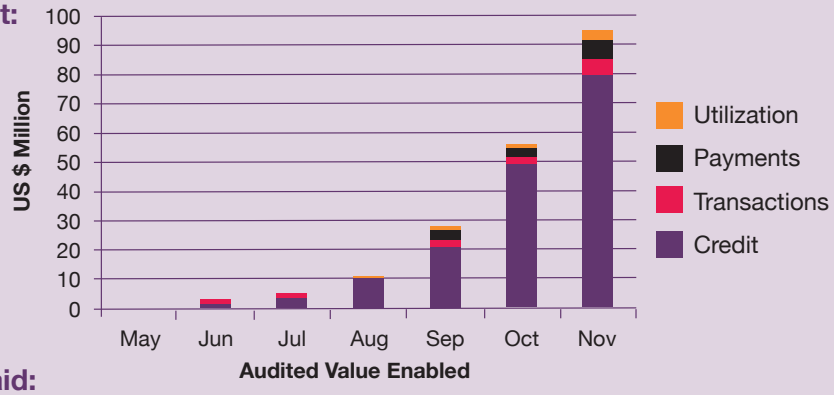
Coupled with improved training on the bank's products and services (**figure 2**), bank staff could now better link the right products and services with the position of their customers during their unique banking life cycles. Customer interactions were consequently more relevant and meaningful, resulting in sales strike rates of almost one in two (50 percent). This is a noteworthy result because direct marketing strike rates are only about five percent.[6] This outcome demonstrates the superior effectiveness of relationship marketing over direct marketing, a very interesting dimension of competitiveness. **Figure 3** shows the overall results of these efforts.

While the bank's customers experienced better-focused interactions from bank staff, the bank, in turn, experienced a financial uplift by increased sales and activity in four ways, as shown in **figure 3**.

Figure 3—What Was Achieved and What Bank Staff Said to the Project Team

Outcomes

What they got:



What they said:

"We will use your work to boost sales scorecard performance," AVP sales
"Come and help us meet our scorecard targets," AVP New Business
"Where have you been all our lives?," Provincial sales manager
"When are you coming to help us?," Provincial sales manager
"The great thing is that it is not rocket science," EVP
"We need to entrench your work," VP
"This is big," VP
"Go big," EVP

While big data was instrumental to success, note that it was incidental. The bank did not seek to solve a business problem with big data. Rather, by first appropriately understanding the problem and then objectively implementing the best response from a set of alternatives, the bank ended up with a big data-driven approach to customercentricity.

So did the foundation of the data-driven project qualify as big data? Based on the big data definition introduced earlier, yes. Those definitions are:

- **High-volume data**—Multi-terabytes of data were produced.
- **High-velocity data**—Transaction volumes were around 1,000 transactions per second at peak.
- **High-variety data**—Structured and unstructured data, both internally and externally sourced from across multiple divisions of the bank and from specialist data vendors. They included government gazettes and national, provincial and regional economic forecasts. The potential of these disparate data sources was unlocked by data fusion for data enrichment
- **Innovative processing**—New database technology was needed to accelerate the daily data processing required to produce up-to-date customer insights to the field in a timely manner.
- **Enhanced insight and decision making**—Better customer insights mean significantly higher quality customer engagement, resulting in enhanced financial outcomes, as shown in **figure 3**.

The Impact of Governance

Data governance is one of the greatest challenges to corporate governance because many boards ignore the risk posed by the mismanagement of data.[7] Demonstrating the potential to appropriately mitigate this risk, 16 areas of alignment were found between data governance (using the Data Management Association International [DAMA's] framework) and corporate governance (using Deloitte's framework) that could be meaningfully applied in pursuit of risk mitigation.[8, 9]

Consider what the impact of today's corporate governance and data governance disciplines would have been if the big data project was taken on now, starting with corporate governance.

For data governance, note that the impact is partially reflected by the integrity pillar in **figure 4** and partially by privacy principle two in **figure 5.**

The overall governance implications of the big data project are clearly significant. Three of the six pillars of corporate governance would demand at least some change to the project's approach, with data governance possibly having the most governance implications for implementation.

Figure 4—The Implications of Today's Corporate Governance Pillars

Pillar[10]	Impacted?	Comments
Governance	Yes	While an executive committee provided a means of control for a project that could have incurred incremental operational risk for the bank, today, data governance, IT governance and even the enterprise program management office (EPMO) could form additional controls in large corporations.
Strategy	No	There were already direct links to the bank's strategy.
Performance	No	There were already direct links to the bank's performance.
Integrity	Yes	While some consideration for the quality of the insights was applied by testing the data, there was no consideration for metadata or master data management, which are modern imperatives for data.
Talent	Yes	There was no consideration of the succession risk in a project that spanned multiple years.
Risk	-	Considered in the next section

Figure 5—The Impact of Today's Privacy Regulations Should the Case Study Have Been Performed Today

Privacy Principle	Impacted?	Comments
1. Data collection should be limited, lawful, fair and with the knowledge or consent of the data subject where appropriate.	No/limited	Customer data previously captured online and in branches and stored on the bank's operational databases were used.
2. Personal data should be relevant to the purposes for which they are to be used, and they should be accurate, complete and kept up to date.	Yes	Clarity would be required on purpose and relevance, given that some personal data will have been captured decades ago and that some personal data have a regulatory component, e.g., know your customer (KYC). Furthermore, in banking, data quality (DQ) is encapsulated in regulation driven by Basel Committee on Banking Supervision regulation no. 239 (BCBS239). While some DQ was performed, note that because BCBS239 extends to data governance, metadata and reference data, more DQ initiatives would be needed. Limited attention was applied to governance, metadata and reference data management in the project.
3. The purposes for which personal data are collected should be specified by the time of data collection and the subsequent use limited to the fullfilment of those purposes.	No/limited	Data used for analysis, even if they come from a database and are not explicitly collected for a project, should be checked to ensure that they do adhere to the limited-use principle. This regulation was not in place at the time of the project.
4. Personal data should be protected by security safeguards against risk factors such as loss or unauthorized access, destruction, use, modification or disclosure.	Yes	While the need for information security and cyber security is clear today, another keyword to note is "destruction." This implies the need for appropriate data life cycle management strategies, policies and procedures that were not in place at the time of the project.
5. There should be a policy of transparency around the organization's practices and responsibilities for personal data.	Yes	With the emphasis on the word "organization," there were no overarching data governance (including compliance) structures for the bank at the time. There were, thus, no transparent processes, responsibilities and accountabilities for (personal) data as there are by means of data stewards and data governance today.
6. Individuals have the right to request what information an organization has on them.	No/limited	The right of access to information does not have clear implications for this type of initiative.
7. A data controller should be accountable for complying with the previous measures.	Yes	While there was financial oversight of the initiative, there was no formal data oversight as would be provided by today's data governance structures. Increased oversight of regulatory compliance would also be required to mitigate reputation risk.

The Impact of Risk

The greatest risk boards of directors need to protect against is reputation risk.[11] Because an organization's reputation can be negatively impacted today by, for example, the incorrect or inappropriate use of data or by not complying with privacy regulation, appropriate controls need to be put in place to mitigate this risk.

Corporate governance mitigates some of this risk by enterprise risk management (ERM) within the risk pillar, while data governance mitigates some of this risk by means of the policies, procedures, standards, guidelines and tools used to perform and assess various characteristics of the data asset, and to ensure adherence to the enterprise's policies for audit purposes.

Originally, the executive committee provided a means of risk management, noting that data governance as a risk mitigator was not yet as formal as it is now. Today, more formal ERM would be required for a project of this scale and impact, and it would have to be presented for review by senior members of the bank. Furthermore, cyber security was in its infancy, relatively speaking.

An important matter for a data team to understand about cyberrisk is the risk of a breach of personal information both before deployment and on deployment. This means risk must be mitigated using appropriate response plans, the content of which may differ by jurisdiction. Besides the regulatory requirement for breach reporting, some jurisdictions also need to understand the risk of significant harm arising from the breach. This risk necessitates an assessment of the sensitivity of the exposed data and the probability that these data will be misused.[12] Many executives still have no idea where their sensitive data are, even though there are modern tools available to support their discovery.[13]

The Impact of Compliance

In 2015, 109 general privacy laws were active globally, and 49 percent of them were in the European Union. A significant addition to this list today would be the EU's General Data Protection Regulation (GDPR), enforceable beginning in May 2018.[14] Given that the European model is the leading global privacy model, the key elements of privacy legislation from this model should be considered in the context of this big data case study (there will be some similarities across other jurisdictions).[15, 16]

Doing the project today would be impacted by principles two, three, four and five, with consequent implications for project management, team size, team composition, and the time and financial resources required to execute the project. Also, principle seven requires the appropriate oversight and assurance of all customer-facing data-driven initiatives today.

> **"The modern GRC landscape has a significant impact on how an enterprise-scale big data project would be undertaken today."**

Conclusion

The modern GRC landscape has a significant impact on how an enterprise-scale big data project would be undertaken today. Much of the impact falls under corporate governance's integrity pillar. This pillar aligns data governance with corporate governance, helping ensure that data activities subscribe to enterprise standards of integrity.[17]

Figure 6 summarizes the major areas of impact of GRC on a big data project applicable from the perspective of the European model of privacy, which, as noted, is the dominant global model.

Figure 6—The Drivers of the Biggest Impact to an Enterprise-Scale Big Data Project

Category	Governance	Impact Summary
Governance	Corporate	Given the scope and duration of the project, succession planning is needed to ensure the appropriate level of continuity for long-term projects.
Risk	Corporate and data	There is a clear need to establish the relevant data controls and oversight and to understand the risk and impact of a breach of sensitive personal and financial information both before and during deployment.
Compliance	Data	There is a need to ensure the requisite level of data quality. Ensure that the privacy regulations around these data in the relevant jurisdictions are adhered to if any data are purposefully collected (i.e., not already existing in a database). Check the applicability of the limited use principle (principle three in **figure 5**).

This article provides an overview of the likely impact of GRC on today's big data initiatives. Given the span of risk and compliance issues and the relationship between corporate governance and data governance, this article is not exhaustive in content, in highlighting the complexities of each jurisdiction, in highlighting the complexities of data and information movement between jurisdictions, or even in highlighting the relevant content in a single jurisdiction. The article does, however, highlight the need to be increasingly aware of regulatory considerations—such as those concerning privacy—as part of both current and proposed big data projects, particularly if data are involved in driving how the enterprise interacts with its customers.

Endnotes

1 Sicular, S.; "Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused With Three V's," *Forbes*, 27 March 2013, *https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#4626650842f6*

2 United Nations Educational, Scientific and Cultural Organization, "Concept of Governance," *www.unesco.org/new/en/education/themes/strengthening-education-systems/quality-framework/technical-notes/concept-of-governance/*

3 Lark, J.; "ISO 31000 Risk Management: A Practical Guide for SMEs," International Organization for Standardization, Switzerland, 2015, *https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_31000_for_smes.pdf*

4 English Oxford Living Dictionaries, "compliance and comply," *https://en.oxforddictionaries.com/definition/compliance*

5 *Op cit,* Sicular

6 Chaffey, D.; "Marketing Campaign Response Rates," *Smart Insights*, 11 October 2012, *www.smartinsights.com/managing-digital-marketing/planning-budgeting/marketing-campaign-response-rates/*

7 Yordanova, V.; *Filling the Gaps of Big Data Regulation*, master's thesis, Maastricht University, The Netherlands, 2015

8 Pearce, G.; "Align Data Governance With Board Governance Imperatives," TDAN.com, 3 May 2017, *http://tdan.com/align-data-governance-with-board-governance-imperatives/21355*

9 Data Management Association International, Body of Knowledge, *https://www.dama.org/content/body-knowledge*

10 Deloitte, "The Role and Benefits of a Corporate Governance Framework," *The Wall Street Journal*, 24 May 2013, *http://deloitte.wsj.com/riskandcompliance/2013/05/24/the-role-and-benefits-of-a-corporate-governance-framework/*

11 Dowling, G.; "Reputation Risk: It Is the Board's Ultimate Responsibility," *Journal of Business Strategy*, vol. 27, iss. 2, 2006, p. 59–68

12 Jones, P.; L. Walker; "How to Navigate Landscape of Global Privacy and Data Protection," American Bar Association, USA, 2–4 November 2016, *https://www.americanbar.org/content/dam/aba/images/franchising/annual16/course-materials-16/w22-navigate-global-privacy.pdf*

13 Pearce, G.; "Boosting Cyber Security With Data Governance and Enterprise Data Management" *ISACA® Journal*, vol. 3, 2017, *www.isaca.org/Journal/archives/Pages/default.aspx*

14 General Data Protection Regulation (GDPR), "GDPR Portal," European Union, *www.eugdpr.org/*

15 *Op cit,* Dowling

16 Bank for International Settlements, *Principles for Effective Risk Data Aggregation and Risk Reporting*, Switzerland, 2013, *www.bis.org/publ/bcbs239.pdf*

17 *Op cit,* Chaffey

Auditing Big Data in Enterprises

亦有中文简体译本
www.isaca.org/currentissue

There is no stagnation in information security. One major national incident often leads to more robust reporting requirements, paperwork and additional duties. In 2013, Edward Snowden's actions became a catalyst of change for accountability, insider threat programs and the auditing of privileged users. Though the resulting good practices highlight what needs to be done to adapt to new threats posed by those with privileged access, the strategy to accomplish this mission can be outdated.

How can an information systems security officer (ISSO) or information systems security manager (ISSM) find suspicious behavior among the breadth and depth of information that comes pouring out of information systems? A system might have 10 users or 100 users, each putting in eight hours of activity per day, in addition to continuous background chatter mixed with various service groups and working group accounts. Most auditors are responsible for multiple systems and are likely updating plans and baselines, performing compliance checks, giving security education classes and briefings, attending mandatory meetings, approving or denying requests for accounts, and addressing myriad other activities. Depending on the size of a system and the auditor's review logs, the system may produce a week's worth of data in one day. The auditor is expected not only to perform the due care of ensuring the log exists and is uncorrupted, but also to review the logs for abnormalities and malicious behavior.

The amount of data reviewed has changed the scope of an information security professional from an auditor to a data mining and analytics expert. That change demands a new set of skills.

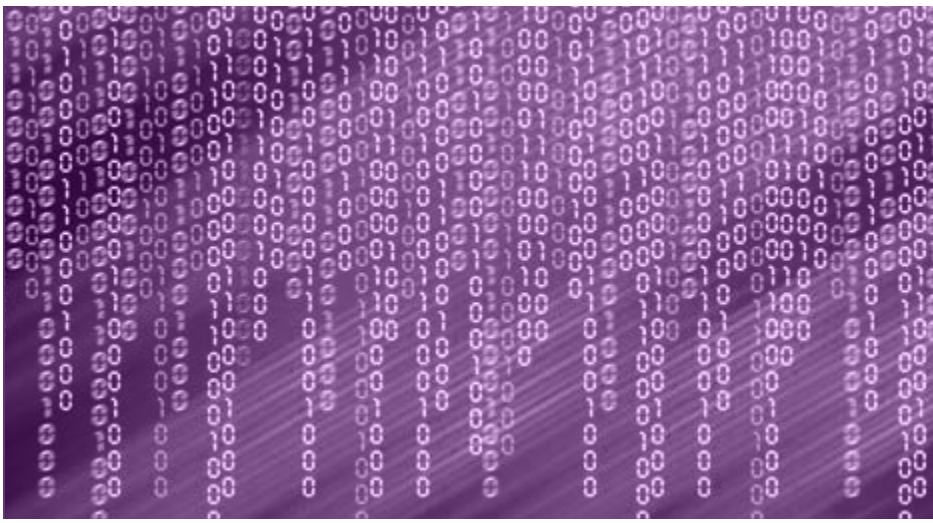
System Audit

A system audit is a countermeasure used to review and analyze the actions of users on a system. In an age where separation of duties is best practice, the system audit is typically performed by a designated security professional as opposed to a system administrator. An audit is a shallow review of system events that ends rather quickly, as opposed to a deep discourse that continues for weeks and months. Data mining may seem counterintuitive to an auditor. After all, one of the primary roles of an ISSO or ISSM is to ensure information integrity. Defending against the manipulation of data by authorized or unauthorized persons is a founding principle of information security. However, data mining and analytics are rooted in manipulating data.

To audit big data, the word "audit" must be left behind. It is an insufficient term to describe the security review of a system. Even as objective, goal and mission should not be used interchangeably but should instead point to a duration of time (short term, middle term and long term, respectively), so, too, is auditing a technique used for smaller amounts of data. A standalone system can be audited. A peer-to-peer system can be audited. A networked system that exists over a wide area network (WAN) or a local

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

http://bit.ly/2xmxjH6



Abdullah Al-Mansour, Security+
Is an information systems security professional. His interests include analytics, data mining and technology.

Enjoying this article?

- Read *Data Privacy Audit/Assurance Program.* *www.isaca.org/auditprograms*
- Learn more about, discuss and collaborate on governance of enterprise IT (GEIT) in the Knowledge Center. *www.isaca.org/governance-of-enterprise-it*

area network (LAN) that produces encyclopedic volumes of data weekly cannot be audited. These more complex networks must be data mined.

Preexisting Resources

Thankfully, popular software, such as MATLAB, has inadvertently addressed the needs of the security professional by being highly reliable tools in fields that utilize mathematics and scientific modeling to analyze data. These same tools that assist in other professional communities' methodologies must be embraced and adopted for a post-Edward Snowden security environment.

> **"The use of patterns makes data mining scalable."**

At the base level, ISSOs must speak the language of computing, not just compliance. Whether C++, Visual Basics or Python, to effectively data mine event-related logs, the ISSO will need to become familiar with a programming language. The ISSO must understand, on a conceptual basis, dictionaries, lists, arrays (e.g., two-dimensional arrays, three-dimensional arrays), Boolean, defining functions, conditional statements and loops, to name a few. The ISSO is often the first line of defense and must become more engineering-minded as the burden of catching and detecting malicious activity increases. Security departments will need to invest in engineering education as it pertains to the science of data manipulation and analytics.

Patterns

How does one find the proverbial needle in the haystack? The answer is through patterns.

No one has time to sift through mountains of data. The use of patterns makes data mining scalable. A system has patterns, and the patterns form baselines. An information system is not limited to a primary baseline. Service accounts, privilege accounts, general user accounts, first shift, second shift and testing times can all be grouped individually and cohesively for the purpose of finding commonalities or discrepancies. A typical security event log can be divided into successes and failures and then compared for recurring failures that later lead to a success. Patterns can be found through coding, conditional statements, loops and the like.

Analytics

Once patterns are gathered and centralized, analytics can be employed to measure the frequency of occurrence, the bit sizes, the quantity of files executed and average time of use. The math involved allows a data miner to grasp the big picture. Individuals are normally overwhelmed by the sheer volume of information, but automation of pattern-recognizing techniques makes big data welcome.

The larger the sample size, the easier it is to determine patterns of normal and abnormal behavior. Network haystacks are bombarded by algorithms that notify the information archeologist about the probes of an insider threat.

Education

As with all new developments, education is a founding necessity of data mining. The benefits of coding to gather information and analytics to dissect it are lost if a data miner does not know how to interpret the information. The ones and zeros must have substance. The averages that make up the bell curves of statistics determine the likelihood that an event has occurred, is occurring or will occur.

Such statistics are useless to the untrained reviewer. There are several reputable organizations that offer free classes for those who want to pursue careers as data analysts. Udacity[1] is an online learning platform that offers several classes—beginner, intermediate and expert—and teaches data analysis using Python software with coding libraries Numpy and Pandas. EdX[2] is another free website that has formed educational partnerships with Harvard

University (Cambridge, Massachusetts, USA), Microsoft, Massachusetts Institute of Technology (MIT) (Cambridge, USA) and others. EdX offers an introduction to data analysis using Microsoft Excel.

Lessons Learned

There is no one magic formula to audit big data. Experiences have to be translated into code and built upon. For example, a script was deployed to check for the daily audit logs. Should the audit log not exist, the ISSO would be notified through automation. Each day the script would check for the expected date of the audit and, as expected, the audit and the date would be in the appropriate write-protected folder. However, the script was not checking to ensure that the previous days' audit logs were in the same folder. Each day the original file was overwritten by the new file. The error in audit scripting may have been an isolated event, or the overwrite could have been systemic. Small lessons learned, such as this, help to develop a more refined automation process that measures information assurance, and that system of measurement can be spread across the enterprise to find similar outliers on other networks.

Data Structure

Another aid in the war on outliers is data representation. There is nothing worse than being an ISSO for a system that has only raw data. From the old Windows event viewer to a Solaris audit log, raw files are heinous to survey. The least a system administrator could do is delimit the lines and include some column headers. A descending numerical index could also help.

The flow of the data should be organized and, given today's functionality, employ the option of graphical representation: Linear representation, bar graphs, pie charts, analytics and color can help make the data much easier to interpret. Thousands of lines of data and countless hours of scrolling can, in fact, become a five-minute study of a line graph accurately displaying patterns of activity for the day, week or even month.

Communication

A key ingredient in any process, including data mining, is communication. If an ISSM is unaware of the anomalies or trends occurring across the enterprise, the definitions and pattern identification that can mitigate and prevent those trends may not manifest. The user computing habits of Company A, which is located on the west coast of a country, need to be juxtaposed with Company A's satellite factory residing on the east coast of that country.
An obstruction to good communication is self-preservation. There exists a natural reluctance to share information because it could paint a negative portrayal of a person or work location, and this reluctance hinders the overreaching data mining process. If one site participates in honest data collection and another site does not, eventually both sites will not. Without communication, data mining on an enterprise level will always be hindered.

> **"Communication provides a centralized location where analytics can be gathered and assessed to find trends and patterns."**

Communication provides a centralized location where analytics can be gathered and assessed to find trends and patterns. If the data are padded, the ability to develop countermeasures is slowed and their effectiveness is reduced. As with most successful enterprise-level endeavors, effective communication starts at the top levels. If there is a policy in place to foster cohesion, functional managers can execute that policy and craft processes that support and sustain it. Weak communication is indicative of a poorly constructed policy, which translates into a misunderstood vision and inevitably leads to restrictive communication.

Networks are producing more information than ever before. Auditors must be equipped with the tools needed to meet the challenges of ensuring confidentiality, integrity, access control and availability. To achieve this mission, an auditor's mind-set must evolve from a smaller data management skill set. Without the tools that come from data mining and analytics, the auditor will be overwhelmed on a daily and weekly basis. As a result, the quality of review will degrade from assured due diligence to due care or perhaps due diligence for only the first couple hundred lines of captured data.

> **"Quantitative analysis adds depth to an audit and introduces models by which events can be predicted based upon numerical trends."**

Learning how to write scripts that loop through audit logs in search of specific patterns is crucial. Graphical representation of the data opens the door to analytics and allows the auditor to see the big picture and identify trends. Communication will facilitate the distribution of data on user behavior and increase the pool of information for better statistical analysis. These are keys for effective enterprise auditing.

Quantitative

Success at an enterprise level requires an ISSO to write scripts that provide a greater analysis of events. This data might be the number of people who log in every week or the daily size of an audit log. The aggregation of this data can be used to determine the average rate of occurrence, which, in turn, establishes a baseline of normality for a system. Recording the frequency of occurrence can also be used to anticipate events such as malfunctioning scripts or influxes of user activity. Quantitative analysis adds depth to an audit and introduces models by which events can be predicted based upon numerical trends.

Conclusion

Without analytics, enterprise-level auditing is a diminished discipline, limited in scope and effectiveness. Without an educated auditing workforce, armed with a programing language for automation and a data-mining philosophy and skill set, the needs of leaders at the enterprise level will go unmet. Leaders will not have the data needed to analyze on a large scale nor a workforce that is capable of getting them the data on a weekly or daily basis.

The beauty of analytics, from a security perspective, is that it allows the security department to align with the critical functions of corporate business. It can be used to discover recurring incidents and common trends that might otherwise have been missed. Establishing numerical baselines or quantified data can supplement a normal auditor's tasks and enhance the auditor's ability to see beneath the surface of what is presented in an audit. Good communication of analyzed data gives decision makers a better view of their systems through a holistic approach, which can aid in the creation of enterprise-level goals. Data mining adds dimension and depth to the auditing process at the enterprise level.

Endnotes

1 Udacity, *https://www.udacity.com/*
2 edX, *https://www.edx.org/*

A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance

Process guidelines and a framework for boards of directors and senior management must be considered when providing oversight, examination and risk management of third-party business relationships in the areas of information technology, systems and cyber security.

It is hard to find any enterprise that does not rely on third parties to support its operations. Senior management and the board of directors are ultimately responsible for the risk that third-party vendors, contractors and systems impose on the enterprise.

Third parties include, but are not limited to, technology service providers; payroll services; accounting firms; invoicing and collection agencies; benefits management companies; and consulting, design and manufacturing companies. Most third-party commercial relationships require sending and receiving information, access to the enterprise network and systems, and using the enterprise's computing resources. The risk posed at different levels and the impacts range from low to very significant.

Outsourcing an activity to an outside entity is by no means removing the responsibility, obligation or liability from the enterprise, but these activities are considered integral and inherent to operations. As a result, the enterprise is obliged to identify and mitigate the risk imposed on it by third-party commercial relationships.

The number of security breaches and incidents that are the result of third parties is rising. Based on PricewaterhouseCoopers (PwC's) Global State of Information Security surveys from 2010, 2011 and 2012, the number of security incidents attributed to partners and vendors increased from 20 percent in 2010 to 28 percent in 2012.[1] The problem is worsening as the number of enterprises relying on third-party vendors and contractors is on the rise.

Soha System's Third Party Advisory Group surveyed information technology and security managers, directors and executives and found that "with 63 percent of all data breaches linked directly or indirectly to third-party access, those contractors and suppliers who need to get access to corporate applications in order to get their job done represent risk to any enterprise."[2]

The issue of third-party risk is greatly complicated for global enterprises by the sheer number of third parties and contractors that they use to supplement staff requirements and/or services.

The pressure is increasing on global, national, and large or small enterprises to plan, perform, remediate, monitor and report the results of the risk assessment, degree of risk and compliance (regulatory or nonregulatory) that third-party vendors may impose.

Information systems enterprises grant third parties access to company applications, network infrastructure and data centers. However, the senior management team needs to be aware of the severity of such invasive activities to weigh the associated risk factors and to ensure that appropriate procedures are put in place to counter and mitigate the risk.

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

http://bit.ly/2fQRcuH

Robert Putrus, CISM, CFE, CMC, PE, PMP
Is a principal with The Roberts Company LLC *(www.therobertsglobal.com)*. He has 25 years of experience in program management, compliance services, information systems and management of professional service organizations. Experienced in the deployment of various cyber security frameworks/standards, Putrus has written numerous articles and white papers in professional journals, some of which have been translated into several languages. He has been quoted in publications, articles, and books, including those used in master of business administration programs in the United States. He can be reach at robertputrus@therobertsglobal.com.

Types of Risk a Third Party May Have on an Enterprise

When a third party stores, accesses, transmits or performs business activities for and with an enterprise, it represents a probable risk for the enterprise. The degree of risk and the material effect are highly correlated with sensitivity and transaction volume.

> **"When a third party stores, accesses, transmits or performs business activities for and with an enterprise, it represents a probable risk for the enterprise."**

Enterprises are ultimately responsible for safekeeping, guarding and complying with regulation and law requirements of the sensitive information regardless of the contract stipulation, compensation, liability or mitigation stated in the signed contract with the third party.

Outsourcing certain activities to a third party poses potential risk to the enterprise. Some of those risk factors could have adverse impacts in the form of, but not limited to, strategic, reputational, financial, legal or information security issues. Other adverse impacts include service disruption and regulatory noncompliance.

The process approach in this article parallels the 2017 US Office of the Comptroller of the Currency (OCC) examination procedures that supplement OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."[3] The supplement outlines key processes to manage the risk of third-party relationships. Its processes could well be extended as best practices for industries beyond financial enterprises. Its processes are:

1. **Life cycle phase 1: Planning**—Management develops plans to manage relationships with third parties.
2. **Life cycle phase 2: Due diligence and third-party selection**—The enterprise conducts due diligence on all potential third parties before selecting and entering into contracts or relationships.
3. **Life cycle phase 3: Contract negotiation**—Management reviews or has legal counsel review contracts before execution.
4. **Life cycle phase 4: Ongoing monitoring**—Management periodically reviews third-party relationships.
5. **Life cycle phase 5: Termination and contingency planning**—Management has adequate contingency plans that address steps to be taken in the event of contract default or termination.

Oversight and Approach to Third-Party Data Security: The Development of the Risk Register

It is the intent of this article to introduce a credible, objective and supportive measurement illustrating the degree of compliance and oversight demanded from third parties in proportion to the degree of risk to which the enterprise is exposed.

Data security extends to the third-party relationships in the areas of, but not limited to,

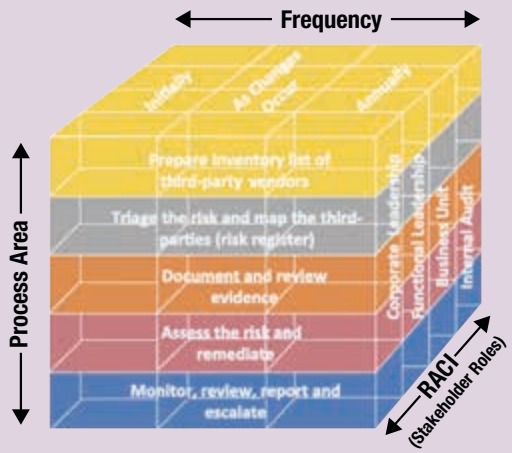
outsourcing IT services, applications, systems, infrastructure and transaction processing. The impact of third-party data security encompasses the enterprise's operations, supply chain, information technology and security, all levels of management (including the board of directors), and much more. Due to the impact that data security has on the enterprise, the representation of the stakeholders from different parts of the enterprise in the due diligence assessment and decision making is well justified and is left to the discretion of management as they deem appropriate.

The proposed systematic approach assumes that stakeholders are contributors to the efforts, reports, conclusion, recommendations and decisions related to third-party data security risk and compliance.

The foundation of the proposed assessment methodology is broken into three dimensions, as illustrated in **figure 1**:

1. **Process area**—This represents the degree of risk and compliance against which third parties are measured. It represents the development steps of the risk register, which is the critical and final outcome of the methodology presented in this article. The development and conclusion of the risk register is a successive approach represented by five tiers.
2. **Frequency**—This is the repeatable period or schedule of the examination/reporting required from the third parties by the enterprise receiving the services. The frequency is an integral part of the risk register since it relies on the third-party levels of risk and types of substantiated required evidence.
3. **Responsible, accountable, consulted, informed (RACI)**—This is the roles and responsibilities model for any activity that the stakeholders of the enterprise manage and oversee. The RACI cross-functional stakeholders could be drawn from various departments such as compliance, information technology, supply chain, legal and human resources. The basic elements of the RACI model are:
   - **Responsible**—The stakeholders who perform the work
   - **Accountable**—The stakeholders who are accountable for the work and decision making
   - **Consulted**—The stakeholders who must be consulted before decisions are made and/or tasks are concluded
   - **Informed**—The stakeholders who must be informed when a decision is made or work is completed

Figure 1—Risk-Based Model of Third-Party Data Security and Compliance



The Proposed Process Approach

The following are the recommended procedural steps of the risk-based management approach:

- **Prepare inventory list of third-party vendors**—One size does not fit all. When compiling the list of third parties and developing the criteria to assess the third parties' security risk to the enterprise, the list must be within the context of the industry, types of rendered services and the degree of impact of service dependencies on the enterprise. The enterprise's expectations of third-party data security compliance will vary and depend on:
  - The business relationship and what is rendered (products or services) by the third party—e.g., if the nature of the rendered services is transactional data, the Statements on Standards for Attestation Engagements (SSAE) 18 is effective for Service Organization Control (SOC) report opinions.
  - The criticality to the core processes of what is rendered to the enterprise—e.g., when the relationship between the enterprise and the third party is governed through information technology outsourcing (ITO) services.

– The data and cyber security impact that the third party has when there is a data exchange/transmission with the enterprise—e.g., what are the methods of secure transmission and types of encryption used to transfer data, such as confidential or proprietary information, over a secure channel?
– The type and nature of the data exchange (intellectual, product, financial, human resource, health, private) between the enterprise and the third party—e.g., the compliance of data exchange related to the patient health information is governed in the United States under the Health Insurance Portability and Accountability Act (HIPAA).

"Depending on the services rendered, the third party may exert multiple risk factors on the enterprise, which will increase the due diligence and compliance assurance required from the third party."

– The entity type of the third party (e.g., public, private, government)—e.g., if the entity is a US government agency, it will require compliance with the US Federal Information Security Management Act (FISMA). This act requires each federal agency to develop, document and implement an agencywide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source.

- **Triage the risk and map the third parties (risk register)**—When dealing with a third party, the enterprise must examine the types of risk that are posed. Depending on the services rendered, the third party may exert multiple risk factors on the enterprise, which will increase the due diligence and compliance assurance required from the third party.

The risk level must be assessed and recorded in the third-party risk register as critical risk, moderate risk or low risk. This is mostly a qualitative assessment, determined by the RACI team and guided by the risk categories, which include:

– **Strategic risk**—This is dependent on the uniqueness and the volume of the transactions that are offered by the third party. This is the risk that happens when the value to the enterprise is highly aligned with technology risk management. For example, large enterprises may rely heavily on a third party for technology support and processing critical information. Safeguarding informational assets will impact the enterprise's value and reputation.
– **Information management and security risk**—This is a combination of information technology services, information technology security and regulatory compliance risk. For example, a from-and-to transfer of information will pose a number of security challenges, such as data security during the transmission. Additional risk factors include confidentiality, user access, media location, physical security, device security and fourth-party risk, if any.
– **Resiliency risk**—This is related to the enterprise's mission-critical activities and how resilient the third party is to ensure information availability, disaster recovery, business continuity, incident management, recovery time objective (RTO), recovery point objective (RPO) and single point of failure (SPOF).

There could be regulatory compliance expectations or key controls in place that are exclusive to the third-party industry type, nature of rendered services or market capitalization. For example, the third party may require complying with the US Sarbanes-Oxley (SOX) Act, HIPAA, the US Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard

(PCI DSS), and the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)'s ISO/IEC 27001 or presenting attestation reports such as SOC 1 or SOC 2. These requirements must be taken into consideration when assessing the risk categorization of the third party. However, in the absence of regulatory compliance attestation reports, the enterprise must treat the third party differently. The enterprise may require an on-site assessment or send a questionnaire to be completed by the third party at a frequency that the enterprise deems appropriate.

In addition, the enterprise may establish red-flag rules when there are internal or external events taking place that impact the third party and the control environment and that impose significant risk. Some of these events could be merger and acquisition, divestiture, major organization changes, entering new markets, and geographic expansion. Such events will justify the enterprise to demand assurance in the form of a new security assessment or evidence that the key controls are in place and operating effectively.

- **Document and review evidence**—The enterprise will determine the appropriate documents required of the third party to produce and present. This is based on the entity's type and the nature of the business relationship.

For publicly traded companies, an enterprise located in the United States may request and examine reports related to SOX compliance, HIPAA, GLBA, PCI DDS, SOC 1, SOC 2 or ISO 27001. That may be sufficient as evidence that the third party has the key controls in place, and this must be asserted by the senior executives.

In Canada, there are broad laws that regulate security and privacy, such as the federal Personal Information Protection and Electronic Documents Act (PIPED) Act; Bill 198, referred to as Canadian SOX (C-SOX); the Health Information Protection Act; and regulatory standards set by PCI DSS.

In Mexico, there is the Law on the Protection of Personal Data Held by Private Parties. In Europe, there is the European Union Data Protection Directive. In Japan, there is a statute that covers internal controls for public companies. It is referred to as J-SOX.

However, the other category of third party, i.e., a third party that has no regularity compliance reports to provide, may require the enterprise to perform an audit, a walk-through or complete questionnaires as the needed evidence that key internal controls are in place and operating effectively. The frequency (six months, annual or biannual) of the data security assessment will depend on the risk category that the enterprise has determined. It is critical to have the types of reports and the frequency of examinations of the key controls stated when the contract is negotiated or renewed.

The type and frequency of data-security-related evidence or documentation for the third party to substantiate must be logged in the third-party risk register that the enterprise maintains.

"It is critical to have the types of reports and the frequency of examinations of the key controls stated when the contract is negotiated or renewed."

- **Assess and remediate the risk**—The objective of this step is to complete the development of the third-party risk register with a built-in scoring technique to assess and aggregate the risk for each individual third party. This register should use the risk category levels of critical risk, moderate risk or low risk, as described earlier.

The individual third parties will be classified and placed in the appropriate risk category with the approval of the enterprise RACI team. In the third-party risk register, the enterprise will specify the required document to be produced by the third party, the frequency and any remediation or additional controls that may mitigate the risk to an acceptable level.

- **Monitor, review, report and escalate**—Monitoring, reviewing and reporting third-party risk is an ongoing process. It should be performed on a regular basis and also be triggered if certain events take place, such as merger and acquisition, divestiture, major organization changes, entering new markets, and geographic expansion. The third-party risk register will provide guidance for the enterprise's required action and follow-up.

The RACI team represents the appropriate balance of the required governance for the enterprise's follow-up, escalation, accountability and decision making. This provides authenticity, legitimacy, objectivity, credibility and support to the third-party risk process.

Walk-Through Example

The following is a hypothetical example that is used to determine the constituted risk and to develop a third-party risk register using the approach proposed in this article and the following assumptions:

- Determining security risk measurement is the objective of the hypothetical example used. If the third party is unable to provide the regulatory compliance reports, it is recommended to use revised types of standards and/or an assessment questionnaire, such as the one presented in **figure 2**.
- Apply and roll out the process equally to all or selected third parties. As deemed appropriate, adopt the key controls from a published standard, such as US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, ISO 27001, the SANS 20 Critical Security Controls for Effective Cyber Defense, or develop a risk assessment. For the example illustrated in **figure 2**, the highest average score of risk (impact x presence) is 15. Risk is calculated based on the highest score of total risk (105) divided by 7, the number of assessment questions in **figure 2**.
- The number of third parties identified as being part of the evaluation is 80. This represents the number of entities that are sanctioned by the enterprise's RACI team to be regularly reviewed, evaluated, monitored and placed in the enterprise's third-party risk register.
- A scale of 1 to 5 is used to determine the impact and to amplify the significance of the stated controls seen fit. The scale is a subjective measure and is consistent with the definition of the risk categories and risk levels discussed earlier. The scale from 1 to 5 is determined and agreed to by the RACI team (**figure 2**).
- A scale of 0 to 3 is used to illustrate the presence of control, i.e., the degree of the operating effectiveness of the stated control at the third party (**figure 2**).
- An illustration of an aggregate risk for Third Party 1 is placed on the risk category scale. The aggregate risk of Third Party 1 is 7, which is the result of the calculation made in **figure 2**. It is left to the user of this methodology to determine the scaled range of critical risk, moderate risk and low risk (**figure 3**).
- All 80 identified third parties should be mapped according to **figure 2** and **figure 3**.
- The third-party risk register is used to classify where the third party is placed with respect to the risk categories and the expected documents to be produced and presented by the third party (**figure 4**).
- A summary of the total number of third parties and how many fall within the risk category (critical risk, moderate risk and low risk) is examined in **figure 5**.

Figure 2—Information Security Assessment Questionnaire: Key Controls

Information Security Assessment Questions	Impact (1–5)	Presence of Control 0=N/A,1= Yes, 2=Partially, 3=No	Risk (Impact x Presence) Subtotal
1. Governance of Information Security			8
1.1 Does the organization have written information security policies?	4	2	8
1.2 <list>			
2. General Security			4
2.1 Is antivirus software installed on every workstation?	4	1	4
2.2 <list>			
3. Network Security			5
3.1 Does the organization use demilitarized zone (DMZ) architecture for Internet systems?	5	1	5
3.2 <list>			
4. Systems Security			6
4.1 Does the organization implement encryption for confidential information?	3	2	6
4.2 <list>			
5. Resiliency: Business Continuity/Disaster Recovery			12
5.1 Does the organization implement redundancy or high availability for critical functions?	4	3	12
5.2 <list>			
6. Incident Response Plan			6
6.1 Does the organization have a written incident response plan?	2	3	6
6.2 <list>			
7. Auditing/Client Reporting			8
7.1 Will the organization provide relevant certificates of applicability, e.g., ISO 27001, SOC?	4	2	8
7.2 <list>			
TOTAL			49
Average Risk for Third Party 1 (Total/Total number of controls)=49/7			7.0

Figure 3—Aggregate Risk Category for Third Party

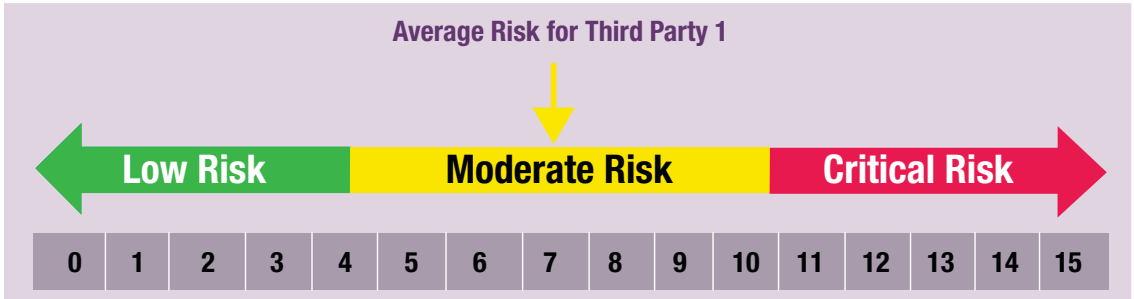


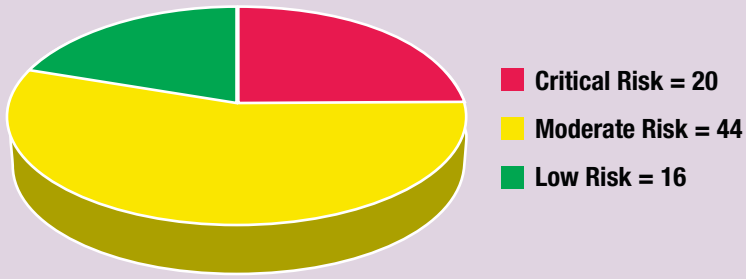
Figure 4—Third-Party Risk Register

Level of Risk	Control/Evidence Type	Frequency of Control	Internal Auditor	Business Unit	Functional Leaders	Corporate Leaders
Critical	SOC, PCI, HIPAA, SOX, external audit	Annual	R	A	C	I
Moderate	External/internal audit, self-assessment	Annual/as needed	R	A	C	I
Low	Self-assessment	As needed	R	A	C	I

RACI: R = Responsible A = Accountable C = Consulted I = Informed

Figure 5—Management Summary: Risk Examination of Third Parties

Total Number of Examined Third Parties	Third Parties Numbers of Risk Criteria	Third Parties Number of Risk Moderate	Third Parties Number of Risk Low
80	20	44	16



Advantages of the Outlined Process Approach

One of the challenges facing the enterprise in forming a team to manage third-party data security risk and compliance is the cost justification of such an investment. Using traditional accounting methods, such as discounted cash flow, to determine the return on investment (ROI) for cyber security initiatives may not be very suitable in this case.

A previous *ISACA® Journal* article, "A Nontraditional Approach to Justifying Cyber Security Investments," provides a platform for justification. It is based on the enterprise business model where objective, critical success factors (CSFs) and business challenges are all linked and supported by cyber security initiatives.[4]

Using a risk-based management approach to third-party data security risk and compliance can yield numerous benefits, including:

1. Establishing a single repository of third-party suppliers
2. Achieving the accountability and ownership needed to apply a consistent approach with all third parties and have expectations for supportive documents to substantiate risk management

3. Building trust by using the RACI model to ensure team cohesion on achieving desired outcomes. The credibility, accuracy and results of managing risk are highly dependent on more than one person participating in the areas of expertise that make up the RACI team and the cross-functional representations within the enterprise
4. Establishing risk-based segmentation of third parties based on categories established by identifying the third parties that are critical to the enterprise's well-being and identifying those that pose the highest risk
5. Developing and monitoring remediation and communication between the enterprise and third parties
6. Developing content for negotiating future contracts with other third parties
7. Providing timely communication and rapid response to changing regulatory requirements and third-party relationships
8. Improving compliance with federal, state, local and industry requirements
9. Streamlining efforts and maximizing staff productivity with a focus on high-priority third-party risk
10. Substantiating the enterprise's authenticity, objectivity and credibility by managing third-party risk

Conclusion

The trend of enterprises in various industries using third parties is on the rise. An Institute of Internal Auditors Research Foundation survey shows that 90 percent of respondents are using third-party technology. More than 65 percent of respondents rely in a significant manner on third parties.[5]

Consequentially, the risk exerted on enterprises parallels this trend. In the face of growing cyber security threats and compliance requirements, vast numbers of enterprises are seeking to determine the exposed risk and implement strategies to manage it.

This article presents a risk-based management approach to third-party data security risk and compliance through the development of a third-party risk register. It provides a systematic approach to evaluate and quantify the severity of and the exposure to risks presented by working with third-party vendors.

Once the level of risk is determined, the enterprise will be able to establish and dictate the type and frequency of support documents/reports required of third-party vendors so management can substantiate and assert compliance with laws, industry standards and best practices.

Endnotes

1 PricewaterhouseCoopers, *2013 Global State of Information Security Survey*, 2013
2 Soha Systems, *Third Party Access Is a Major Source of Data Breaches, Yet Not an IT Priority*, 2016, *http://go.soha.io/hubfs/Survey_Reports/Soha_Systems_Third_Party_Advisory_Group_2016_IT_Survey_Report.pdf*
3 Office of the Comptroller of the Currency, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2013-29, USA, 30 October 2013
4 Putrus, R. S.; "A Nontraditional Approach to Prioritizing and Justifying Cyber Security Investments," *ISACA® Journal*, vol. 2, 2016, p. 46–53, *www.isaca.org/Journal/archives/Pages/default.aspx*
5 The Institute of Internal Auditors Research Foundation, *Closing the Gaps in Third-Party Risk Management Defining a Larger Role for Internal Audit*, 2013, *http://cdn.cfo.com/content/uploads/2013/12/Crow_IAA_Study.pdf*

Making the SoA an Information Security Governance Tool

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

http://bit.ly/2wBsSUj

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)'s ISO/IEC 27001:2013 standard has defined the requirements for an information security management system (ISMS). An ISMS simultaneously encompasses IT security management and exceeds the strict boundaries of IT infrastructure and software. Indeed, an ISMS spans all of an organization's activities. It broadens the security view to all assets including physical assets (e.g., documents, premises, offices) and human assets (e.g., employees, contractors, suppliers).

Broadening one's view allows for the organization to see the true state of all assets. Both physical and human assets may host, reflect or transmit sensitive information that may pose strategic, reputational, regulatory or financial risk if lost, deformed, breached or leaked.

Daniel Gnana, CISA, ISO/IEC 27001:2013 LA, PRINCE2
Is the founder of ISO27K Audit Consulting. He has more than 20 years of experience in IT, including audit and security governance. He also provides training courses in audit, and he helps IT providers in their journey to obtain ISO/IEC 27001:2013 certification. He can be reached at danielgnana@gmail.com.

To guarantee the awareness of every information security aspect, an ISMS requires any organization to focus on 14 control objectives, which are listed in **figure 1**. The numbering in **figure 1** starts at 5 so that each control objective number aligns with the related ISO chapter.

Introducing the SoA

The ISO/IEC 27001:2013 standard reveals the Statement of Applicability (SoA) as a requirement related to information security risk treatment. It states, "Produce a statement of applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification of exclusions of controls."[1]

The explanation provided in the standard shows how an SoA tightly links risk assessment and risk treatment. That said, detailing such a link assumes that the organization has previously performed a risk assessment and is conscious of the current stakes, vulnerabilities and countermeasures available.

Since an SoA covers 14 themes, as previously mentioned, the risk assessment is indirectly assumed to include these themes. Once again, this applies to more than just the IT realm.

What is next? Surprisingly, the SoA is only mentioned once in the ISO/IEC 27001:2013 standard, which leads to a frequent misunderstanding that the SoA is a supplementary document in place only to comply with the standard and nothing more.

Is the SoA a trivial addition in the ISO/IEC 27001:2013 standard? Certainly not. If an organization has the desire to utilize the real benefits of the ISO/IEC 27001:2013 standard, which is to install information security governance, then it must utilize the SoA in its full capacity. The SoA is a tool that allows top management to see the comprehensive strengths,

Figure 1—Control Objectives for an ISMS

Control Objective	Set of Measures	Number of Measures
5: Information Security Policies	5.1 Management direction for information security	2
6: Organization of Information Security	6.1 Internal organization	5
	6.2 Mobile devices and teleworking	2
7: Security of Human Resources	7.1 Prior to employment	2
	7.2 During employment	3
	7.3 Termination and change of employment	1
8: Asset Management	8.1 Responsibility for assets	4
	8.2 Information classification	3
	8.3 Media handling	3
9: Access Control	9.1 Business requirements of access control	2
	9.2 User access managment	6
	9.3 User responsibility	1
	9.4 System and application access control	5
10: Cryptography	10.1 Cryptographic controls	2
11: Environmental and Physical Security	11.1 Secure areas	6
	11.2 Equipment	9
12: Operations Security	12.1 Operational procedures and responsibilities	4
	12.2 Protection from malware	1
	12.3 Backup	1
	12.4 Logging and monitoring	4
	12.5 Control of operational software	1
	12.6 Technical vulnerability management	2
	12.7 Information systems audit cosiderations	1
13: Communications Security	13.1 Network security management	3
	13.2 Information transfer	4
14: System Acquisition, Development and Maintenance	14.1 Security equipment of information systems	3
	14.2 Security in development and support processes	9
	14.3 Test data	1
15: Supplier Relationships	15.1 Information security in supplier relationships	3
	15.2 Supplier service deilvery management	2
16: Information Security Incident Management	16.1 Management of information security incidents and improvements	7
17: Information Security Aspects of Business Continuity Management	17.1 Information security continuity	3
	17.2 Redundancies	1
18: Compliance	18.1 Compliance with legal and contractual requirements	5
	18.2 Information security reviews	3
		114

* Highlighted measures affect more than IT

weaknesses and paths to mitigate the organization's information risk. Even further, this tool allows for follow-up enhancements to be carried out for information security.

Stated in other terms, the SoA must be considered a dual-role instrument rather than a simple document. First, it can be used as a health diagnostic tool for the organization to protect its information, and second, it pilots the general paths to improve organizational health.

"The SoA is a difficult exercise and requires the person conducting it to have enough seniority and authority to determine the person who best knows about the enterprise's security controls."

Decisions to Make Before Implementing the SoA

Prior to carrying out the SoA, there are some decisions the organization's top management have to make:

- **Confirm the organizational perimeter**—Ensure the ISMS perimeter is well defined and approved by the head of the organization as the target to be ISO/IEC 27001:2013 certified. Which businesses are concerned? Are there specific activities to focus on within those businesses, and if so, in which countries? Who are the stakeholders?

  As an example, suppose a company whose main business is to provide services related to a data center. In such a case, the main concerns reside in this perimeter, regardless of whether the company has other premises or not. Concretely, when scanning the SoA, restrict the physical security (theme 11) to the data center only.

- **Aim for a quick-win SoA**—Decide on a preliminary simple, but nonetheless reachable, version of the SoA in a short period of time, e.g., within a quarter. For each ISO requirement to mitigate the information security risk, strive to first get a quick insight of the actions currently carried out that fit such a requirement. Getting a quick insight for each of every 114 requirements calls for discernment between completeness and efficiency. An outdated and obsolete SoA may not reflect the current situation anymore and does not help decision making.

- **Identify the appropriate employee level at which to implement the SoA**—Decide on the employee profile that will be capable of rolling out each measure. This role should be able to investigate with enough authority; here are some considerations to keep in mind:
  - Regarding the previously defined perimeter, are these control objectives (**figure 1**) and set of measures applicable to the ISMS?
  - After investigation, can the information obtained be considered reliable?
  - As calculated, can the coverage rate of such a measure be considered acceptable for the organization, given the risk level?
  - If the coverage rate is low and it could take considerable effort to increase coverage, can the organization afford to remain at this point and accept the risk?

Avoid having a small SoA with no substance or with no reliable results. An ineffective SoA can happen after assigning someone whose lack of authority will lead to run constantly after the right answers. The SoA is a difficult exercise and requires the person conducting it to have enough seniority and authority to determine the person who best knows about the enterprise's security controls. Authority and seniority are also important to convince interviewed people to cooperate to help the person making the SoA determine the level of reliability and completeness of each answer.

Implementing the SoA

Once the preliminary steps mentioned previously are completed, there are three major steps to build a realistic and effective SoA:

1. **Filter and keep only the control objectives and the measures corresponding to the organization's scope**—First, regarding the organization's activities aspiring to comply with the ISO/IEC 27001:2013 standard, select each control

objective and every set of measures addressing the scope; consequently, disregard any objective and set of measures that fall out of scope, i.e., those that are nonapplicable to the organization.

For example, consider a subsidiary company in which supplier relationships are handled by the headquarters' human resources (HR) department. In such a case, objective 15, "supplier relationships," may be out of scope for that organization, making it inapplicable in the organizational context.

However, there are control objectives (CO) running as universal constants that are applicable to any organization:

- CO 5 (Information Security Policies)
- CO 6 (Organization of Information Security)
- CO 7 (Security of Human Resources)
- CO 8 (Asset Management)

A careful reading of the ISO/IEC 27001:2013 standard helps clarify that the previously mentioned control objectives are compulsory. Indeed, any organization targeting such a standard has to fix at least one high-level information security policy and one set of responsibilities to control its application throughout the organization. Any organization has to manage the assets and the stakeholders; therefore, it is necessary to identify them.

2. **With the help of the risk assessment results, shed light on the priorities relating to every set of measures**—To be able to determine the minimum responses that correlate to each set of measures of the SoA, it is worth analyzing the organization-level risk assessment and ranking the corresponding priorities (e.g., 1 = low risk, low priority; 2 = medium risk, medium priority; 3 = high risk, high priority) to weigh every measure.

   Avoid waiting until the perfect risk assessment is complete. Perfection is a lure and a hurdle against a successful quick scan of the SoA. Rather, develop a first version by considering which control objective the organization considers a major risk. Should the enterprise take up the exercise again, the second version can widen the scope of the risk assessment.

3. **For each measure deemed applicable to the organization, detail it to understand how far the measure is currently applied**—The following guidelines are elaborated on with examples drawn from a subsidiary company's SoA, theme 7, "human resource security," domain 7.1, "prior to employment," requirement 7.1.1., "screening of candidates' background." The purpose of these excerpts is to provide a concrete view of what actions are possible. Each applicable measure is broken down into five items as follows:

"Avoid waiting until the perfect risk assessment is complete."

   - Scope of responsibilities. In this subsidiary context, two types of responsibilities are considered:
     - The HR department is responsible for hiring personnel for fixed or long-term contracts; candidate background screening is the HR department's responsibility.
     - Any department, including HR, that is willing to hire subcontractors is responsible for verifying a candidate's background.
   - Declining the ISO/IEC 27001:2013 requirement in the organizational context given the scope; declining one or more items to come later:
     - **Requirement 1 (responsibility of HR department)**—Before hiring personnel, the following verifications are to be performed for considered candidates: identity control, criminal record, education, professional credentials and contact of former employers.
     - **Requirement 2 (responsibility of all departments)**—Before hiring subcontractors, the same verifications previously mentioned should be performed.
   - Examining how much the concerned organization is complying with previous requirements:
     - Compliance with requirement 1: 1 (Full compliance)
     - Compliance with requirement 2: 0, 2 The organization has handled the personal

verification of the subcontractors' suppliers; however, the reality and the completeness of such verification is never checked by the organization.

- Calculating a requirements coverage rate:
  - In the organization context, the coverage rate is 60 percent (∑compliances=1,2/∑Requirements=2).
- Decision improvements and deadline:
  - **Improvements**—First, the organization shall indicate to their suppliers which control objectives are required (e.g., identity, education; credentials; references). Second, the organization shall require their subcontractors' suppliers to provide their verification process documentation to ensure it complies with the control objectives previously mentioned. Third, the organization shall take periodic control of the supplier's verification evidence.
  - **Deadline**—First quarter of 2018.

Serving Information Security Governance

By its very detailed nature, the SoA, with its 114 measures covering 14 control objectives, cannot be reasonably delivered for governance meetings. However, the SoA becomes a goldmine for a synthesis of the weaknesses and paths to achieve control objectives. **Figures 2** and **3** help show the possibilities of synthesis of coverage rates and decisions. **Figure 2** provides an example of mapping the coverage rate with each measure for control objective 7, HR security.

Figure 2—Coverage Rate for HR Security

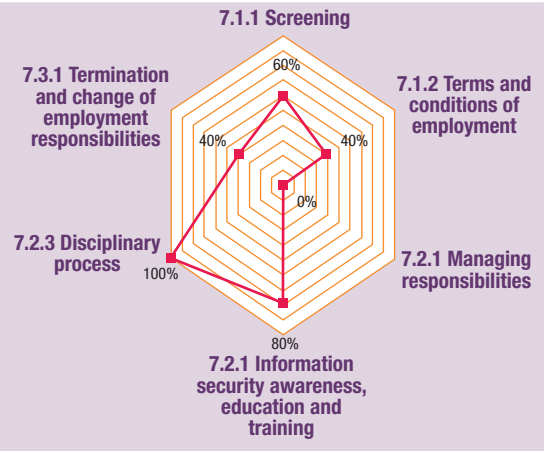


Figure 2 shows that when it comes to HR security, the sample organization has not yet provided an appropriate response to requirement 7.2.1 Managing Responsibilities, which most likely will

Figure 3—Organizational Decision-Making Response

Theme	Decision: No Additional Action	Decision: Additional Action	Total
5: Information Security Policies		1	1
6: Organization of Information Security		1	1
7: Security of Human Resources		2	2
8: Asset Management	1	3	4
9: Access Control	1	1	2
10: Cryptography		1	1
11: Environmental and Physical Security		4	4
12: Operations Seurity	1	6	7
13: Communications Security	1		1
14: Systems Acquisition, Development and Maintenance	1		1
15: Supplier Relationships	—	—	—
16: Information Security Incident Managment	1	3	4
17: Information Security Aspects of Business Continuity Management	1		1
18: Compliance		3	3
	7	**25**	**32**

be an obstacle to strengthen the other measures related to human resources.

By extension, such a synthesis can be applied to other control objectives and give an overview of risk areas concerning information and can consequently help determine risk mitigation strategy for the entire organization.

Figure 3 illustrates a specific area of concern: What is the next step after assessing a coverage rate as nonsatisfactory? In the example shown, there are 32 measures that are not covered enough, of which seven measures will not require additional action. These types of decisions are made considering the residual risk given the current action with regard to the ISO/IEC 27001:2013 measure recommended. Such a decision-making process cannot be undertaken in the dark; it requires the commitment of top management.

Conclusion

Since the SoA is compulsory, take advantage of it by gaining a quick insight of the controls coverage, not only in one's information system, but also in the weakest links of the security chain, such as some departments that care less about IT. Getting quick insight helps an enterprise set quick and efficient measures to mitigate major risk factors. All this insight helps achieve the ultimate objective of providing top management with a reasonable assurance of the continuing suitability, adequacy and effectiveness of their ISMS.

> **"However, the SoA becomes a goldmine for a synthesis of the weaknesses and paths to achieve control objectives."**

Endnotes

1 International Organization for Standardization, ISO 27001:2013, subclause 6.1.3, d), *https://www.iso.org/isoiec-27001-information-security.html*

Evasive Malware Tricks

How Malware Evades Detection by Sandboxes

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

http://bit.ly/2xY9V25

Sandboxes are widely used to detect malware. They provide a temporary, isolated and secure environment to observe if a suspicious file attempts anything malicious. Of course, criminals are well aware of sandboxes and have created a wide range of techniques to detect if there is a malicious file in a sandbox. If the malware detects a sandbox, it will not execute its true malicious behavior and, therefore, appears to be another benign file. If all goes well from the criminal's point of view, the sandbox then will release the file, deliver it to its intended user and the malware can launch the attack against the real user's environment.

It is a cat-and-mouse game where sandbox vendors add new techniques to detect malware, and criminals develop creative ways to evade detection and respond to the new detection techniques added to the sandbox.

Clemens Kolbitsch
Is leading the antimalware group at Lastline and works on various projects related to analysis and detection. As security researcher and lead developer of Anubis, he has gained profound expertise in analyzing current, malicious code found in the wild. He has observed various trends in the malware community and successfully published peer-reviewed research papers. In the past, he also investigated offensive technologies, presenting results at conferences such as BlackHat.

This article describes a representative sample of the techniques criminals use to evade detection, including the most recently developed methods.[1] This is not meant to be comprehensive, especially considering that new evasion techniques are continually being created. With every sandbox revision, criminals respond with a new evasion technique.

This article provides specific examples of three types of evasion techniques:

- **User behavior-based evasion**—Used to detect user actions that indicate the presence of a real user or inaction that indicates a sandbox. Examples of user behavior-based evasion include using Application.RecentFiles.Count and triggering macro code on close.
- **Virtual machine (VM)-based evasion**—Used to detect artifacts that are indicative of a VM-based sandbox. Examples of VM-based evasion include looking for Zone:Identifier and Windows Management Instrumentation (WMI) based evasions.
- **Timing-based evasion**—Used to evade sandboxes by delaying execution of malicious behavior or detecting sandbox timing artifacts. Examples of timing-based evasion include using delay application programming interfaces (APIs), sleep patching and time bombs.

User Behavior—Based Evasion Examples

Criminals deploy a range of techniques to detect user activity that, they assume, would not be present in a sandbox. Two of the most recent examples of this are using Application.RecentFiles.Count and triggering malicious code when a document is closed.

Use Application.RecentFiles.Count

A recent Dridex malware dropper (malware that is

designed to subsequently install additional malware) was distributed as a document file containing macros. As background, Dridex is known as Bugat and Cridex (a form of malware specializing in stealing bank credentials via a system that utilizes macros from Microsoft Word). The macros use Application.RecentFiles.Count to check how many files have been accessed recently. A low count suggests that there is not a person using the machine and, therefore, the machine is more likely to be a sandbox.

Trigger Macro Code on Close
Early sandboxes did little to emulate user activity beyond opening a file inside Microsoft Office. As a result, only code registered for the Document_Open event would be triggered within the sandbox. However, real users typically interact with a document much more. They scroll as they read, and once they are done, they close the document. This discrepancy between a real user's behavior and a sandbox can be observed, and malware now often triggers its code via the Document_Close event, meaning it will only execute the code once the document is closed.

VM-Based Evasion Examples

In addition to looking for user activity, criminals program their malware to detect when it is running in a virtual machine and, therefore, likely is a sandbox. As with user activity, there is a long list of techniques criminals use, the most recently detected examples of which are described here.

Look for Zone:Identifier
When a file is downloaded from the Internet onto a computer running Microsoft Windows, the operating system adds an alternate data stream (ADS) to the file to store Zone:Identifier metadata. This metadata includes information about the file, such as information about the URL from which the file was downloaded, and Windows uses it to show appropriate warning messages to the user before opening potentially untrusted content.

On the other hand, when a file is copied into a sandbox for analysis, this Zone:Identifier metadata is usually not present, as the sandbox cannot know where the file originated. Malware will check for this discrepancy. The presence of the Zone:Identifier ADS hints at a real user machine. If it is not found, the malware concludes that it is in a sandbox.

WMI-Based Evasions
The WMI interface allows Microsoft Windows machines and any service running on them to query information about running processes, available services, hardware (e.g., disk) information and more. Typically, system administrators use WMI to automate tasks.

> **"At the very least, sandboxes have to monitor the primary subject, i.e., the program that is to be executed, and the processes with which it interacts."**

At the very least, sandboxes have to monitor the primary subject, i.e., the program that is to be executed, and the processes with which it interacts. Interactions can be as simple as one program starting another or injecting new code into a target process. WMI is simply another type of inter-process communication (IPC), but it uses a more complicated client-server model. More precisely, it uses advanced local procedure calls (ALPC) to send queries to be executed in the context of system server processes.

If a sandbox is not able to intercept this type of communication, it will miss the activities performed by malware using WMI. Examples of malware using WMI to evade sandboxes include:

- **Checking cores count**—Due to resource constraints, sandboxes attribute the minimum required central processing unit (CPU) cores to a VM, typically just one, so they can run in parallel on as many VMs on a server as possible. However, most modern computers have multiple CPU cores. Malware will execute a WMI query to fetch the cores count, and if the value is one, it concludes that it is running inside a sandbox.

- **Checking disk space and physical memory**—Just like the case for CPU cores, VMs are typically allocated a limited amount of disk space and physical memory. To detect if it is running on a VM, malware checks if the total disk space of the drive is low, such as below 80 GB. Similarly, it checks to see if there is a small amount of physical memory, such as less than 1 GB of RAM. These configurations are not typically found on end user machines.

Without the ability to see this type of IPC, a sandbox is unable to intercept (and manipulate) the data returned by the server process. Thus, malware finds the limited hardware resources and detects the sandbox.

BIOS Info

Basic Input/Output System (BIOS) information for VMs and emulators is different from BIOS information for a real system, and it often contains strings indicative of VMs. Malware can create a list of strings found in BIOS information for VMs and can check if the current system BIOS information contains those strings. If so, malware can be fairly certain that it is running in a VM.

> **"Some sandboxes are programmed to simply wait and watch for a period of time, and if a file does not do anything malicious, it will release the file."**

Geolocation Blacklisting

The Internet offers various services that allow a user to request geolocation data based on the client's IP address. Maxmind is one such service, and malware can query this service to get information about the system on which it is running. One piece of available information is the company to which the IP is assigned. Malware compares this data to a list of known vendors, e.g., security companies. A match will indicate that it is executing inside a sandbox.

Check Username

Malware also fingerprints the sandbox using the name of the logged-in user. This trick works because some vendors do not randomize the Windows user under which the analysis is run. The malware simply checks the username against a list of well-known usernames attributed to sandboxes. For example, older versions of two well-known public sandboxes, Hybrid Analysis and Malwr.com, used to have fixed usernames, KR3T and PSPUBWS, respectively. This makes it easy for malware to detect these sandboxes based on the name of the current user.

Using Specific Instructions

Modern virtualization technologies support instructions that will unconditionally provoke a "VM Exit" into the hypervisor (a system that creates and runs VMs). This allows a VM to modify how the instruction triggering the VM Exit behaves, similar to an interrupt handler. However, this interrupt introduces a discrepancy in the execution time: When executed on a real machine, such instructions are faster than when they are executed inside the hypervisor managing VMs. Malware can use this discrepancy to detect the hypervisor, thereby tipping it off that it is running inside a VM. For example, it can measure the execution time of the CPUID instruction and compare it to the expected execution time of this instruction on a real machine.

Timing-Based Evasion Examples

A final category of evasion includes techniques that use a variety of timing mechanisms. Recently detected examples include using delay APIs, sleep patching and time bombs.

Using Delay APIs

Some sandboxes are programmed to simply wait and watch for a period of time, and if a file does not do anything malicious, it will release the file. To avoid this, malware uses the Sleep and NtDelayExecution APIs available in Windows. Malware calls these functions to sleep for a period of time to outwait the sandbox.

Sleep Patching

Sandboxes will patch the sleep function to try to outmaneuver malware that uses time delays. In response, malware will check to see if time was accelerated. Malware will get the timestamp, go to sleep and then again get the timestamp when it wakes up. The time difference between the timestamps should be the same duration as the amount of time the malware was programmed to sleep. If not, then the malware knows it is running in

an environment that is patching the sleep function, which would only happen in a sandbox.

Time Bombs
Another way that malware tries to outwit sandboxes is to include code that will only run on a specific date sometime in the future—criminals can be very patient—especially for targeted attacks. The goal is simply to outwait any timing delays introduced by a sandbox.

Recommended Techniques for Detecting Malware

To be effective, security technologies must be able to detect malware that uses these and many other techniques to avoid detection, including new evasion strategies that criminals continue to develop in response to ever-improving security systems.

The good news is that while evasive malware poses a challenge to traditional sandboxes, modern analysis sandboxes are built on a technique called full system emulation. The key difference between sandboxes based on virtual machines and those based on code emulators is that VMs typically do not fully virtualize the CPU used to run malware code. Instead, it passes most instructions through to the underlying hardware-supported hypervisor for execution.

A code emulator, on the other hand, directly handles each instruction executed within the analysis system and is thus able to tamper with the execution in any way the system wants to. This is done in a way that is completely transparent and invisible to the malware program under analysis.

For example, a full system emulator can tamper with the outcome of string comparison instructions (e.g., when used to compare the username of the system) and force execution down a path that reveals a program's true intent. Similarly, it can detect when a program is executing instructions that allow fingerprinting the hardware configuration and manipulate the effect of this code in a way to trigger additional behavior, helping it to correctly classify malware.

Even more, using full system emulation gives the sandbox complete visibility into the inner workings of programs running inside the analysis sandbox. That is, instead of only observing how a program interacts with the operating system (e.g., via system calls), a code emulator can also track data that are processed by the instructions making up the malware program. As a result, the sandbox can not only track what type of data are read from the operating system, but also how they are used, to what values they are compared (e.g., in code fingerprinting the system), to where the data are sent (when leaking confidential data) and much more.

Last, but not least, by having instruction-level visibility into the programs under analysis, a code emulator can also reason about code paths that the malware program did not execute in a particular analysis run. For example, the system can see what other potential behavior may be lurking in the malware that was not triggered during the dynamic analysis, giving the sandbox even more information for classifying a piece of malware.

"The good news is that while evasive malware poses a challenge to traditional sandboxes, modern analysis sandboxes are built on a technique called full system emulation."

Conclusion

Criminals are motivated, creative and persistent. For every sandbox enhancement used to detect evasive malware, criminals will develop a technique to avoid being detected and often use multiple techniques in combination to improve their success with detecting a sandbox. Security companies must offer, and their customers must implement, advanced malware detection technologies that are effective regardless of who has made the most recent move—the cat or the mouse.

Endnotes

1 Lastline, *An Introduction to Advanced Malware and How It Avoids Detection,* 2017, https://go.lastline.com/rs/373-AVL-445/images/Lastline_Intro_to_Advanced_%20Malware_WP.pdf

sponsored feature

Deloitte.

The AICPA's New Cyber Security Attestation Reporting Framework Will Benefit a Variety of Key Stakeholders

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

http://bit.ly/2wCOG3A

Sandra Herrygers
Is a partner at Deloitte & Touche LLP and is the global assurance leader.

Gaurav Kumar
Is a principal at Deloitte & Touche LLP, specializing in assurance and risk and controls transformation services.

Jeff Schaeffer
Is a managing director at Deloitte & Touche LLP, specializing in risk management, corporate governance, and compliance and controls transformation within the financial services industry.

As a relentless wave of cyberattacks continues, organizations are under intense pressure from key stakeholders and regulators to implement and enhance their cyber security programs to protect customers, employees and the valuable information in their possession. According to research from IBM Security and the Ponemon Institute, the average total cost per company, per event of a data breach is US $3.62 million.[1] Initial damage estimates of a single breach, while often staggering, may not take into account less obvious and often undetectable threats such as theft of intellectual property, espionage, destruction of data, attacks on core operations or attempts to disable critical infrastructure. These effects can last for years and have devastating financial, operational and brand ramifications.

Given the broad regulatory pressures to tighten cyber security controls and the visibility surrounding cyberrisk, a number of proposed regulations focused on improving cyber security risk management programs have been introduced in the United States over the past few years by various governing bodies. One of the more prominent is a recently issued regulation by the New York Department of Financial Services (NYDFS) that prescribes certain minimum cyber security standards for those entities regulated by the NYDFS. Based on the entity's risk assessment, the NYDFS law has specific requirements around data encryption, protection and retention, third-party information security, application security, incident response and breach notification, board reporting, and annual certifications.

However, organizations continue to struggle to report on the overall effectiveness of their cyber security risk management programs. The American Institute of Certified Public Accountants (AICPA) released a new cyber security risk management reporting framework[2] intended to help organizations expand cyberrisk reporting to a broad range of internal and external users, including the C-suite and the board of directors (BoD). The AICPA's new reporting framework is designed to address the need for greater stakeholder transparency by providing in-depth, easily consumable information about an organization's cyberrisk management program. The cyber security risk management examination uses an independent, objective reporting approach and employs broader and more flexible criteria. For example, it allows for the selection and utilization of any control framework considered suitable and available in establishing the entity's cyber security objectives and developing and maintaining controls within the entity's cyber security risk management program—whether it is the US National Institute of Standards and Technology (NIST)'s Cybersecurity Framework, the International Organization for Standardization (ISO)'s ISO 27001/2 and related frameworks, or internally developed frameworks based on a combination of sources. The examination is voluntary, and applies to all types of entities, but should be considered a leading practice that provides the C-suite, boards and other key stakeholders clear insight into an organization's cyber security program and identifies gaps or pitfalls that leave organizations vulnerable.

Who can benefit from a cyber security risk management examination report? Such a report can be vital in helping an organization's BoD establish appropriate oversight of a company's cyber security risk program and credibly communicate its effectiveness to stakeholders, including investors, analysts, customers, business partners and regulators (**figure 1**). By leveraging this information, boards can challenge management's assertions around the effectiveness of their cyberrisk management programs and drive more effective decision making. Active involvement and oversight from the BoD can help ensure that an organization is paying adequate attention to cyberrisk management. The board can help shape expectations for reporting on cyberthreats while also advocating for greater transparency and assurance around the effectiveness of the program.

Organizations that choose to utilize the AICPA's cyber security attestation reporting framework and perform an examination of their cyber security program may

be better positioned to gain competitive advantage and enhance their brand in the marketplace. For example, an outsource service provider (OSP) that is able to provide evidence that a well-developed and sound cyber security risk management program is in place in its organization can proactively provide the report to current and potential customers, evidencing that it has implemented appropriate controls to protect the sensitive IT assets and valuable data over which it maintains access. At the same time, current and potential customers of an OSP want the third parties with whom they engage to also place a high level of importance on cyber security. Requiring a cyber security examination report as part of the selection criteria would offer transparency into outsourcers' cyber security programs and could be a determining factor in the selection process.

Insurance carriers that write cyberinsurance policies could use information from customers' cyber security examination reports during the underwriting and risk assessment process to help them evaluate the company's risk posture and potential exposure by more effectively determining coverage needs. They could further use the information to enhance their competitive advantage by potentially offering benefits to customers that demonstrate an effective cyber security program. Conversely, customers and prospects could leverage their own cyber security examination reports to demand better pricing on cyberinsurance policies based on their preparedness in the event of a cyberattack.

The value of addressing cyber security concerns and questions by conducting a cyber security risk management examination before regulatory mandates are established or a crisis occurs is quite clear. Organizations can view the new cyber security attestation reporting framework as an opportunity to enhance their existing cyber security programs and gain competitive advantage. The attestation reporting framework addresses the needs of a variety of key stakeholder groups and, in turn, limits the communication and compliance burden. Organizations that view the cyber security reporting landscape as an opportunity can use it to lead, navigate and disrupt in today's rapidly evolving cyberrisk environment.

Figure 1—Using the New AICPA Cyber Security Reporting Framework to Lead, Navigate and Disrupt

Endnotes

1 Ponemon Institute, *2017 Cost of Data Breach Study,* IBM Security, June 2017, *www.ibm.com/security/data-baed/index.html*
2 American Institute of Certified Public Accountants, System and Organization Controls for Cybersecurity, USA, 2017, *www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx*

help source

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

http://bit.ly/2ySgksA

Q We are in the process of selecting a data loss prevention (DLP) tool. After discussing it with vendors, we realized that successful implementation of DLP depends on classifying data to identify key words that enable the DLP to recognize data to be protected. The challenge is we have a huge amount of data that are scattered all over. Therefore, we are still struggling with the right approach that will help us classify the data. How should we approach this problem?

A Data or information is a primary enabler for any organization, as established in COBIT® 5. Organizations today generate, process, use and store volumes of data/information. Many organizations face similar problems when classifying data/information. Although there is no panacea to this problem, it can be addressed based on the approaches used by various organizations.

ISACA's *Data Leak Prevention*[1] white paper identifies three key objectives for a DLP solution:

- Locate and catalog sensitive information stored throughout the enterprise. (Data classification)
- Monitor and control the movement of sensitive information across enterprise networks. (Network-level controls)
- Monitor and control the movement of sensitive information on end-user systems. (End-user controls)

The white paper provides guidelines for implementing DLP. These guidelines are:

- Data classification should be the first step of the program.
- Define and implement data classification and protection policies.
- Implement and configure DLP solutions per policy.
- Identify and monitor the risk associated with limitations of DLP solutions in protecting the organization's data.

The major objective of DLP is to prevent secret and confidential information from reaching unintended recipients. Organizations expect that DLP should be able to detect whenever such secret or confidential information is transmitted beyond the boundaries of the organization. An effective DLP implementation requires careful planning and cultural change, which are not possible without identifying and classifying the organization's data and information.

One more point also needs to be considered: implementing only DLP solutions may not provide the required level of assurance on the protection of data. It may have to be supplemented with implementing and integrating digital rights management (DRM) and access management solutions.

Other aspects to consider while implementing a DLP solution include:

- Generally, regulatory requirements mean data leaks can be catastrophic for organizations, and the possibility of liability and litigation are main drivers for organizations to consider DLP technologies.
- Many times, DLP is deployed by organizations with a focus on protecting intellectual property rights and trade secrets only.
- DLP and digital rights managements (DRM) implementation should be considered as an organizational program rather than as an IT initiative.
- Such programs may have multiple projects/phases and may require one to three years to fully implement depending on the size of the organization.
- DLP can protect data/information within the organization's perimeter, but cannot be extended beyond boundaries such as DRM.
- Data classification forms the foundation for DLP to be successful.
- DLP is not an adequate protection in cases where the organization uses cloud technologies.

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

At this point, the focus is on the first step: the classification of data.

Data classification best practices suggest the following steps:

1. Define a classification scheme in which the data/information within the organization is identified and classified in predefined buckets (e.g., top secret, confidential, sensitive, internal, public). Organizations may adopt a different scheme depending upon the nature of their data/information.
2. Identify the organization's data that are in soft form (digital or electronic) and hard form (physical documents). Also, note that there is a great deal of data/information in the heads of employees who deal with data while carrying out their responsibilities.
3. Define a data classification and protection policy that will apply across the organization. The policy should address the privacy policy and related compliance.
4. Determine the method to classify the data. The best approach for this is to use a risk management framework to help in determining the nature of the data.
5. Classify and label the data.
6. Implement controls for protection.

Organizations face major challenges while executing the fifth step, primarily due to:

- The volume of data generated, processed and stored
- Multiple data owners and coordination among them
- Cross-functional dependency and accesses required by such teams
- Classifying and labeling historical data

The following suggestions may be considered while executing the data classification process:

- Educate business process owners about data classification and the protection policy, including the privacy policy.
- Ask business process owners to identify data elements and the source of the data. This will help in identifying data owners/custodians. For example, employee data generated and owned by the human resources (HR) function, but used by other departments, must be classified by HR, and others must use that classification.
- Form small data sets that make meaningful information from data elements and classify them. For example, employee number, name, date of birth, address and date of hire can form a data set that is generally used by other functions such as payroll and physical security. Many independent data elements cannot be classified, with a few exceptions (e.g., credit card numbers).
- Identify the data sets (partial or complete) used in the report/document when classifying such information and determine the classification level of the report/information based on the classification of the data sets. Most information or reports generally contain multiple data sets. Generally, the highest level shall prevail. For example, employee personal information is confidential; therefore, the payslip of the employee is automatically classified as confidential.
- Determine and document exceptions.
- Maintain a function-focused and centralized data set inventory that validates the data's classification.
- Implement a process for periodic review.
- Implement an ongoing classification process.

Once the classification process is underway, further steps to optimize security may be considered. Labels used to classify data can be used as key words while implementing DLP solutions.

A last point to be noted is that though DLP solutions significantly improve an organization's ability to manage risk associated with data leaks, implementation of these solutions is complex and prone to errors and mistakes that may hamper achieving objectives. Careful planning and preparation, communication and training are essential for successful DLP programs.

Endnotes

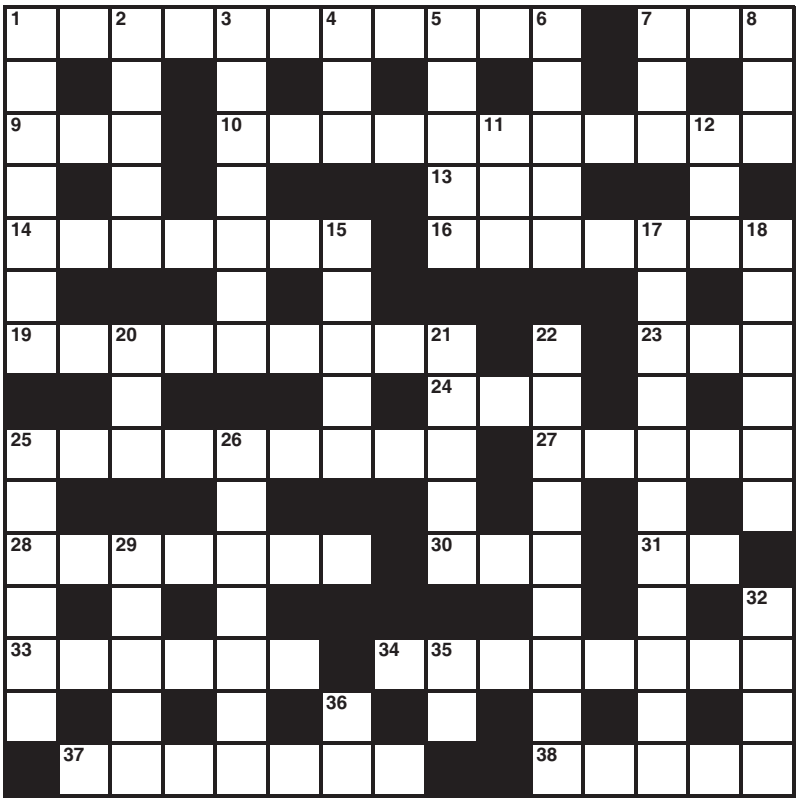
1 ISACA®, *Data Leak Prevention*, USA, 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Leak-Prevention.aspx*

crossword puzzle

by Myles Mellor
www.themecrosswords.com

ACROSS

1 Persuade others to practice good security principles, for example
7 1,000 megabytes
9 Security demands to validate access credentials
10 Aka for flash drives, 2 words
13 One in Spanish
14 Destructive intrusions, cyber ____
16 iPod attachments
19 Means to an end, not necessarily a moral or principled action
23 Keyboard key
24 Historical period
25 Software to combat malware
27 More accurate or loyal
28 Kind of challenge response test in computing that protects against bots
30 Regular payment for a service
31 Roman 6
33 Places on top of, 2 words
34 Global ransomware attack
37 Captures data illegally and then demands money in payment for it, for example
38 Firm and stable



DOWN

1 Confined to only certain people
2 Military offensive
3 Inveigled
4 Last word of the Golden Rule
5 Inspire with ideas and concepts
6 Computer message indicating something is not right
7 US National Security Agency (NSA) address ending
8 Position tracking device
11 Core activities and principles of a company
12 Completion
15 ____ phishing, email spoofing attack
17 Clearly defined and formulated
18 Immune to attack
20 Place
21 Trials
22 Stores of information
25 Important factor in audit of mobile devices
26 They are one dimensional computer arrays
29 Form of encrypting ransomware that attacks Windows-based systems
32 Abbreviation relating to a company policy where employees bring their own devices such as mobile phones to use at the workplace
35 Temperature control
36 Afternoon time

Answers on page 58

quiz#175

Based on Volume 4, 2017

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

TRUE OR FALSE

KHAN ARTICLE

1. There are less than 18 social media platforms globally that have started to grow and have an enterprise-level following.
2. Brand value and awareness can be created by engaging with customers on social media.
3. The four key areas of concern due to the growth in global privacy regulations are privacy, content ownership, intellectual property (IP) infringement and unauthorized activities.
4. A social media crisis and communication plan is unnecessary and any member of staff can deal with whatever crisis arises.

NGAMBEKET ARTICLE

5. In 2010, a software developer who worked remotely for a US firm outsourced his work to China. He could not be caught for many years.
6. It is forecasted that by 2020, 82.4 percent of the US workforce will be remote.
7. In recent years, many technology companies such as Google, Amazon and IBM have started to invest massively to offer cloud-based services to respond to businesses' expectations.
8. The biggest risk associated with a mobile workforce is loss or damage to assets such as laptops, tablets and customer data when they are in possession of remote employees.

WLOSINSKI ARTICLE

9. In 2016, 554,454,942 records were breached from 974 reported incidents.
10. Of the 554,454,942 breaches reported in 2016, 49 percent of the incidents were for personally identifiable information (PII), 28 percent were for credit and debit card data, and 23 percent were for physical health information (PHI).
11. Governance of privacy-related information requires that a custom strategy be developed for any organization and should include activities such as identifying the stakeholders and developing vision, mission and value statements with goals and objectives.
12. A privacy impact assessment (PIA) questionnaire should be used to inform the privacy officer of possible concerns and potential problems when a computer system is developed or changed.
13. The four types of privacy controls are encryption, access, confidentiality and prevention.

NICHO, KHAN, MOHAN ARTICLE

14. A key issue often cited by information systems (IS) executives in the last three decades is aligning IT with business.
15. Research indicates that alignment of IT with the business was the top IT management concern for four consecutive years since 2012.
16. IT is considered to be very important to the delivery of the overall business strategy and vision.
17. The value driver for financial IT includes maintaining the ratio of IT operational expenditure (OPEX) to the company's OPEX, adherence to the approved budget and ensuring IT cost recovery based on the approved budget.

CPE quiz

Prepared by
Kamal Khan
CISA, CISSP, CITP, MBCS

Take the quiz online

http://bit.ly/2fXWWGR

CPE quiz #175

THE ANSWER FORM

Based on Volume 4, 2017

TRUE OR FALSE

KHAN ARTICLE

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

NGAMBEKET ARTICLE

5. _____
6. _____
7. _____
8. _____

WLOSINSKI ARTICLE

9. _____
10. _____
11. _____
12. _____
13. _____

NICHO, KHAN, MOHAN ARTICLE

14. _____
15. _____
16. _____
17. _____

Name _____

PLEASE PRINT OR TYPE

_____

Address _____

_____

CISA, CRISC, CISM or CGEIT # _____

_____

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current *Journal* subscribers. An electronic version of the quiz is available at www.isaca.org/cpequiz; it is graded online and is available to all interested parties. If choosing to submit using this print copy, please email, fax or mail your answers for grading. Return your answers and contact information by email to info@isaca.org or by fax to +1.847.253.1755. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA. Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address. You will be responsible for submitting your credit hours at year-end for CPE credits. A passing score of 75 percent will earn one hour of CISA, CRISC, CISM or CGEIT CPE credit.

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

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

standards guidelines tools and techniques

ISACA Member and Certification Holder Compliance

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

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

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

ITAF™, 3rd Edition

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

IS Audit and Assurance Standards

The standards are divided into three categories:

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

Please note that the guidelines are effective 1 September 2014.

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

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

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

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

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

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

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

Reporting
2401 Reporting
2402 Follow-up Activities

IS Audit and Assurance Tools and Techniques

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

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

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

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

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

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

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

ISSN 1944-1967

Subscription Rates:

US:
one year (6 issues) $75.00

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

Remittance must be made in US funds.

advertisers/websites

leaders and supporters

ISACA®

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

NEW! Online Review Courses

Get the training you need. Prepare to obtain your CISA, CRISC or CISM certification and be recognized among the world's most-qualified information systems professionals. ISACA's Online Review Courses provide internet accessible, on-demand instruction and are ideal for preparing you and fellow audit, assurance, control, security and cyber security professionals for ISACA's certification exams.

Visit: www.isaca.org/examonlinereview to learn more.

CISA® CRISC™ CISM® CGEIT®

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

Featured Exam Prep Materials

CISA® Review Manual, 26th Edition

The *CISA® Review Manual, 26th Edition* 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 revised according to the 2016 CISA Job Practice and represents the most current, comprehensive, peer-reviewed IS audit, assurance, security and control resource available.

The 26th edition 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 Service Management; Protection of Information Assets.

The manual also serves as an effective desk reference for IS auditors.

Member: US $105.00
Non-member: US $135.00
Print Product Code: CRM26ED
eBook Product Code: EPUB_CRM26ED

BESTSELLING PRODUCT

CISA® Review Questions, Answers & Explanations Database—12-Month Subscription

The *CISA® Review Questions, Answers & Explanations Database* is a comprehensive 1,000-question pool of items that combines the questions from the *CISA® Review Questions, Answers & Explanations Manual, 11th Edition.* The database has been revised according to the recently updated 2016 CISA Job Practice.

The database is available via the web, allowing CISA Candidates to log in at home, at work or anywhere they have Internet connectivity. This database is MAC and Windows compatible.

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CISA candidates to identify their strengths and weaknesses and focus their study efforts accordingly.

Member: US $185.00
Non-member: US $225.00
Product Code: XMXCA15-12M

The *CISA® Review Questions, Answers & Explanations Database* is also available on CD-Rom in Spanish.

CISA® Review Questions, Answers & Explanations Manual, 11th Edition

Designed to familiarize candidates with the question types and topics featured in the CISA exam, the *CISA® Review Questions, Answers & Explanations Manual, 11th Edition* consists of 1,000 multiple-choice study questions that have previously appeared in the *CISA® Review Questions, Answers & Explanations Manual 2015* and the *CISA® Review Questions, Answers & Explanations Manual 2015 Supplement.* The manual has been updated according to the newly revised 2016 Job Practice.

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

- *CISA® Review Manual, 26th Edition*
- *CISA® Review Questions, Answers & Explanations Database – 12 Month Subscription*

Member: US $120.00
Non-member: US $156.00
Product Code: QAE11ED

Available in: Chinese Simplified, Italian, Japanese, and Spanish

CRISC™ Review Manual, 6th Edition

The *CRISC™ Review Manual, 6th Edition* is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The manual has been enhanced over the past editions and represents the most current, comprehensive, peer-reviewed IT-related business risk management resource available worldwide.

The 6th edition manual is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- IT Risk Identification
- IT Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting

Member: US $85.00
Non-member: US $115.00
Print Product Code: CRR6ED
eBook Product Code: EPUB_CRR6ED

Order online at ***www.isaca.org/bookstore***

CRISC™ Review Questions, Answers & Explanations Manual, 4th Edition

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

The 500 questions in this manual have been consolidated from the *CRISC™ Review Questions, Answers & Explanations Manual 2015* and the *CRISC™ Review Questions, Answers & Explanations Manual 2015 Supplement.*

Many questions have been revised or completely rewritten to be more representative of the CRISC exam question format, and/or to provide further clarity or explanation of the correct answer. These questions are not actual exam items, but are intended to provide CRISC candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam.

Member: US $72.00
Non-member: US $96.00
Product Code: CRQ4ED

Available in Spanish
Product Code: CRQ4EDS

CRISC™ Review Questions, Answers & Explanations Database—12-Month Subscription

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

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CRISC candidates to identify their strengths and weaknesses and focus their study efforts accordingly.

Member: US $185.00
Non-member: US $225.00
Product Code: XMXCR14-12M

NEW!

CISM® Review Manual, 15th Edition

The *CISM® Review Manual, 15th Edition* is designed to helpyou prepare for the CISM® exam. This comprehensive, easy-to-navigate manual is organized into chapters that correspond to the four job practice areas covered in the CISM exam. The Manual is primarily designed as a tool for exam prep, but can also be useful as a reference manual for information security managers.

New to the 15th Edition:

- **In Practice Questions** help you explore the concepts in the CISM Review Manual in your own practice.
- **Knowledge Checks** are designed to help reinforce important concepts from the Review Manual to further enhance your learning.
- **Case Studies** provide real-world scenarios to help you gain a practical perspective on the Review Manual content and how it relates to the CISM's practice.
- **Comprehensive Index** has been updated to make navigating the Review Manual easier and more intuitive.

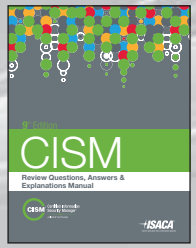
Member: US $105.00
Non-member: US $135.00
Print Product Code: CM15ED
eBook Product Code: EPUB_CM15ED

NEW!

CISM® Review Questions, Answers & Explanations Manual, 9th Edition

The CISM®Review Questions, Answers & Explanations Manual, 9th Editionconsists of 1,000 multiple-choice study questions, answers and explanations, which are organized according to the CISM job practice domains.

The questions, answers and explanations are intended to introduce the CISM candidate to the types of questions that appear on the CISM exam. This publication is ideal to use in conjunction with the *CISM Review Manual 15th Edition.*



Member: US $120.00
Non-member: US $156.00
Product Code: CQA9ED

NEW!

CISM® Review Questions, Answers & Explanations Database—12-Month Subscription

The *CISM® Review Questions, Answers & Explanations Database* is a comprehensive 1,000-question pool of items that contains the questions from the *CISM® Review Questions, Answers & Explanations Manual 9th Edition.*

The database is available via the web, allowing our CISM candidates to log in at home, at work or anywhere they have Internet connectivity. The database is MAC and Windows compatible.

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CISM candidates to identify their strengths and weaknesses and focus their study efforts accordingly.

Member: US $185.00
Non-member: US $225.00
Product Code: XMXCM15-12M

CGEIT® Review Manual, 7th Edition

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

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

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

Member: US $85.00
Non-member: US $115.00
Print Product Code: CGM7ED
eBook Product Code: EPUB_CGM7ED

CGEIT® Review Questions, Answers & Explanations Manual, 4th Edition

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

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

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

- *CGEIT® Review Manual, 7th Edition*

Member: US $60.00
Non-member: US $75.00
Product Code: CGQ4ED

Order online at ***www.isaca.org/bookstore***

Train Your Employees. Prep for Enterprise Success.

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

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

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

ISACA®

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

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

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

Audit Life-Cycle and Risk Management Solution

available on AppExchange

works with Google Drive

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

Built by Auditors, For Auditors.

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

www.rcap.online

TRONIXSS