Featured articles:

Big Data—Not a Panacea
Big Data Analytics for Sophisticated Attack Detection
Data Privacy and Big Data—Compliance Issues and Considerations
And more...
110,000 strong
200 chapters
180 countries
45 years

Thank you for helping us achieve 45 years of excellence!

Learn more at www.isaca.org
Let TeamMate
Bring Focus to Your View of Controls

The unique combination of adjustable Dimensions and Perspectives provided by TeamMate CM gives you the power to view key control information in a way that is most relevant to you.
Columns

3
Information Security Matters: Cyberrecovery Preparation
Steven J. Ross, CISA, CISSP, MBACP

6
The Network
Rosemary M. Amato, CISA, CMA, CPA, CSSGB

9
Cloud Computing: Securing an Evolving Cloud Environment
Matthew Neely

12
Information Ethics: ISACA’s Corporate Social Responsibility
Vasant Raval, DBA, CISA, ACMA

16
IS Audit Basics: The Logical Reason for Consideration of IT
Tommie Singleton, CISA, CEGIT, CPA

Features

19
Big Data—Not a Panacea
Muzamil Riffat

22
Big Data Analytics for Sophisticated Attack Detection
Nikes Virvilius, CISA, CISSP, GPEN, Oscar Serrano, CISA, CISM, CRISP, and Luc Diandurand

27
Data Privacy and Big Data—Compliance Issues and Considerations
William Emmanuuel Yu, Ph.D., CISM, CRISC, CISSP, CISP, CSSLP

32
Selecting the Right Cloud Operating Model
Thomas Schaefer, CISA, CISM, CISSP, OEH, Michael Hofmann, CISA, CISM, CRISC, CEGIT, CCISO, OPM, Peter Loos, Ph.D., and Peter Fettke, Ph.D.

39
Electronic Documents Information Security Compliance
Haris Hamidovic, Ph.D., CIA, ISMS IA, and Amra Hamidovic

42
Writing Good Risk Statements
Benjamin Power, CISA, CPA

45
Audit-focused Mining—New Views on Integrating Process Mining and Internal Control
Martin Schuetz, CISA, CIA, Alexander Ruehle, CISA, CIA, and Nick GehMe, Ph.D., CISA

51
Internal Audit’s Contribution to the Effectiveness of Information Security (Part 2)
Paul John Steinbart, Robyn Raschke, Graham Gal and William N. Dilla, Ph.D., CPA

Plus

56
Crossword Puzzle
Myles Mellor

57
CPE Quiz #154
Based on Volume 1, 2014—Data Privacy Prepared by Kamal Khan, CISA, CISSP, CITP, MBACS

59
Standards, Guidelines, Tools and Techniques
S1-S4
ISACA Bookstore Supplement

Journal Online

Want more of the practical, peer-reviewed articles you have come to expect from the Journal? Additional online-only articles will be available on the first business day of each month in which no Journal is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA® members during their first year of release. Use your unique member login credentials to access them at www.isaca.org/journalonline.

Online Features

The following articles will be available to ISACA members online on 2 June 2014.

Data Privacy—Protecting This Asset Is a Priority
Horace McPherson, CISA, CISM, CEGIT, CRISC, CISSP, PMP

Sabiduria Empresarial Informática. Parte de la Respuesta a la Contraposición de Intereses Entre Ti y el Negocio
Jenly J. Cano, Ph.D., CFE

Similarities Between Banking Regulations of Turkey Made by BRSAs and COBIT 5 Governance Area
Fatih Altinel, CISA, and Yeliz Kilinc

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

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

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

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.
Cyberrecovery Preparation

In many of the articles I have written in recent years for this column, I have addressed the subject of cyberattacks—planned, intentional, malicious attempts to steal, modify or destroy information from a targeted organization. There is no shortage of well-publicized cases and they appear in the media regularly. The issue is no longer whether cyberattacks occur, but what to do about them. The majority of the literature that I have seen deals with preventing such attacks from being successful. Some concern detecting an attack when it does occur. Nothing that I am aware of deals with building the capability to recover from cyberattacks.

There is a fair amount written on how to clean up after an attacker—a government, a terrorist or a criminal—has penetrated an organization’s systems. The steps include detection; isolation of affected devices and network segments; recognition of what has been stolen, altered or destroyed; identification and removal of malware; recovery of lost data; and implementation of new security measures and resumption of processing.

I humbly propose a framework for preparing for recovery from a cyberattack before one occurs. This is not disaster recovery as we have known it in IT operations. The damage is logical, not physical. And the solution involves more than relocation to an alternate data center.

ACCEPTANCE

Elisabeth Kubler-Ross (no relation) famously stated that there are five stages of grief, beginning with denial and finishing with acceptance. I would like to suggest that in preparing to recover from cyberattacks, most organizations are still in denial and must move to acceptance before they can even begin to finance and build the mechanisms of cyberrecoverability. People should realize that there are bad people in the world trying to do bad things to good systems. The protectors’ information resources need to be effective 100 percent of the time; the bad guys need to get through only once. Unfortunately, cyberattacks are as relevant a threat to systems as frauds, floods or fires.

Still, you should not give way to despair. The adage, “When there is nothing to be done, it is best to do nothing” does not apply. First of all, there are things to be done and, second, the mere effort to do something about cyberpreparation, to coin a term, is valuable if only to help identify vulnerabilities in your information systems.

TRUSTED IMAGES

Cyberrecovery starts with having trusted images of software and data to fall back on. (Assuming that all organizations make regular backups of their data and know how to restore them, I will restrict this discussion to recovering affected software.) Since malware latches onto software and perverts it, it is necessary to have a copy of what every executable looked like before an attack to know what it was then and to eliminate malicious changes. It is also necessary to keep copies of all authorized changes to software to distinguish them from the unauthorized ones.

AIR-GAP DATA CENTER

Recovery from a cyberattack requires a data center at a remote facility that is to be used for a variety of related purposes. These include storing the trusted images, testing the integrity of those images, identifying software and data that may have been attacked, determining the point prior to an attack where software and data may be trusted, and validating the integrity (or lack thereof) of software and data after an attack. This is not the same as the alternate data center that is the basis for recovery from a physical disaster. At the most basic level, it is an air-gap facility, totally disconnected from the primary one (figure 1).

The air-gap means not only that this data center must be remote, but that there are no telecommunications capabilities either. Some of this is paranoia, a handy attribute for security professionals. Trusted images need to be stored in the air-gap data center. If you trust the Internet, you could use a virtual private network (VPN) to get them from your production site to the air-gap data center. I do not trust the Internet. In which

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the Journal’s most popular columns since 1998. He can be reached at stross@riskmastersinc.com.
case, you could have a private, point-to-point circuit. I think those can be tapped. You could encrypt the line. I think some very sophisticated bad guys, especially those who are government-sponsored, know how to crack encryption algorithms. (Is it paranoia when someone really is trying to attack you?) In the absence of any technology for secure transmission of the trusted images, I advocate that they should be physically transported on magnetic tape or hard drives.

STORAGE
The air-gap data center must have sufficient storage to hold the executable versions of all of an organization’s software. The storage vehicle may be either portable disk or tape, so there is a need for devices to read the media and transfer them to a disk array. It is necessary to keep the trusted images for a very long time, because persistent malware can stay dormant for months or more.

I would expect that trusted images would be delivered to the air-gap data center on at least a daily basis, not because software changes that often, but because a cyberattack is at its essence a failure of change management. You need a daily image to determine whether an unauthorized change had occurred that day. If no known change has occurred, yesterday’s trusted image should be identical to today’s. If it is not, something untoward occurred, potentially an attack.
SERVERS AND SOFTWARE

If there was a known change, it is possible to validate that the changes made were only the authorized ones. By treating software as data, hash-totaling software can be used to check for correctness and security of data in a trusted image. Thus, the air-gap data center requires a number of servers on which to run the validating software. How many servers? The answer depends on how you will validate your software and how much software you will validate at a time. Note that the same servers will be used to validate all your software when an attack occurs, so the numbers of servers to install in the air-gap data center may be greater than the number you will need prior to an attack. In this case, virtualization will be useful to reduce the physical hardware footprint. Remember, this is not an alternate data center; there is no need to duplicate all the devices used in production.

Literally, as I was typing this, I received notification that the US National Institute for Standards and Technology (NIST) has issued its Framework for Improving Critical Infrastructure Cybersecurity (of which ISACA® participated in development and in which ISACA's COBIT® 5 is included as an informative reference). Notably, it proposes five functions that must be concurrent and continuous: identify, protect, detect, respond and recover [emphasis added]. To my knowledge, this is the first time that there has been anything approaching a standard that calls for recoverability in the struggle against cyberthreats. I believe that trusted images and an air-gap data center are necessary to meet NIST’s essential requirements for cyberrecovery, though not in themselves sufficient. I advocate that a comprehensive architecture is needed to effectively mitigate these threats, a topic to which I will return in another article.

ENDNOTES

1 Kubler-Ross, Elisabeth; On Death and Dying, Scribners, USA, 1969
2 Attributed to Lord Melbourne, the UK Prime Minister and mentor to the very young Queen Victoria
3 If it were inside the organization’s production data center, people who have access there might also enter the one dedicated to cyberrecovery. Sadly, several instances of system penetration seem to have started with a rogue insider, so the two must be physically separate.
4 This, in turn, depends on the staffing and procedures for performing the validation, a topic I will return to in a future column.
5 I realize it is not a standard, but a framework. Since it comes from NIST, it takes on the aura of a standard and that is enough for me—and I hope many others—to see it that way.
Rosemary M. Amato is a director for Deloitte based in Amsterdam, The Netherlands. She is the program director for the Global Client Intelligence program and leads a team of professionals located around the world with the responsibility for providing timely, complete and accurate quantitative global client information to those who require it to serve clients with distinction. She has been with Deloitte for almost 17 years and, prior to her current role, led the Global Enterprise Risk Services (ERS) Knowledge Management team. She currently sits on ISACA’s Knowledge Board and cochairs ISACA’s Knowledge Management and Education Committee.

Opinions expressed in this interview are her own and do not represent opinions of Deloitte.

Do you have something to say about this article?
Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Q: How do you think the role of the information systems (IS) auditor is changing or has changed?
A: The role of the IS auditor has definitely changed and I believe it will continue to change. That is just the normal evolution in the workplace. If we do not change, we become stale—outside forces are demanding that we change to keep up with what is happening in the businesses we audit. However, there is one area in which we are not reacting to change enough. We must get involved with regulatory discussions as they are happening and provide input. I believe, in the past, IS auditors would just wait until laws were put into existence, then change audit programs to accommodate the new requirements. As IS auditors, we need to be advocates to make sure the public understands the impact of a new law and not just allow things to be forced upon us. We need to be trusted business advisors both within our business community and the outside world of regulation. I am sure many IS auditors are getting involved in this area, but I do think there is room for improvement.

Q: What do you see as the biggest risk factors being addressed by governance, risk management, security or audit professionals? How can organizations protect themselves?
A: This is a difficult question to answer as risk is so encompassing. It is changing every minute, every hour, every day, and it is so different depending on what country you are in, what industry you are in, and so forth. Right now, everything dealing with the cloud is a big area of focus. But, do we really understand what it means when data are in the cloud? Organizations can protect themselves by doing their research, getting facts, analyzing data and making sure that before they step in to do something, they understand the risk factors and have a risk framework in place to mitigate risk as soon as it is identified. Continued vigilance and awareness are key. You do not know what you do not know, but you can work at trying to know it earlier rather than later.

Q: How do you believe the certifications you have attained have advanced or enhanced your career? What certifications do you look for when hiring new members of your team?
A: Getting my Certified Information Systems Auditor® (CISA®) certification was definitely a boost to my career, as was achieving the Certified Management Accountant (CMA) certification. Certifications build a professional’s self-confidence and they show the outside world that you have gone that extra step to demonstrate that you are a professional in the area in which you specialize.

Certification helps define a professional. When I interview candidates for my team, I look for certifications in the areas in which they are going to be working. If they say they are a professional, they should be certified in something and be active in the organization that offers the certification.

Q: What will be the biggest compliance challenge in 2014? How should it be faced?
A: Compliance challenges in 2014 will continue to inundate the profession. I think the biggest compliance challenge will be to just understand all the regulations—old, new and those yet to be written into law. We will need to be advocates to make sure regulations are put into law only when they have an objective that can be clearly met and executed, and, more important, are able to be assessed properly for their effectiveness.
ON MY DESK RIGHT NOW
I’m never at my desk. Working virtually, I can be anywhere, but there is always a cup of coffee or tea nearby.

WHAT ARE YOUR THREE GOALS FOR 2014?
1. Taking better care of my physical well-being
2. Taking better care of my mental well-being
3. Remembering that life has so much to offer and not let it pass you by, but grab it for all it is worth

WHAT’S YOUR NUMBER ONE PIECE OF ADVICE FOR OTHER GOVERNANCE, RISK AND COMPLIANCE PROFESSIONALS?
Continue to learn and learn and learn. You will always have opportunities if you never stop learning.

WHAT’S YOUR FAVORITE BENEFIT OF YOUR ISACA MEMBERSHIP?
Participating on the Knowledge Board and cochairing the Knowledge Management and Education Committee—I can give back while gaining so much knowledge.

WHAT DO YOU DO WHEN YOU’RE NOT AT WORK?
Read, travel, read, snow ski (when not injured), read, cook, just enjoy life, and read. (See a pattern there?)
2014
GOVERNANCE, RISK, AND
CONTROL CONFERENCE

an IIA & ISACA Collaboration

Where Governance and Risk Management Align for Impact

August 18–20, 2014 | Palm Beach, Florida, USA

Join in an IIA and ISACA event that delivers the tools you need to stay ahead of the challenges impacting global Governance, Risk, and Control. Earn up to 18 CPEs!

Save US $200 when you register by June 6!
Attendance is limited, so don’t delay.
Register today at www.theiia.org/goto/GRC2014
Matthew Neely is the director of strategic initiatives at SecureState (www.securestate.com). Neely uses his technical knowledge to lead the Research & Innovation team to develop threat intelligence tools and methodologies for the challenging problems of the information security industry. Previously, he served as SecureState’s vice president of consulting and manager of the Attack & Defense Team. With more than 10 years of experience in the area of penetration testing and incident response, Neely brings the ability to think like an attacker to every engagement. He uses this skill to find creative ways to bypass controls and gain access to sensitive information. Prior to working at SecureState, Neely worked in the security department at a top-10 bank where he focused on penetration testing, assessing new technology and incident response.

The chief information officer (CIO) of a large utility provider had decided to move email, file shares, video sharing and the company’s internal web site to the cloud and needed to know the security requirements for this project within two weeks. The organization already had security requirements in place for traditional third-party vendors; however, these requirements were not a good fit for the cloud services the company was looking to adopt.

The director of security at the utility provider approached SecureState, a management consulting firm specializing in information security, with the problem.

Unlike traditional third-party solutions where the vendor is responsible for all, or most, of the security controls in the cloud, there are often cases where the client is responsible for managing and maintaining key security controls. For example, if a company was hosting a home-grown application at a Platform as a Service (PaaS) provider, the client would generally be responsible for the security of the application itself (figure 1). The cloud provider of the PaaS would be responsible for securing the platform and infrastructure supporting the application. However, if a company selected a Software as a Service (SaaS) application, the cloud provider would generally be responsible for all layers of the stack and the client would have very little responsibility or control over the security of the application (figure 2).

With that in mind when moving to the cloud, it is critical to clearly outline who is responsible for each component and have requirements that give the organization its desired level of security while being flexible enough to fit the different service models available from cloud providers.
For this utility provider, the move of these initial four services was part of a larger effort to eventually migrate all corporate IT services to the cloud, so in addition to quickly developing requirements for the applications listed previously, the director of security also needed a way to rapidly assess and categorize future cloud service providers to determine what minimum set of controls should be applied. This system also needed to be flexible enough to support new technology developments as cloud solutions mature. Further, a system would need to be put in place to track and monitor compliance of these key business partners to the required controls.

BUILDING A FRAMEWORK

To assist with this, SecureState created a program to review, approve and manage these cloud providers. The program was built around a custom cloud security framework (CSF) that the team developed. This framework was comprised of numerous components including:

- Data classification and cloud service provider categorization guidelines
- A control set
- Vendor questionnaires mapped back to the control set
- Federated identity management standards

To create this framework, the team met with stakeholders to gather business, technical and security requirements. The framework leveraged the utility company’s existing security policies, procedures and standards while adding requirements specific to cloud computing environments.

The controls in the framework were broken down by the classification of the data processed and/or stored by the provider (public, internal, confidential and regulatory). Each level added another layer of controls that needed to be present in the environment. To ensure that the controls were properly applied to various cloud models and use cases, a lookup table was created to show who is commonly responsible for managing each of the controls in the framework, depending on what type of cloud service model (e.g., SaaS, IaaS, PaaS) is being used.

Special attention was given to the regulatory requirements related to the data that would be stored and processed by the cloud providers, as the utility company needed to comply with several different regulations:

- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards because the utility provides power generation and transmission
- Payment Card Industry Data Security Standard (PCI DSS) because the utility processes credit cards
- US Health Insurance Portability and Accountability Act (HIPAA) because the utility self-insures its employees for health benefits

Requiring all cloud service providers to meet these regulatory requirements would be onerous, if not impossible. Therefore, appropriate regulatory controls would be applied only in environments that required them.

For example, portions of the utility’s employee health insurance process would migrate to the cloud specifically related to the corporate file share. Because of this, additional steps needed to be taken to ensure that the provider of the file-sharing service could meet the related HIPAA requirements.

Once the framework was completed, the team met with executives at the organization to review the CSF. During this meeting, SecureState conveyed the importance of the framework to the business and outlined how the organization should align to it. Once executive management buy-in was obtained, the framework was adopted for use by all lines of business moving services to the cloud, not just IT. This provided the company with a unified approach to managing the security of cloud services, thus ensuring all corporate data moved to the cloud were appropriately secured.

MANAGING THE SECURITY OF CLOUD SERVICES

The director of security also needed to develop processes to prioritize, review and track which cloud services were approved for use, as well as a program to manage and track what data were being stored and/or processed by these cloud services. Without a robust program in place, the security department would quickly lose control of where sensitive data were stored and which vendor had been approved or denied.

The SecureState team created an online portal where lines of business inside the utility can enter requests to have potential cloud service providers (CSPs) reviewed. Once a provider is entered for review, a questionnaire is generated based on the type of cloud service used and the data stored and/or processed by that provider. This questionnaire is then sent to the point of contact at the cloud service provider to gather information on what security controls are present in their environment. Once the questionnaire is complete, SecureState works with the CSP and client to snap the cloud service into the CSF. To ensure the lines of responsibility are clearly defined, each requirement in the CSF is assigned to either the CSP or client. Depending on the categorization of the data being stored or processed by the provider, additional testing or interviews outside of the questionnaire may be required to determine which controls are present and to verify that they are properly implemented.
A similar process is also followed to ensure that the controls the organization is responsible for implementing internally are present and properly implemented for each new cloud service entering into the environment.

During this review process, risk posed by the proposed solution is enumerated and areas where the solution did not meet the CSF are outlined. Using this information, the utility’s security group can determine if the new solution poses an acceptable level of risk, if the solution would be rejected or if it requires additional controls.

This portal also provides an inventory of which approved cloud applications/providers are currently being used in the environment and any exceptions associated with each provider. Additional reminders are set up to reassess each CSP annually, at a minimum. The depth of the reassessment is determined by the type of data processed or stored by the provider and any control exceptions granted.

LESSONS LEARNED

Since implementing the CSF, the utility has applied it to four initial cloud services and a handful of subsequent providers. While applying the framework, a number of lessons were learned:

1. Getting in front of the providers before the contract is signed to gain the full support of the providers. The utility had a large challenge applying the CSF to the initial set of vendors, as the contracts with these vendors had already been signed by the time security was brought in to review them. Because of this, the team had little leverage to get the vendors to make changes to their environments to meet the utility’s security requirements.

2. Ensuring the use and completion of the utility’s questionnaire. Many of the providers preferred to provide third-party audit reports such as Service Organization Control 2 (SOC2) reports or self-assessments such as the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) instead of completing the utility company’s questionnaire. In these cases, the team would map the results back to the framework manually. Unfortunately, in most cases the information provided in the SOC2 report or CAIQ did not contain enough detail and further interviews and assessments were required to fill in the gaps. These processes ended up taking longer than initially planned. As a result, it was determined that this process would go more smoothly if the questionnaire was completed first. Thus, the team focused on streamlining the questionnaire and warned the project team that if the vendor did not complete it, the time required to review the vendor would lengthen, possibly impacting the project timeline. With this concern in mind, often the line of business could pressure the prospective providers to complete the questionnaire.

3. Prioritizing provider assessments based on services provided. Follow-up interviews and assessments took longer than initially planned, and a method to prioritize service providers had to be developed to ensure high-priority service providers were assessed first. In some cases, lower-priority providers that housed only public data received minimal follow-up interviews and assessments. This was done to ensure that providers could be reviewed and approved quickly with the resources available.

4. Educating the line of business on the cloud provider review process and following that process. Large projects that went through the company’s central procurement, or project management, office were easily flagged for provider review. However, many smaller projects that were initiated by the lines of business were small enough that they did not require involvement from these groups. Therefore, the security team did not hear about some smaller projects until they were fully implemented and, in some cases, had been in operation for a few months. To address this, the security department now makes a concerted effort to reach out to all lines of business to educate them on the process while working to quickly review new providers so this review is not a bottleneck in the process.

CONCLUSION

By pulling together the right team, the utility was able not only to address its initial problem of providing security requirements for the first group of vendors, but also to develop a solution to manage future cloud vendors. This solution allowed the utility to quickly and easily review future providers and also provide a program to manage them, thus ensuring corporate information stored in-house or in the cloud is protected equally.

The best way to start this process in any organization is to inventory the existing cloud services already in use. Many organizations have already started to leverage cloud services, often without audit, IT or security’s knowledge. By generating an inventory of which service providers are currently being used and what data are being stored or processed there, the organization can get a handle on what corporate data may be underprotected in these environments and use this information as leverage to start its own internal project to create a CSF for the environment.
ISACA’s Corporate Social Responsibility

While an organization’s code of ethics is often seen as inwardly driving an entity to its duty, a corporate social responsibility (CSR) program works as the predominant, if not the sole, instrument of an organization’s intentions to contributing to greater good. Often contextless and worded for a long tenure, the code of ethics is more like a constitution: The fewer the revisions, the better the document. In contrast, a CSR program is an action-oriented plan; it addresses content in terms of goals and programs, albeit still presumably anchored on the code of ethics of the institution.

On 2 January 2014, ISACA® announced its formal corporate social responsibility (CSR) program.1 We often hear about CSR plans and achievements of large corporations. In contrast, CSR programs of professional bodies, as a collective of its membership, are less publicized—or at least less frequently noticed or studied. Nevertheless, CSR efforts of professional bodies offer a huge potential for unique contributions to communities; indeed, the fact that many professional bodies are actively involved in CSR and ISACA’s entry following some informal experiments in the past is certainly noteworthy.

Conceptually, an entity’s code of ethics should be mirrored in its CSR program. Although perhaps feasible, it is difficult to imagine having a CSR program without an enunciation of one’s code of ethics. How could an entity define its duties without clarifying the moral ground on which it stands? The code combined with the articulation of identity and core values of an organization make the CSR program genuine. How could a profession serve communities without knowing what it stands for? Or, what is it good at? Every professional association is different in its true identity. The Australian Academy of Ophthalmology can help prevent blindness by building awareness of the care of eyesight, while the American Physical Therapy Association (APTA) can transform societies by optimizing body movement to improve the human experience.2 After all, an institution’s talents and strengths are uniquely leveraged to carve out its social responsibility agenda; a generic do-good template does not help either the institution or the society it serves.

ASSOCIATIONS AS SEPARATE ENTITIES

A profession is a reasonably well-defined occupation that meets a defensible set of criteria for being a profession.3 It is not necessary for a profession to have a professional body or association “either because sufficient identity and coherence is provided through employment, or because (particularly in rapidly evolving areas) formal organization has few benefits.”4 The presence of an association, where one exists, could provide a common platform that may articulate shared values, virtues of the profession, common interests and how they are protected, the practice of advocacy, and the community service. Broadly, a professional body can give greater identity and provide a channel for the profession to reach out to the community. The synergies of individual members are hard to leverage if the bond provided by their association is weak or missing.

While every association essentially represents its members, the variety and complexity in the mosaic of professional bodies is substantial. Certain professional organizations are gatekeepers, very specific in membership requirements, qualifications, licensing and practice of the profession. A narrow definition of a professional body is that it is a self-regulating occupational group capable of legally prohibiting others from practicing. Physicians and lawyers belong to such a body. On the other hand, a broader definition of a professional body—applicable to institutions such as ISACA—would emphasize elements like qualification; group identity; special, uncommon knowledge; and knowledge used in the service of others. Certification and licensing can still be important, but right to professional practice may not be exclusive to its membership.5

Whereas a professional body is essentially a collective of its members, it is important to distinguish the institution from its members.

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 interests include information security and corporate governance. Opinions expressed in this column are his own and not those of Creighton University. He can be reached at vraval@creighton.edu.
A force in and of itself, an institution sets standards and develops a vision for the group and, thus, should exercise leadership responsibilities. It has more resources than any individual member could dedicate to the profession's overarching goals. It also has a greater reach, more powerful voice and political clout; its voice as a collective cannot be easily ignored by influential leaders, including lawmakers. Thus, the institution sets itself apart from its membership at an even higher threshold of ethical conduct, moral duty and social responsibility.

Professional bodies often are empowered to represent the unique knowledge and insights of the collective. For example, it seems certain that the American Institute of Certified Public Accountants (AICPA) has grounds to provide input to proposed revisions to the US tax code. The American Medical Association most likely would put forth its positions on issues like obesity. And ISACA certainly could offer a considered opinion on what can be done to address concerns expressed in the open letter by chief executive officers (CEOs) of technology companies to President Obama regarding the National Security Agency's practices, for example. After all, professional expertise should be deeply engaged in what a profession can do for communities. Abstaining from providing insights of the profession toward solving societal problems would border on the compromise of the collective's moral duty.

A professional institution can make an impact on society by deploying two related approaches. First, it can mold members' behavior and motivate their actions toward the common good; second, by its own actions as a representative body, it can harness and drive common energy and professional competencies. As related to CSR, each is worth further examination.

PROMOTING MEMBERS' BEHAVIOR
A first essential responsibility of the institution is to help its members focus on promoting member behavior conducive to duties of a member. Such demands from its membership should be holistic in nature and yet enforceable, and should be regarded as the minimum—and perhaps only the minimum—that a member would likely deliver. A modest beginning in setting the tone of service to the community lies in having a relevant, well-crafted and understandable code of ethics. To keep moral duty at the front and center of the profession, it is also critical for the profession to make continuing education in ethics a requirement. Most institutions specifically direct members to obtain certain hours of continuing education periodically in the area of ethics. This institutional action sends a message that ethics is not a tangential outcome, but rather a central characteristic of the profession. The power of such a leadership initiative that guides its members lies in the multiplier effect it creates: It reaches every member of the institution, emboldens the group and extends the horizons of the profession's impact.

DUTY AS A COLLECTIVE
Duty at an individual member level can be lifted into higher, institution-level social responsibility goals. An extension of the ethical tone at the top is in the CSR of the professional body, suggesting its duty to the society in achieving greater good. Toward this end, competencies of a profession can be harnessed, coordinated and steered to address many societal problems faced today. For example, identity theft has become a chronic societal problem. The Identity Theft Resource Center (ITRC) reports that, as of this writing, 79 incidents of identity theft had occurred in 2014, causing the potential compromise of more than 1.4 million records. In comparison, total breaches in 2013 were 619, impacting nearly 58 million records. As an association known for risk management, ISACA and its chapters around the world could help prevent identity theft through community education locally in the chapter regions. This puts the competency of the profession to work for the benefit of the society as a whole.

Professional bodies primarily focus inwardly, in serving and supporting members to excel in their competencies at work. This is, of course, extremely important for the profession; its identity, reputation and value lie in the success of its members. Once this goal is on a stable path, it is time for the institution to look outward. It is simply a matter of recognizing that one level of goals has been attained and the time is right to reach for higher-level goals. For example, the American Physical Therapy Association proposed in 2013 a new vision statement to its membership:

Most significant about the new vision is its outward perspective. This reflects physical therapy's maturation from an inward-facing profession that aspired to the elements outlined in Vision 2020—autonomous practice, direct access, doctor of physical therapy, evidence-based practice, practitioner of choice, and professionalism. Now that the profession has largely achieved these aspirations, it can envision the impact that physical therapy can and must have on individuals, communities, and populations.
CSR is just one of many ways in which an institution can become outward looking. Every institution may aspire to positively impact individuals, communities and populations. However, the critical alignment to this laudable goal must come from the comparative advantage the institution possesses between itself and its collective membership. Thus, value to the society can be uniquely enhanced based on the overlap of what the community needs and what the institution and its members can provide. For an optimal CSR program, the institution should strive to harness its code of ethics, values and competencies into a meaningful array of unique contributions to people everywhere in its physical and virtual domain.

Finally, it should be noted that to execute an institutional CSR program, the human capital of the kind that only professional members can offer will be needed. Outsourcing of competencies that mirror the profession may not be considered a core-level CSR action item, although such items may help achieve part of the agenda. Therefore, while we begin by differentiating between the institution and its membership, we end with one striking conclusion: the CSR of the institution rests on the values and motivation of its membership. The more glued the members are to the institutional CSR program, the more effective the outcomes, and the larger the membership force, the greater the potential good.

**ISACA’S CSR PROGRAM**

As announced early this year, ISACA is formally launching an experimental CSR program. Contributions anticipated from this program will take four forms:

- ISACA will donate funds to one or more international organizations selected by the working group; organizations selected must meet the criteria established by the volunteer group overseeing the CSR program. Two organizations have been identified for 2014, the first of which is Enactus. The remaining organization will be announced once contact has been made and the details surrounding the donation have been finalized.
- Chapters, volunteers, members and staff can apply for funding from ISACA to be donated to local/regional organizations meeting specific criteria. The volunteer group will review all submissions and determine whether funding will be granted.
- ISACA will donate funds to relief agencies in areas significantly impacted by natural or man-made disasters. (ISACA has been doing this for several years; the CSR program formalizes the process.)
- ISACA staff will be provided a limited number of paid hours off per year to participate in approved volunteer activities.

As is often said, “the truth is in the details.” Consequently, the merits of the ISACA CSR can only be assessed after more information is available. It seems fair to say that this program focuses on infusion of resources, or is input-based. The articulation of outcomes—their relevance and quality, for example—may not be controllable by any single donor contributing to a pool of funds generated from several philanthropies. This is offset by the fact that benchmarks used to select the donee organization provide an assurance of desirability and achievement of outcomes. Effective ways to follow the money all the way to the end goal can take multiple paths.

Donating funds to relief agencies is certainly a worthy gesture. Here, the intention appears to follow a two-fold converging path: Resources will be supplied by ISACA, while actions “on the ground” will come from volunteers, including ISACA members. In this modest beginning, the intention seems to be to provide relief. As the program matures, ISACA may want to consider motivating its chapters to mobilize its resources and energies toward preventive, detective or even corrective measures to the problem. If the anticipated disaster, or its impact, can be mitigated by contingency planning, for example, it may make sense for ISACA and its members to get involved in helping with disaster recovery planning and attendant training of populations that the disaster, if materialized, would strike.

In November 2013, the Philippines was hit by Super Typhoon Haiyan. The damage in human life and physical assets represents a national calamity of epic proportions. Looking forward, perhaps proactive efforts are needed to develop a typhoon or other disaster plan and appropriate responses to help cut down on the massive costs of such events. With the Manila Chapter of ISACA surpassing 900 members on its roster, would it not be comforting to have the chapter membership take charge of people’s awareness and education of typhoon-related happenings and related recovery responses? This is not to say that the chapter members did not
help in the disaster relief (many of them may have been deeply involved in the disaster recovery), but rather to envision a concerted effort under the umbrella of an organization that is capable of driving such programs.

The final item merely refers to one type of resource, ISACA staff providing social services on compensated time. The nature and types of services that may be approved remain to be disclosed. In any case, could this consideration be extended to ISACA members? Would it be appropriate, for example, to provide credit toward experience requirements for certification if a member provides profession-related services voluntarily and without compensation?

COMMON THREADS OF PROFESSIONAL CSR PROGRAMS

First, the institution should mold member behavior toward duty to society. The glue that naturally binds an individual member to professional duties can be in the code of ethics of the institution. If it is not emphasized enough, chances are the membership will have its own interpretations and outcomes will vary across members. Second, we need to distinguish between competencies deployed at the employer organization through the delivery model and the same competencies engaged in community service through the realization model. The delivery model hinges upon specific accountability in a specific project. The realization model “involves the professional working with the client or stakeholders in a more collaborative way to produce outcomes that are owned by the latter. While it will still involve the use of expertise, it is closer in principle to the work of a counselor or facilitator.”

What you need to put in at your place of employment is often clear and well defined; it is your job that is at stake. Duty to society is almost invariably voluntary and unsupervised; you may think of doing it but find enough priorities to push it way down the list of things to do. Even when you finally get to the act itself, the situation may demand more than your tool kit. Putting the same skill set to work in communities often can be a challenge; it is not just the knowledge or experience that counts. A member’s willingness to do good should be accompanied by his/her leadership traits.

For ISACA, an in-depth look at the realization model would help carve out a potentially fruitful CSR program. Such a model would provide a platform to build the program. To support the program, a balanced scorecard combined with relevant features of the COBIT® framework would help. Early stages of the program would also require a discussion of a number of programs that are likely good examples of CSR efforts as customized to the vision of ISACA and its members. And, of course, frequent feedback from those involved in the actual mission should help streamline and refine the program going forward. ISACA expects the program to grow and flourish during and following this pilot program. Indeed, as is often said, a journey of a thousand miles begins with a first small step; ISACA has put in motion a worthy goal.

ISACA, much like other associations, will face many challenges in executing an effective CSR program. Political, social, legal and economic issues invariably crop up in programs like this; appropriate response to such issues will become necessary. Much work in CSR is likely to be collaborative in nature; it takes more than just resources or skills to carry out the actual mission. An enrichment of a profession-centric vision into a society-centric vision, while laudable, will require considerable courage and persistence on the part of ISACA’s leaders. Certainly, we are not there yet, but the beginning of a journey with great potential is good news.

ENDNOTES

2 American Physical Therapy Association (APTA), www.apta.org/Vision/
5 Ibid.
6 Identity Theft Resource Center (ITRC), www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html
8 Op cit, ISACA
9 Op cit, Lester, p. 5
The need for consideration of IT in internal and external audits seems intuitively obvious. This is emphasized by the fact that the vast majority of individuals are immersed in IT—from smart phones to complex TV/media systems to work technologies. Yet there are still gaps from time to time where entities or individuals have not completely thought through the reasons why IT needs to be continually evaluated by senior management, and examined by internal and external auditors.

**Pervasiveness of IT**

Most, if not all, would agree that IT has become prevalent, including among accounting and finance functions and in financial reporting. Some of the effects and needs related to this pervasiveness include:

- 24/7 requirement of IT
- Need to detect errors early
- More automated controls, fewer manual controls
- Complexity—integration of multiple technologies
- Electronic work flow
- Paperless transactions (e.g., electronic data interchange [EDI])
- Networks that extend beyond the entity

The complexity issue is a particularly acute one. Complexity needs to be broken down and understood by auditors to effectively perform the larger realm of audit (e.g., the financial audit for Certified Public Accountants [CPAs]). But, the very nature of complex IT makes that process difficult; thus, the need for lifelong learning and constant continuing education by IS auditors.

Another acute issue is the increase in electronic work flow and paperless systems. If customers at a gas station pump their own gas and say “no” to the receipt option, how does an auditor audit that class of transaction? Aside from an IS auditor using IT tools (e.g., computer-assisted audit tools [CAATs]), it would require someone to print the data for examination and there would still be an inherent lack of confidence in the data.

To compound the other issues, entities have welcomed their vendors via supply chain tools, and increased the risk associated with both systems and financial data.

The point being made is not just the pervasiveness of IT, an obvious conclusion, but the associated increase in IT-related risk to the business and to audits. Thus, there is a need for IS auditors and their knowledge, skills and abilities to assess risk, address risk and develop adequate mitigating controls for risk.

**Criticality of IT**

IT is often critical to a business or entity. Easy examples include eBay.com and Amazon.com, but traditional brick-and-mortar companies are also sometimes extremely dependent on IT. Walmart and the airline industry are two obvious examples. There is a very long list of entities that find IT critical to their products or services.

Thus, for those entities, it is important to understand IT and how it relates to the business processes to gain an adequate understanding of the entity. That would be a particularly important for a CPA doing a first-year audit, for example.

IT can affect any of the following, and other things not on this list, regarding an entity:

- Business model
- Goals, objectives and plans
- Competitiveness
- Business risk
- Transaction flows
- Data flows
- The whole business process stream
- Transaction reporting
- Accounting and financial reporting risk

For example, in applying COBIT® to an organization, most, if not all, items on the previous list would be considered. That said, many of them would not be simple to evaluate and/or understand adequately without a great deal of effort and possibly some research or serious assessment of IT.

And, because of its criticality, IT likely increases a variety of business risk factors associated with these items.
Change Control

Change control is something that should be evaluated on every financial audit, and many internal audits. The scope of change control varies within different organizations based on facts such as custom programming (including middleware) and complexity of the organization's IT.

Some common deficiencies include:

- Lack of control over access to coding
- Lack of control over changes to programs
- Ineffective decisions in replacing or upgrading IT

The last issue is one that is common to all organizations regardless of size. In fact, smaller entities are probably more likely to forego formal processes of change management and even sometimes make changes based on poor decision making simply because a smaller entity is less likely to have a wealth of IT knowledge.

Application Development (AppDev)

Generally speaking, AppDev is part of change management, but it is a special case. Some applications make significant calculations automatically within the application. If the application is custom developed in-house, this is particularly risky and dangerous.

For instance, it is fairly common for cost of goods sold (COGS) to be calculated by the application as part of the posting of a sales transaction. If COGS is a material account, and it usually is, the entity should be careful to make sure it has an effectual level of assurance over that calculation.

There is one example where a utility wrote its own code and had a simple mistake in an if-then-else statement. For fewer than 1,000 units the rate was US $x.xx/unit. For 1,000-5,000 units, the rate was a flat US $yy.yy plus US $z.zz/unit in that range. The variable, having been set to zero before the if-then-else, was left at zero for those fewer than 1,000 units (note that no customer complained). This led to a US $37 million understatement of revenues.

Entities should take extra care with material automated calculations.

Logical Access Controls

Logical access control is another area that should be evaluated on every financial audit and many internal audits. The previous
discussion alluded to pervasiveness and expansion of IT and the
nature of systems causing the need for effective logical access
controls to become paramount.

Some common deficiencies include:
• Weak access controls over financial applications
• Failure to take advantage of effective SoD using least
  privileges in access controls
• Elevated privileges that do not return to normal
• Terminated users whose credentials remain active

Thus, access controls represent a fairly robust area of risk.
Because of the complexity of systems and networks, and the
expansive nature of those systems, there is usually a need for an
IS auditor to evaluate access controls in most organizations.

Third-party Providers
More and more organizations are specializing in services that
entities are outsourcing to them. Add to that the proliferation
of cloud services, which are third-party providers as well, and
there is an increase in the number of business processes or
functions that are being outsourced.

This adds risk to the business process stream as a whole.
How does the entity have reasonable assurance that adequate
controls are in place at the third-party provider? Would those
controls be better if the process was internal? The point, once
again, is the increase in risk and the presence of IT.

Business Continuity Planning and Disaster Recovery Planning
With regard to business continuity planning (BCP) and
disaster recovery planning (DRP), risk has increased over
the disaster aspect. With cloud computing and the increased
complexity of systems, there is greater probability of a
system failure that can affect computer operations. Thus,
risk involves both incurring such a failure and being able to
properly restore computer operations.

The bottom line for the discussion thus far is that there are
many aspects of IT that represent an inherent risk (IR) with a
relatively high assessment. That IR is generally independent of
traditional risk factors, such as those associated with the risk
of material misstatement.

IMPLICATIONS OF IT: “THE FORCE BE WITH YOU”
There is a bright side to the IT invasion. IT is a two-edged
sword: It is able to inflict wounds on the entity, but able to
defend the entity as well.

The following is a short list of some of the beneficial
uses of IT:
• The potential to identify efficiencies in audit procedures
• The potential to rely on effective automated controls
• The potential to leverage CAATs to perform IT-substantive
  procedures over more expensive manual procedures
• The power of data analytics in effective decision making
  and management
• The ability to identify beneficial feedback to management
  (e.g., value-added management comments)

As part of my dissertation, “The History of EDP (IT)
Auditing,” I interviewed about 45 pioneers of the IS audit
profession. Without exception, they believed the event
with the largest impact was the
advent of CAATs. Not only can
IS auditors analyze financial
data, but they can also analyze
nonfinancial data. IS auditors
can draw inferences about the
operational effectiveness of
controls, or even the presence of
controls, by examining the right
kind of data. Usually, IT-substantive tests are less expensive
overall than manual substantive tests.

The last point on the list is important because most, if not
all, organizations have something broken in the IT space that
needs to be fixed.

CONCLUSION
Admittedly, there are a number of challenges related to IT.
Much of this article focused on the increase in risk associated
with IT in the current-day environment. Those challenges are
elevated by rapid changes in IT, including the complexity of
IT, for both new/emerging systems and existing systems. One
key point is the presence of IR related to IT that needs to be
identified, assessed and mitigated.

However, there is good news. First, the adequately
prepared IS auditor can be a huge asset to any organization
by being able to assess and mitigate risk. Second, that same
IS auditor can also leverage IT to provide efficiencies and
effectiveness to the organization, e.g., the use of data analytics
in a business entity or the use of a CAAT in an audit. Last, the
environment is not likely to change for the foreseeable future;
therefore, there will be a need, whether acknowledged or not,
for IS auditors for a long time to come.

ENDNOTES
1 Singleton, Tommie; “The History of EDP Auditing,”
dissertation, University of Mississippi, 1995
The buzz and commotion surrounding big data and related topics simply cannot be ignored. The term “big data” refers to a deluge of information that is generated every second through myriad digital devices that record and practically dictate the patterns of one’s personal or professional lives. The amount of data generated each day is so huge that an exact quantification is quite improbable. What is known is that it is very “big” and the chain of information created by computers and then used by another set of computers continues to grow at an unprecedented and unimagined pace. The real challenge lies not in the availability of data, but in deriving useful knowledge from them.

“They don’t know that we know they know we know.”1 This quote, while humorous, highlights the fact that sometimes what we know is only half the knowledge. We require further insights to reach what can be called a single version and source of value proposition information.

The availability of a huge amount of data has triggered some dubious projects with unrealistic expectations. Although there is little doubt that huge benefits can be derived from effectively utilizing the powers of big data, there are a number of risk factors that organizations should consider before embarking upon the big data journey.

**VICTIM OF POST HOC ERGO PROPTER HOC FALLACY**

Post hoc ergo propter hoc is a logical fallacy in which conclusions are derived entirely on the chronology of events rather than by taking all of the related factors into consideration. The following is a typical example of this fallacy: Radio station A increased its advertisement budget by 20 percent and noticed a substantial increase in its revenues. Therefore, to overcome its continuously declining revenues, radio station B commits to increase its advertisement expenditure. In this primitive example, two correlated events (increase in advertisement and increase in revenues) are confused with causation, i.e., one event (increase in advertisement) caused the second event (increase in revenue).

The post hoc ergo propter hoc concept seems to elude decision makers of different organizations when it comes to big data considerations. As a result of initiatives taken by their peers/competitors, marketing pitches by consultants or just the general perception of big data’s benefits, organizations seem to be in a race to jump on the big data bandwagon. Often, the defined and clear objectives, careful analysis of the effort to initiate and maintain the program, and other variables are not being given proper consideration.

**BIG? DATA? MASTERING THE ART OF IGNORING**

A key reality check is determining the most significant aspect of big data. Is it “big” or “data”? Both? Neither? The correct answer would be neither.

Just having the sheer volume of data through modern data-capturing technologies is of little significance. What is done with the data and how they are used in the decision-making process take paramount importance. Different expressions (e.g., data overload, data fatigue, needle in a haystack, plucking diamonds from the waste, sipping from the hose) frequently appear in big-data-related literature. This points to the simple fact that there is a great possibility that most of the data being captured today needs to be ignored.

Most of the data being captured today needs to be ignored.

There is no denying the facts that the volume of data generated and captured today is soaring at an unprecedented pace and some initial success has already been demonstrated for using data effectively. There is also no denying that without proper planning and objective setting, organizations embarking upon the big data journey will be shooting in the dark and unrealistically hoping to hit the bull’s eye.

---

Muzamil Riffat has more than 10 years of experience in IT audit, IT security, software development and project management. He has worked for consultancy, private, semigovernment and government organizations. He holds several general and vendor-specific professional certifications. Riffat is responsible for IT audit function in a large government organization.
DISSECTING THE ATTRIBUTES OF BIG DATA

The three V’s (volume, velocity and variety) of big data were introduced more than a decade ago, but are frequently used to define big data. Figure 1 identifies the key challenges that need to be considered for each attribute.

APPLYING PROJECT MANAGEMENT PRINCIPLES TO THE DECISION TO IMPLEMENT BIG DATA

Big data is just another way of looking at data and it should be treated as such. The urgency to implement a big data program should not trump the rationality for initiating the program in the first place. The business problem/enhancement on hand, the suitability and practicality of solving the problem with a big data initiative, and the expected return on investment (ROI) should be explicitly documented, agreed upon and approved. At the minimum, the following questions should be answered factually:

- **What** is the problem/objective of the big data project?
- **Why** does one think it can be solved using big data?
- **When** will the anticipated ROI be realized?
- **Who** are the team members? The individuals involved in the big data project should have characteristics of embracing change, being receptive to emerging technologies and have a fondness for data manipulation.
- **How** will the different organizational units (e.g., IT, business, research) collaborate on the project and how will one know that one has reached the goal?

All requisite project management principles of initiating and planning, executing, monitoring and controlling, and closing should be applied to big-data-related projects. Figure 2 illustrates the phases of a typical software development life cycle (SDLC) project and the corresponding key considerations.

While considering the previously mentioned key controls, it should be kept in mind that:

- The list is generic, nonexhaustive and includes only key considerations. All organizations should assess the deliverable for each phase as per their implemented project management methodology.
- It is assumed that information security is involved in each phase and related deliverables are approved.

CONCLUSION

By utilizing the powers of big data, organizations can significantly enhance their business processes and proactively act on risk. However, by failing to plan for big data initiatives, organizations will surely be planning to fail in obtaining the desired results.

Auditors should carefully assess and ensure that all big-data-related projects are carried out as per the established project management methodology. Periodic status reports should be provided to management to ascertain the feasibility of ongoing efforts in the project.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Key Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>The large quantity of data that is produced. It is the reason for “big” in the big data expression. In 2011, humans created 1.8 zettabytes of data. This is equivalent to 200 billion high-definition movies that are each at least 120 minutes long. It would take one person 47 million years to watch all of those movies. It is estimated that the world’s total data double every two years.</td>
<td>• How does one capture all these data? • Even with plummeting hardware costs, the storage of huge amounts of data is an expensive proposition. • Power constraints are impeding the enhancements in computer processors’ clock cycles, which in turn are impacting the implementation of Moore’s law.</td>
</tr>
<tr>
<td>Velocity</td>
<td>This relates to the speed at which data are received and analyzed. In the past, data were analyzed on a historical basis. The current trend is to perform analysis and make decisions on a real-time or near real-time basis.</td>
<td>• Given the huge amount of data, how practical is it to scan the complete data set for the required information? • How can data parameters be designed so that latency in data capture, analysis and decision making can be minimized? • Different systems might produce data at different speeds (batch, streams, real time). The accurate correlation of such data is a challenge.</td>
</tr>
<tr>
<td>Variety</td>
<td>Information exists in structured, semistructured and unstructured ways.</td>
<td>• For machines, it is fairly easy to analyze the structured data set. The complexity arises when the information is available heterogeneously. • The completeness of information cannot be suitably ascertained.</td>
</tr>
<tr>
<td>SDLC Phase</td>
<td>Key Considerations</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| Planning and initiation| • Management approval and commitment have been formally obtained.  
• The objectives and scope of the program are agreed upon and approved.  
• The feasibility analysis has been performed, clearly outlining the cost-benefit analysis.  
• The proposed technological implementation integrates with the current infrastructure architecture.  
• Initial risk assessment has been carried out and steps have been taken to mitigate identified risk factors.                                                                                                                                 |
| Requirements            | • All key stakeholders and end users are involved to define the requirements.  
• The requirements are aligned with the overall business strategy.  
• The defined requirements take into consideration key business issues.  
• All regulatory or legal requirements related to data usage and privacy have been taken into consideration.                                                                                           |
| Design                  | • The detailed hardware and software requirements to support the project have been documented and approved.  
• Performance requirements have been documented and approved by specifically considering the attributes (volume, velocity, variety) of big data.  
• Data input and output cover the interfaces from all key systems.  
• Technical specifications are defined, taking into account the security requirements and the impact on the current IT infrastructure and business processes.                   |
| Development             | • A standard coding/scripting convention is used. It is expected that new requirements will be added to the program; therefore, it is important that development is carried out in a standard manner.  
• Periodic testing procedures (unit testing) are carried out to ensure the accuracy and completeness of information retrieved.                                                                                     |
| Testing                 | • Detailed testing procedures are carried out.  
• A method for ensuring that data output is complete and accurate has been determined.  
• Integration, stress and user acceptance are carried out.                                                                                                                                                  |
| Implementation and rollout | • The different components of the system are assessed for readiness.  
• Policies and procedures for production system support and maintenance are carried out.  
• Backup and recovery procedures are defined.                                                                                                                                                               |
| Post-implementation     | • A postimplementation review is carried out.  
• Satisfaction from the business users and management is solicited to ensure that expected benefits have been derived from the project.                                                                         |

**REFERENCES**


Manyika, James; Michael Chui; Brad Brown; Jacques Bughin; Richard Dobbs; Charles Roxburgh; Angela Hung Byers; *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, McKinsey Global Institute, May 2011


**ENDNOTES**

1 NBC, *Friends*, season 5, episode 14, 1999


4 Moore’s law is the observation that, over the history of computing hardware, the number of transistors on integrated circuits doubles approximately every two years.
Big Data Analytics for Sophisticated Attack Detection

The number and complexity of cyberattacks has been increasing steadily in recent years. The major players in today’s cyberconflicts are well organized and heavily funded teams with specific goals and objectives, some of which are working under a state umbrella. Adversaries are targeting the communication and information systems of government, military and industrial organizations and are willing to use large amounts of money, time and expertise to reach their goals. It is important to understand the problems and limitations that current technologies face against advanced persistent threats (APTs) and the benefits that big data analytics could provide.

Since 2006, there have been a large number of advanced, well-orchestrated attacks against industry, military and state infrastructures. In 2007, Estonia suffered a large-scale cyberattack that significantly affected the government’s online services and financial institutions. In 2008, at least three US oil companies were targets of cyberattacks; none of these companies realized the extent of the attacks until they were alerted by the US Federal Bureau of Investigation (FBI). Millions of pounds sterling were stolen from British shoppers as multiple chip and pin machines were tampered with via a supply chain attack.

In 2010, Google announced that it had suffered a sophisticated attack, named Operation Aurora. This attack affected more than 20 US companies. In the same year, Stuxnet was detected and classified as the “world’s most advanced malware.” It was created to target industrial control systems including oil, gas and power industries. In 2011, RSA was attacked and sensitive information for the company’s SecurID solution was stolen. This has resulted in further attacks against third-party companies, including Lockheed Martin and other US defense contractors that were also using RSA security solutions. Comodo and DigiNotar certification authorities were also subject to attacks, resulting in the generation of several fraudulent certificates for major companies and organizations. In 2012, another state-of-the-art malware named Flame was discovered, which malware researchers noted as the most complex malware ever created, followed by Red October and, in early 2013, Mini Duke.

While it is believed that these attacks were perpetrated by different threat actors, they share certain common aspects and some of them have been categorized as APTs.

STATE OF THE ART
Almost three decades ago, Butler Lampson described how, in the absence of total isolation, it is impossible to safeguard data from unauthorized access and programs from unauthorized execution. Later, Fred Cohen proved the undecidability of detecting computer viruses, stating that it is not possible to build a perfect virus detection tool for a Turing machine. Paul Helman demonstrated that the intrusion detection problem is NP-Hard, which means that it is a decision problem that cannot be resolved in polynomial time in any known way, although it is possible to compute approximations to the solution. Based on these findings, it is assumed that intrusion detection is undecidable and, as such, algorithms are bound to produce a number of decision errors.

The most widely used approach in intrusion detection is signature-based detection, the shortcomings of which have been discussed extensively. A simple testing methodology using known attack patterns revealed substantial limitations in intrusion detection systems while detection rates have been shown to change drastically using small variations of known attack patterns.

From the early days, the research community focused on alternative attack detection methods (behavioral/statistical). Machine learning techniques have been successfully used in certain domains, yet despite extensive academic research efforts, such systems have had limited success in the field of intrusion detection. Although some of these systems show promising results in controlled environments (detection rates higher
than 90 percent and false-positive rates lower than 0.33 percent), they achieve disappointing results in real environments (63 percent detection and 8 percent false positives). In the last few years, intrusion detection systems (IDSs) have tried to leverage cloud-based approaches to optimize their detection capabilities. Cloud-based approaches allow for the collection of information from a very large pool of users and data analysis at a central point. There has been research on the development of fully distributed IDSs to address the limitations of central and hierarchical systems; however, only small-scale implementations have been realized. Although centralized detection may enable quicker responses to emerging threats (e.g., a new, fast-spreading worm), it offers limited benefits against APTs because in targeted attacks, the number of infections (usually a handful) is too low to raise an alarm. Similarly, early warning systems (EWSs), which are used extensively for the detection of emerging threats (e.g., worms, botnets), face significant limitations in identifying threats that affect only a very small number of individuals. EWSs also face scalability issues due to the continuous increase of data traffic.

TECHNOLOGY LIMITATIONS

APTs have unique characteristics that significantly differentiate them from traditional attacks:

- APTs make frequent use of zero-day exploits or modify/obfuscate known ones and, thus, are able to evade the majority of signature-based end points and network intrusion detection solutions. In addition, the attacks are generally spread over a wide period of time and, as a result, are often outside the limited detection/correlation window of these systems.

- Attackers focus on a specific target and are willing to spend significant time and explore all possible attack paths until they manage to subvert its defenses.

- Based on the analysis of the major APT attacks, it is evident that some perpetrators are supported by nation-states that have significant enabling capabilities (intelligence collection, manufacturing, covert physical access) for cyberattacks.

- APTs are highly selective. Only a small and carefully selected number of victims are targeted, usually in nontechnical departments of an organization, as they are less likely to identify and report an attack.

Due to these characteristics, current cybersecurity solutions fail to provide an effective defense against such threats. Following are the main shortcomings of the most common security technologies.

Network/Host-based Intrusion Detection Systems

There are two main detection strategies that are currently used by network or host-based intrusion detection systems (NIDS/HIDS):

1. **Signature-based** is still the most common technique and focuses on the identification of known bad patterns. As with every system that uses a blacklist approach, it is vulnerable to attacks for which the signature is unknown, such as zero-day exploits or use of encoding, packing or obfuscation techniques.

2. **Anomaly-based**, which consists of monitoring system activity to determine whether an observed activity is normal or anomalous, according to a heuristic or statistical analysis, can be used to detect unknown attacks, but despite significant research efforts, such techniques still suffer from a high number of false positives. Furthermore, it is not foolproof, as multiple malware samples use a communication channel that resembles legitimate traffic (e.g., over an Secure Sockets Layer/Transport Layer Security [SSL/TLS] connection) and, thus, can easily evade such systems.

Finally, a major challenge for current IDSs is the limited window of time for which the connection state can be maintained. As all modern IDSs are focused on real-time detection, they can support only a short window of time (usually a few seconds) in which attacks can be detected for particular Transmission Control Protocol (TCP) sessions. Port scanning is a practical example of this weakness: A quick port scan against a host will trigger an alert from virtually any IDS. However, if this scan is spread over a period of several minutes and, thus, outside of the detection/correlation window of the network intrusion prevention system (NIPS), the attack will pass undetected for the majority of those systems.

Antivirus Products

Antivirus products face the same limitations as NIDS/HIDS, as their detection method is mainly signature-based, supplemented with heuristic analysis. Only a few products offer behavioral analysis. In addition, it is trivial for attackers
to test a wide range of antivirus products and modify their malware accordingly to evade detection.

**Full Packet Capture**
Full packet captures (FPCs) are specialized devices for capturing and archiving network traffic. They are mainly used by analysts to inspect captured traffic after a specific incident. Although they offer the most complete view of the network at any given time, supporting in-depth analysis, FPCs have key shortcomings:

- Limited analysis options are typically provided with the capture system itself, requiring the use of external tools for low-level traffic inspection.
- They offer very limited (if any) integration with other systems (e.g., NIDS/NIPS).

**Security Incident and Event Management**
Security incident and event management (SIEM) systems collect events from a wide range of sources (e.g., IDS/IPS, antivirus, event logs) and apply statistical correlation to identify potential attacks. The main challenges that such systems face are:

- The limited window of time during which these systems will correlate events—usually a few minutes. Events spread over a larger time period will usually not be correlated, and as a result, a carefully orchestrated attack may end up undetected or presented as a series of seemingly unrelated events.
- The correlation is performed centrally and is therefore limited by the available resources.

**Overall Assessment**
In addition to the weaknesses and shortcomings of the previously mentioned security solutions, perhaps an even more significant factor contributing to the difficulty of detecting APTs is the lack of efficient integration among security solutions. These solutions work as black boxes and tend to offer (limited) integration only if they come from the same vendor. If not, the only possible integration among them is generally through a SIEM system and, thus, suffers from the aforementioned shortcomings. Furthermore, the systems tend to be static, rely on their own (usually proprietary) rules and configuration language, and have their own individual knowledge banks of attack information, with which users must become familiarized.

Also, due to the proprietary nature of these devices and the lack of open standards, an analyst who wishes to write custom rules for detecting specific incidents must do so using a different language for each system (e.g., Snort-compatible signature for the NIPS, new correlation rule based on SIEM specific correlation language).

**BENEFITS OF BIG DATA ANALYTICS**
Taking into account the unique characteristics of APT attacks and the inability of current security solutions to address them effectively, a radical change in the way that security solutions operate is required.

As mentioned, attackers are willing to spread their actions over a wide period of time to evade detection systems. Thus, it is crucial to shift the focus away from real-time detection, which significantly limits the analysis/correlation capabilities. Instead, an approach focused on full-packet capture, deep-packet inspection and big data analytics that would enable the use of significantly more advanced algorithms for analysis and correlation, mitigating such evasion attempts, is preferable.

Although offline analysis (analysis of captured traffic) inevitably results in delayed attack detection, it is important to consider that in the majority of APTs, the perpetrators will spend a significant amount of time trying to reach a specific objective (e.g., exfiltrate sensitive data).32, 33

There are two main reasons why APT attacks are prolonged:
1. After an initial foothold has been gained, attackers need to explore the network, move across subnets, identify where the information that they are interested in is located and exfiltrate it. As all these steps need to be performed as stealthily as possible to avoid detection, significant time is required.
2. Attackers usually wish to maintain their access and continue to exfiltrate data in the future.

In addition, the correlation of events across large timescales and from multiple sources (e.g., analysis of network traffic, event logs and operating system/application artifacts) is crucial for the detection of sophisticated attacks. Even when attackers manage to successfully evade traditional IDSs, inevitably they generate subtle attack indicators (attack metadata) while exploiting the network. Failed login attempts, increased network traffic from a particular host(s), unusual resource utilization and execution of unknown processes can all be correlated and identified as an indication of compromise.
even if they are spread over several hours or days. Unfortunately, such indicators are almost always ignored by current IDSs.

Big data analytics focuses on the aforementioned needs and facilitates APT detection by supporting:

- Dynamic and managed collection, consolidation and correlation of data from any number of diverse data sources, such as network traffic, operating system artifacts and event data (e.g., network devices, IDS). This holistic view of the infrastructure enables defenders to correlate sporadic low-severity events as a result of an ongoing attack. In comparison with modern SIEM systems, big data analytics does not have a limited window of time based on which correlation can be performed.

- Anomaly detection, based on correlation of recent and historical events. For example, an increased volume of Domain Name System (DNS) traffic from a particular system for a small time period can be due to legitimate user actions. However, if such a pattern is also identified in historical traffic over a period of days, it is a potential indication of covert data exfiltration. In addition, such correlation can help limit the number of false-positive alerts. Big data analytics solutions increase the quantity and scope of data over which correlation can be performed.

The ability of big data analytics to correlate data from a wide range of data sources across significant time periods will result in a lower false-positive rate and allow the APT signal to be detected in the noise of authorized user activities. While processing and correlation do not have to be in real time, they should be completed within an acceptable time window (ideally a few hours) to give the defenders an early warning for potential attacks against their infrastructure.

FURTHER RESEARCH

Before big data analytics can be used in operational environments for the detection of sophisticated threats, a few obstacles need to be overcome. More specifically, there is a need for new detection algorithms, capable of processing significant amounts of data from diverse data sources. Additionally, there is a need to further progress issues related to the specific problem of malicious-activity detection using correlated data sources, such as collecting information from untrustworthy sources, storage and processing performance, time synchronization, meaningful visualization of information, and ensuring the security of sensitive indicators of compromise, among others.

Currently, a small number of proof-of-concept deployments that utilize big data analytics for security event detection exist and show promising results. Research on this promising field needs to be intensified to create robust solutions that can address the multidimensional problem of APTs.

CONCLUSION

The current industry approach, which is focused on real-time detection with emphasis on signature matching, although effective against traditional attacks, is unable to address the unique characteristics of APTs.

As mentioned, big data analytics currently faces a number of practical limitations and further research is needed for building an operational solution. That said, big data analytics will significantly enhance the detection capabilities of defenders, enabling them to detect APT activities that are passing under the radar of traditional security solutions.

ENDNOTES

1 The term “advanced persistent threat” (APT), coined by the US Air Force in 2006 as a generic term to describe intrusions without disclosing the classified threat name, has been loosely used to highlight the commonality between these attacks. Perhaps the most accurate definition of APT is given in the National Institute of Standards and Technology (NIST); NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
6 Denning, Dorothy; “Stuxnet: What Has Changed?,”
Future Internet, 16 July 2012, p. 72-687
7 RSA FraudAction Research Labs, “Anatomy of an Attack,”
anatomy-of-an-attack/
8 Leavitt, Neal; “Internet Security Under Attack: The
Undermining of Digital Certificates,” IEEE Computer,
vol. 44, iss. 12, December 2011, p. 17-20
9 Goyal, Ravish; Suren Sharma; Savitri Bevinakoppa;
Paul Watters; “Obfuscation of Stuxnet and Flame
Malware,” Latest Trends in Applied Informatics and
Computing, October 2012
10 Virvilis, N.; D. Gritzalis; “The Big Four—What We
Did Wrong in Advanced Persistent Threat Detection,”
Proceedings of the 8th International Conference on
Availability, Reliability and Security (ARES-2013), IEEE,
Germany, September 2013, p. 248-254
11 Lampson, Butler W.; “A Note on the Confinement
13 Helman, Paul; Gunnar Liepins; Wynette Richards;
“Foundations of Intrusion Detection [Computer Security],”
Proceedings of the Computer Security Foundations
Workshop V, 1992
14 Ibid.
15 Denault M.; D. Gritzalis; D. Karagiannis; P. Spirakis;
“Intrusion Detection: Evaluation and Performance Issues
of the SECURENET System,” Computers & Security,
vol. 13, no. 6, 1994, p. 495-508
16 Spirakis, Paul; Sokratis Katsikas; Dimitris Gritzalis;
Francois Allegre; “SECURENET: A Network-oriented
Intelligent Intrusion Prevention and Detection System,”
Network Security Journal, vol. 1, no. 1, January 1994,
p. 22-39
17 Puketza, Nicholas; Kui Zhang; Mandy Chung; Biswanath
Mukherjee; Ronald A. Olsson; “A Methodology for Testing
Intrusion Detection Systems,” IEEE Transactions on SW
Engineering, 1996
18 Chung, Mandy; Nicholas Puketza; Ronald A. Olsson,
Biswanath Mukherjee; “Simulating Concurrent Intrusions
for Testing Intrusion Detection Systems: Parallelizing
Intrusions,” National Information Systems Security
Conference, Maryland, 1995
19 Op cit, Falliere
20 Op cit, Goyal
21 Op cit, Falliere
22 Op cit, Goyal
23 Op cit, Drummond
24 Op cit, RSA FraudAction Research Labs
Intelligence,” Cloud Security Alliance, 2013
Data Privacy and Big Data—Compliance Issues and Considerations

The big data\(^1\) craze has taken the industry by storm. With the advent of cost-effective technologies and solutions for longer-term storage of vast amounts of transaction data, more and more companies are investing in keeping more and more data for longer and longer periods. It is important to look into the intersection of data privacy in the context of this emerging big data trend, reviewing existing data privacy regulations and considering big data in the context of an accepted data privacy framework.

In the past, due to limited space availability in expensive data warehouses, considerable effort was put into choosing and organizing data to ensure that only valuable data were kept for extended periods of time. Now, this view has changed. With many new technologies and tools, companies are beginning to store everything in horizontally scaled, commercial (commodity) off-the-shelf hardware. The value of the big data ecosystem is to collect and make sense of this large volume of raw data and convert it into useful information.

At the other end of the spectrum, regulators and society as a whole are increasingly concerned about how data are being handled by business. The area of data privacy is becoming a greater concern in the post-Snowden\(^2\) era. These giant pools of data represent tempting targets for surveillance by various security agencies, not to mention repurposing by commercial entities. As a result, there is an ongoing upwelling of outrage and calls for improved data privacy protection.

The biggest source of data is end-user personal and transaction data. A mobile network operator (MNO) could potentially keep all cellular location update (LU) information\(^2\) as opposed to just keeping information on calls or text transactions.\(^4\) An Internet service provider (ISP) could decide to keep a log of all sites visited by users for a much longer period of time (i.e., years). Most ISPs just keep a small fraction (i.e., a few hours) of this information for troubleshooting or caching purposes.\(^5\) Much information can be inferred from transaction data that end users would like to keep private and not made available indiscriminately.

Most users have been unaware of the volume of personal data retained by entities for various purposes. This is beginning to change as awareness of the data privacy debate is increasing. The two trends—increasing popularity of big data and increasing awareness of data privacy—are beginning to come to a head and companies that intend to capitalize on this era of big data need to be conscious about and address these basic ethical concerns.

There are two fundamental areas where one can look for guidance when it comes to enforcing data protection: existing regulation (written rules) and privacy frameworks (implied rules). Existing regulations form the base of compliance requirements. Many of these rules (i.e., consent requirements, declaration of purpose) still hold in the big data world. However, there are also implied rules. These are implicit expectations made between data handlers and data owners (i.e., purpose). For example, if one downloads a single-person arcade game from a mobile application store, one has a reasonable expectation that his/her address book or email information will not be retrieved and stored by the data handler.

Fortunately, there are privacy frameworks to help put some structure around these implied rules.

**WRITTEN RULES**

Even before the era of big data, there had been substantial work done on the issue of data protection and privacy. These are the written rules with which data-handling organizations must comply. Since increasing amounts of personal data started being stored during the
advent of computers in the 1970s and 1980s, there has been growing awareness of the need to protect the individual’s right to privacy.

As electronic commerce becomes more pervasive, concerns have grown about the compatibility of various data privacy and protection regulations in the context of cross-border trade among entities under differing data privacy and protection regimes. Thus, there have been moves to make the various regulatory frameworks more compatible and consistent. For example, the European Union (EU) Data Protection Directive (Directive 95/46/EC) was released in October 1995 to provide a basic framework for proper handling of personal information, and now work has begun on a draft of the General Data Protection Regulation to supersede this directive. This would allow all EU states to subscribe to a common set of principles and coordinate on enforcement.

Various countries such as Malaysia, Singapore and the Philippines have, in turn, explicit legislation on data protection and privacy. A number of these countries have passed regulation in response to the EU Data Protection Directive and have aligned their legislation with the Asia Pacific Economic Cooperation (APEC) Privacy Framework or the Organisation for Economic Co-operation and Development (OECD) Privacy Principles. The EU Data Protection Directive contains adequacy requirements that prevent the transfer of personal data to entities outside the EU that do not comply with EU standards for privacy protection. The APEC and OECD frameworks were created to ensure that states would create compatible regulation to ensure smooth interstate commerce and other forms of interaction.

Other countries, such as the US, have taken a sectoral approach to data protection legislation. The US has specific data privacy regulations for particular sectors, such as the Health Insurance Portability and Accountability Act (HIPAA) for the health care sector and the US-EU Safe Harbor Framework for the export sector that needs to exchange data with EU entities.

The aforementioned are examples of the written rules with which various entities must comply. These explicit rules and regulations continue to apply in the era of big data and have gained greater importance as more and more data are collected, retained and exchanged.

**IMPLIED RULES**

The presence of ever-increasing amounts of data that are being retained for longer periods of time has caused more concern among data-privacy advocates. Regulations may not have been updated or kept pace in the era of big data. Thus, it would be good at this point to take a step back and survey the implied rules for data protection and privacy. A good place to begin is the interaction of the APEC and OECD principles (figure 1).

![Figure 1—Key Privacy Principles](image)

<table>
<thead>
<tr>
<th>OECD Privacy Principles</th>
<th>APEC Privacy Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Collection limitation</td>
<td>• Collection limitation</td>
</tr>
<tr>
<td>• Data quality</td>
<td>• Integrity</td>
</tr>
<tr>
<td>• Purpose specification</td>
<td>• Notice</td>
</tr>
<tr>
<td>• Use limitation</td>
<td>• Uses of personal information</td>
</tr>
<tr>
<td>• Security safeguards</td>
<td>• Security safeguards; preventing harm</td>
</tr>
<tr>
<td>• Openness</td>
<td>• Choice; access and correction</td>
</tr>
<tr>
<td>• Individual participation</td>
<td>• Accountability</td>
</tr>
<tr>
<td>• Accountability</td>
<td></td>
</tr>
</tbody>
</table>

Both APEC and OECD have similar data protection and privacy principles. There are some areas where aspects are moved from one principle to another, but in general they are compatible. Together these principles serve as a good framework that embodies the implied expectations of privacy that any individual may reasonably possess.

The following is a review of these principles in the context of big data:

**Collection limitation**—This is the first principle in both the OECD and APEC frameworks, and it is also the principle that big data can potentially violate the most. Basically, it requires that only the minimum amount of data required for a specific purpose be collected and then retained only for the minimum amount of time required. One of the key selling points of big data and the advent of cheap storage is to collect everything and throw away nothing, with the further manipulation and analysis of data occurring later. It is important that organizations moving toward big data harvesting of information and update the purposes of their applications to ensure that they remain within the spirit of this principle. An additional approach that is taken by some is to anonymize data. This process is sometimes called de-
identification, where identifying ties to an individual are removed prior to the storage of large volumes of transaction data. However, care must be taken here. The simple removal of primary customer indexes might not suffice, as customer-specific information might be extrapolated from seemingly anonymous transaction data. This form of reidentification is a growing risk. Thus, some organizations additionally aggregate the data to further obscure traces of individual behavior. This anonymize-and-aggregate process requires preprocessing and results in a coarser resolution of data, which may be less useful but more protective of privacy. Anonymization is applied in the context of retrieval and long-term storage of data for which users have already provided their explicit consent. As a general rule, organizations wishing to comply with these principles should aim to collect only data necessary and properly destroy unnecessary data as soon as possible.

- **Purpose specification**—This principle requires that the purpose for the collection of data be clearly and exclusively stated. As more data are being retained with big data, the stated purposes for collecting and retaining data must be periodically and carefully reviewed to ensure continued compliance. Original purpose specifications might be too limiting and do not cover the newer use cases offered by big data. It is tempting for organizations to collect data now and find alternative uses for it much later. There have been a number of high-profile cases involving applications collecting address book information and using this information for nondisclosed purposes. This is a typical scenario as address book information is still a manageable volume that does not require big-data-level scale. However, there are now cases of application-collecting usage and location information without proper disclosure of purpose. Historically, information such as this would likely be discarded due to its volume. With big data tools available today, this information can be kept longer. Organizations should clearly state and abide by their data collection purpose to avoid potential regulatory pitfalls.

- **Use limitation**—This principle generally covers disclosure rules, particularly where data must not be shared with other parties or otherwise repurposed without consent. An important action with respect to this principle is onward transfer, which means care must be taken when sharing data with third parties. The big data era has also popularized the concept of selling or monetizing data. In particular, transaction data might be anonymized, but taken together with other data from other sources, may be used to identify individual customers. It is crucial to consider that there are many readily accessible tools, algorithms, application programming interfaces (APIs) and data sets that can be used for reidentification (i.e., combining Twitter postings and Netflix usage to determine customers based on what they are watching).

- **Data quality**—In the traditional data warehousing analytics space, it was required that data be structured upfront and preprocessed into appropriate data models. This provided some initial effort to validate the integrity of the data. In the new big data era, some approaches involve just storing the data as collected without preprocessing. Thus, errors may potentially remain within the stored data set that will be discovered only when the data are used. In some cases, applications are not adjusted to consider the potential “dirtiness” of the data because they were originally written for traditional data warehouses. These applications and services must be reviewed in the context of moving toward modelless data storage and larger amounts of dirtier data.

- **Security safeguards**—This principle requires that organizations that handle personal data provide the necessary safeguards and mechanisms to ensure that personal information does not fall into the wrong hands. As organizations put more data into low-cost commodity storage (e.g., cloud) solutions, it is crucial to review the data access controls on these external systems. A good number of these solutions do not provide the same levels of access control as more mature data-warehousing products. In some solutions, controls are enforced only at the interface level, but not at the lower levels (i.e., Hadoop clusters generally have no fine-grained Hadoop distributed file system [HDFS] access controls or security for metadata). It is important that organizations implement their own controls to plug these potential compliance gaps.

---

**Enjoying this article?**

- Read Privacy and Big Data.  
  [www.isaca.org/privacy-and-big-data](http://www.isaca.org/privacy-and-big-data)

- Collaborate on and discuss privacy/data protection and big data in the Knowledge Center.  
  [www.isaca.org/knowledgecenter](http://www.isaca.org/knowledgecenter)
• **Openness**—This principle requires information, developments and updates to be communicated to stakeholders in the most expedient manner. The implementation of this principle should be as transparent and timely as is implemented today by more mature, enterprise-class data warehouses. Organizations are encouraged to properly and promptly inform users of policy changes and developments. They are also encouraged to remind users of the consent they have already provided for the existing data sets.

• **Individual participation**—This principle emphasizes the role of the individual in the management of his/her data. The customer has the right to request personal data collected through reasonable procedures and receive a timely response. The customer also has the right to erase, rectify, complete and otherwise amend personal data. In the big data era, a good amount of data is not preprocessed in a similar fashion as traditional data warehouses. This creates a number of potential compliance problems such as difficulty erasing, retrieving or correcting data. A typical big data system is not built for interactivity, but for batch processing. This also makes the application of changes on a (presumably) static data set difficult. Organizations may find this particular requirement challenging to implement because of the potentially complex consent mechanisms required for multiple various pieces of collected information and its use. However, if they do find this challenging they might want to reconsider even handling the data in the first place because compliance is likely harder.

• **Accountability**—This principle requires that organizations that collect and store personal data be held accountable for enforcement of the other principles in this policy. This includes actions such as breach notification. The implementation of this principle should be as implemented today by more mature, enterprise-class data warehouses.

   Additional principles that are gaining acceptance and being introduced into regulation include:

   • **A priori consent and explicit opt-in**—This requires that organizations ask for up-front consent and requires explicit opt-in by the individual. Organizations are encouraged to have configuration interfaces that allow their users to manage their privacy consent settings. Big data implementations normally collect data from mediation platforms or raw and unprocessed logging services, which make it difficult to remove customers who have not opted in. This may entail a substantial amount of preprocessing.

   • **Data sovereignty**—Some states have created regulation that affirms that data considered personal should not leave the territory of that state. This creates problems when implementing applications that are essentially global, but whose users may be citizens of such a state.

   • **Extrapersonal protection**—In some jurisdictions, there may be additional, distinct classes of personal information that require additional protections or controls. This class of information is normally called sensitive personal information (i.e., medical records, political views, race, religion).

**CONCLUSION**

Big data provides numerous opportunities for organizations to maximize the potential of the data they already have. A new era of store-everything-and-determine-its-use-(and perhaps monetize it)-later has begun. As organizations mobilize to take advantage of these developments, care must be taken to ensure compliance with both the current written rules (statutory and regulatory requirements) and the implicit rules when handling data covered under various data privacy and protection frameworks.

Data privacy and protection rules and regulations still need to be updated for the era of big data. As a matter of fact, many existing regulations have not been reviewed in the context of data warehousing (e.g., privacy laws covering only wiretapping). Extra care must be taken by organizations and constant vigilance is required in this ever-changing regulatory landscape. This creates more impetus for review in the context of data. However, it would be good to be grounded in key principles aligned with those advocated by OECD and APEC. With these core principles updated in the context of big data, organizations can reap the benefits of big data without potential compliance pitfalls, now or in the future.

**ENDNOTES**


3 LU information is generated every time a mobile moves from cell to cell.

4 Every step made with a mobile phone is known to the MNO. This is the only way an MNO can route a call.


7 Parliament of Malaysia, Personal Data Protection Act 2010 (Act 709), “An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto,” 2010

8 Republic of Singapore, Personal Data Protection Act 2012 (No. 26 of 2012), “An Act to govern the collection, use and disclosure of personal data by organisations, and to establish the Personal Data Protection Commission and Do Not Call Register and to provide for their administration, and for matters connected therewith, and to make related and consequential amendments to various other Acts,” 2012

9 Congress of the Philippines, Data Privacy Act of 2012, RA 10173, “An act protecting individual personal information in information and communications systems in the government and the private sector, creating for the purpose a national privacy commission, and for other purposes,” 2012

10 APEC Secretariat, APEC#205-SO-01.2, Asia Pacific Economic Coorperation (APEC) Privacy Framework, 2005


14 Schnell, Joshua; “Path Fined by FTC for Illegally Collecting Information From Children,” MacGASM, 1 February 2013, www.macgasm.net/2013/02/01/path-fined-ftc-for-illegally-collecting-information-from-children/

Cloud-based services are on the rise. According to recent publications, the cloud is the future for the provision of a wide range of IT services. For example, Capgemini’s latest World Quality Report estimates that cloud-based software testing will encompass 32 percent of all testing by 2015.¹ A Gartner study estimates the market for cloud computing to reach US $150 billion in 2014.² Beyond short-lived hype, this trend should not be ignored from an information security perspective.

Cloud services can allow companies to reduce costs and to operate more flexibly than with a traditional IT infrastructure and thus can enable them to develop new business. However, the promising opportunities of this technology go hand-in-hand with certain risk arising from migrating and operating a business service following the new technological paradigm. One may think, for example, of failures of large cloud service providers such as the Amazon EC2 service in 2011, where customers could not access their data for days,³ the Dropbox vulnerability that allowed users to access files of other users without authorization,⁴ or recent US National Security Agency (NSA) discussions.⁵

In the context of service migration to the cloud, such incidents indicate the importance of considering the spectrum of information security and data privacy risk and properly managing these. Information security professionals are faced with the challenge to come up with solutions for an inherent antagonism related to cloud computing: Abstracting from details (e.g., from where a service is provided) and transfer tasks (e.g., data backup) while at the same time retaining responsibility for mission-critical services and data.

A variety of publications exist covering the economic aspects of cloud migration decisions.⁶ Also, the pros and cons of potential technical architectures and operating models, such as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), are intensively discussed.⁷ Yet, from an information security perspective, an additional and up to now often neglected core element to be taken into account is the information being processed as part of the respective service and thus affected by an intended service-to-cloud migration.

To ensure compliance with internal policies and fulfill given legal or regulatory requirements, the organization needs to be aware of the different types of data used throughout the service to be migrated. For each data type, the organization should actively decide on appropriate security measures to manage related risk.

Therefore, one important step during the early stages of such projects should be the identification of all information objects that are involved in the respective service. Following identification, risk related to the various information objects needs to be assessed. Based on the results of this assessment, a suitable solution can be chosen from available (cloud) deployment models. This helps to avoid compliance violations and unplanned adverse effects on security, which could lead to increased costs and, in worst-case scenarios, even overcompensate benefits expected from migration to the cloud.

A systematic approach to the assessment of such risk is key to reliably determining the required level of protection for data intended to be cloud-processed. The Cloud Service Evaluation Model (CSEM), developed by the authors of this article, suggests an easy-to-adopt method based on a structured questionnaire that can provide guidance in situations where services are to be moved to the cloud.

**CLOUD COMPUTING**

Cloud computing has been widely discussed in recent years, while, not surprising for a young technology, a single, generally accepted definition has yet to emerge. However, the definition from the National Institute of Standards and Technology (NIST) has been referred to regularly and adopted by other governing bodies and professional organizations, such as the European Network and Information Security Agency (ENISA), the British Standards Institution (BSI) and the Cloud Security Alliance (CSA), and, thus, will be employed here:
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.\(^8\)

The five core features that characterize a cloud service are shown in figure 1.

Furthermore, NIST distinguishes the three service models: SaaS, PaaS and IaaS. As further classification criteria complementing the five mentioned core characteristics and the three service models, NIST suggests the deployment model. The four major cloud deployment models to be distinguished are shown in figure 2. From an information security perspective, it is of high importance which deployment model is chosen for a cloud service.

<table>
<thead>
<tr>
<th>Figure 1—Five Essential Cloud Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On-demand self-service</strong></td>
</tr>
<tr>
<td><strong>Broad network access</strong></td>
</tr>
<tr>
<td><strong>Resource pooling</strong></td>
</tr>
<tr>
<td><strong>Rapid elasticity</strong></td>
</tr>
<tr>
<td><strong>Measured service</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Figure 2—Cloud Deployment Models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private cloud</strong></td>
</tr>
<tr>
<td><strong>Community cloud</strong></td>
</tr>
<tr>
<td><strong>Public cloud</strong></td>
</tr>
<tr>
<td><strong>Hybrid cloud</strong></td>
</tr>
</tbody>
</table>


**INFORMATION SECURITY CHALLENGES IN CLOUD COMPUTING**

After having recapitulated the core characteristics of cloud computing, questions regarding related information security challenges arise. For many companies, cost savings and economic efficiency are principal drivers for the use of cloud services. These savings are expected to result from reduced investments compared to in-house IT. Increased scalability requires fewer buffers for high system load situations. Pay-per-use models allow efficient resource allocation. Flexibility enables faster service setup and adjustments. Location independence of cloud services and distribution across multiple data centers improve general service availability. Last but not least, organizations can focus on their core business...
while IT services are sourced to specialists. At least for smaller organizations, it is reasonable to expect that a specialized service provider is able to deliver IT services on a higher maturity level than the organization would be capable of on its own.

Still, bearing in mind all those advantages, there are also challenges to meet when it comes to cloud services. The most prominent among those is, according to industry decision makers, the security of processes, applications and data.9

Savings as a result of not having one’s own IT infrastructure go hand-in-hand with having less control over IT systems and limited room for action in certain cases, e.g., in incident and problem management. Not having to care about the system on a regular basis may, at the same time, mean not being able to solve a problem independently in a critical situation.

Efficient resource utilization is implemented via resource pooling and average load calculations in clouds. If high-load situations for multiple cloud participants coincide (e.g., during the Christmas trade), the resource pool might not be sufficient and, without further contractual provisions, this could lead to service disruptions.

With in-house IT systems, resources such as buffer systems for temporary high-load situations or for business continuity are often used as test systems to improve capacity utilization. In pay-per-use models, some organizations might be more reluctant to invest money to test system resources, which might lead to less-comprehensive testing. The same accounts for resource-intensive security assessments, e.g., for disaster recovery tests that might be scheduled less frequently if the standby backup infrastructure is paid based on a per-use model.

Flexibility of cloud service setup sometimes leads to situations in which business departments set up and use a cloud-based service as a kind of end-user computing, without involving the organization’s central IT. This, combined with lack of adequate governance, might lead to security risk and compliance violations.

Location independence of data processing in the cloud, i.e., not caring and potentially not knowing where specific data are actually stored, may constitute a serious issue from an information security perspective as this contradicts an organization’s ultimate responsibility for its data. Regulations such as national data privacy laws explicitly specify where certain information may be processed. Furthermore, other legal aspects are to be considered, e.g., what happens if data get lost, published or confiscated in a data center in another country under a different jurisdiction? Systems and data hosted by the big players in the cloud service market can be expected to be run more smoothly due to a large resource pool. On the other hand, for example, as recent revelations in the Snowden case show, data hosted with these big players are more prone to access by third parties—a situation that, even if these are governmental institutions, might give rise to some legal concerns seen from an international perspective.

Different types of risk exist here, often related to transparency of the respective cloud service for users. These risk factors can be mitigated partially, for example, through corresponding contractual provisions between user and cloud provider or independent audits. Yet, these issues should definitely not be neglected.

Another issue might be cross-instance effects. Changes to the cloud infrastructure as a whole, or in other users’ instances, may affect one’s own service regarding confidentiality, integrity and availability. In a similar manner, security risk factors on a higher architecture level need to be considered (e.g., in virtualized environments, hypervisor, host system and hardware), which is not under control of the user organization.

The scalability, combined with granular and flexible service fees, facilitates fast-paced changes of the provided services’ dimensions. Such changes might, at the same time, have significant impact on the security posture of the respective system or service, for example, a service such as Dropbox storing documents for a few hundred people in the beginning vs. millions of people shortly after launching. Security processes and controls need to be set up in a way to adequately cope with this.

The last cloud service advantage mentioned at the beginning of this section is the possibility for an organization to focus on its core business while certain IT services are handled by the cloud provider. Again, moving a service to the cloud does not absolve an organization from its ultimate responsibility for the processed data. When moving a service to the cloud, it is crucial from an IT security perspective that the organization ensures the relevant expertise at its disposal to monitor the respective service and fulfill its duties.

This demonstrates that when deploying a service to the cloud, it is of utmost importance to select an adequate operating model that fits an organization’s specific need with regard to security, risk management and control. CSEM offers an easy-to-apply evaluation model. Structured into six individual
steps, the CSEM approach provides users the ability to identify critical features of their service to be cloud-sourced and systematically select a fitting cloud deployment model.

CLOUD SERVICE EVALUATION MODEL OVERVIEW

The overall purpose of the CSEM is to identify a suitable cloud deployment model for a given IT service intended to be moved to the cloud. On one side, there is the given service with its individual features and requirements. On the other side is the spectrum of cloud deployment models as potential solutions. Figure 3 illustrates how the CSEM establishes a link between targeted IT services and potential cloud deployment models. Two main instruments are applied here:

1. A structured target service questionnaire is used to assess the respective service and identify specific features of the data processed within.
2. The deployment model frame of reference presents available cloud deployment models, describing their strengths and weaknesses.

Because the questionnaire and frame of reference use the same evaluation dimensions—confidentiality, integrity, availability and transparency (C/I/A/T)—results can be easily matched and the best-fitting cloud deployment model for a given IT service can be identified in a subsequent step.

DEPLOYMENT MODEL FRAME OF REFERENCE

A detailed assessment of deployment models needs significant expertise and can be time-consuming. On the other hand, the general evaluation of cloud deployment models does not need to be reperformed every time a service is assessed. It can be reused. While allowing individual assessments, CSEM already provides a frame of reference (FoR) containing prepared ratings for four common cloud deployment models as a starting point to accelerate practical implementation.

All deployment models were rated on a three-level scale of low, medium and high regarding their abilities to support C/I/A/T. The assessment of the individual cloud deployment models started with a proposed classification based on statements in current research and professional literature. This proposal was then discussed and refined by subject matter experts (SMEs). Figure 4 shows the resulting FoR, including proposed ratings for common cloud deployment models.

Based on feedback from SMEs, the public cloud deployment model was divided into two sub-classes, reflecting international public cloud offerings (e.g., Google, Amazon) and regional providers, where data processing happens in limited, defined geographic regions and, thus, is subject to the same legislation as the client’s local IT. As a result, figure 4 shows, for example, that the deployment model of an international public cloud received a low rating regarding the confidentiality criteria. Without further measures, it is difficult to identify exactly who has access to data stored in such a public cloud, e.g., from the provider’s side. Integrity was rated medium as, on one hand, certain technical features are implemented to ensure correctness of transfer, processing and storage of data. On the other hand, such models usually do not offer deep insights into the applied measures, and options to control data processing on a detailed level are limited. Due to sheer size and capacity of public cloud providers with distributed data centers all over the world, their service availability features can be considered superior to an average midsized company’s local IT. This results in an availability feature rating of high for public clouds. Of course, other factors such as network availability may also play a role here.

The transparency rating reflects the opportunities for a client (or its auditor) to acquire information on how, where and when its data are processed and to control the data processing. This might be of high relevance if the respective service is subject to certain legal or regulatory requirements and compliance has to be proved. By nature, public clouds abstract from where (and, to a certain extent, by whom) data are processed if no further measures are taken, thus resulting in a low rating for transparency.
The suggested ratings for all other cloud deployment models within the FoR were derived in an analogous manner as described for the international public cloud.

APPLICATION OF THE MODEL
The model described previously can be applied by following a stringent, six-step process (see figure 5).

Identify Affected Data
As a first step, any organization adopting the CSEM to deploy a chosen service in a cloud environment needs to identify and create a list of all individual data objects, which are processed in context of the respective service. A valid approach here can be to inquire with the business specialists for the service. They will be able to point out core data elements, e.g., content of a company web site, order information from an e-commerce system, client names and addresses inside a CRM. If it is not a new service and the service was supported with in-house IT previously, the related systems, interfaces and data storages (e.g., databases, file servers) can be inspected to identify data objects processed by the service. IT specialists can contribute here through identifying technical data objects (e.g., log files, metadata, backups), which are, of course, relevant as part of a holistic assessment, but not always the focus of business experts’ reviews. The collection of data objects needs to pay attention to the whole of processes linked with the targeted service in order to identify all relevant objects. Thus, the information gathering should be performed by business and technical professionals together.
Assess Information Security Requirements

Subsequently, a structured questionnaire (figure 6) is used to assess the C/I/A/T information security requirements for the previously identified data elements. For each of the four main C/I/A/T criteria, respondents are asked to assess the risk level of their data on a three-level scale (low, medium, high). Per the information security goal (e.g., availability), three to six questions are asked. To support structured replies, different types of risk (e.g., compliance violations, financial loss, reputational impact) are to be considered in each answer. After all types of risk have been rated, the overall C/I/A/T risk levels are determined in the next step.

Determine C/I/A/T Risk Levels

To attain an overall risk level for the reviewed service (and the data processed within) regarding each of the main C/I/A/T criteria, the questionnaire answers are condensed. For each criteria, the highest impact rating (figure 6) is considered as determinant and, thus, as reference for selection of a suitable cloud deployment model later.

Evaluate Cloud Service Matrix

The results of the previous step have to be filled in to the comparison column of the cloud service matrix. Either the standard weights (i.e., low equals 1, medium equals 3, high equals 9) can be used, or a custom weighting may be applied. Now the available cloud deployment models, with their capability ratings taken from the FoR, are compared against requirements of the service under review as identified via the questionnaire.

If a deployment model meets or exceeds the required risk level, it is attributed with points matching the required level. For example, the overall data confidentiality requirement for the assessed service is medium, the deployment model private cloud is rated high for confidentiality capabilities in the FoR; hence, the deployment model fulfills the requirement. Because of this, in the evaluation, the deployment model is attributed three points for fulfilling the medium requirement. Please note that, though it offers high confidentiality, only medium was required; therefore, no more than three points can be received here. There is no bonus for exceeding given requirements.

Examine Mitigation Measures

If certain deployment models turn out to be close to the requirements, but slightly miss some individual targets, further measures to achieve fulfillment of requirements can be evaluated in this step. For example, additional local encryption of data before moving them to the cloud could mitigate confidentiality issues in a cloud setup. Certifications or independent service reports (e.g., ISAE 3402) could contribute to transparency, for example.

Select Cloud Operating Model

In the final step, the evaluation matrix (figure 7) lists a comparison of all available cloud deployment models and shows how well they fulfill the specific C/I/A/T requirements of the respective service that is supposed to be moved to the cloud. Those deployment models, the scores of which are closest to the reference score of the target service, are those that are the most suitable and potential candidates for an implementation. If two deployment models arrive at similar overall scores, the most economically efficient solution should be chosen. Current literature suggests that for medium-sized companies, costs usually increase from public cloud deployment models toward individual private clouds. This is also reflected in the economic impact in figure 4. The results of step 5 have to be considered here to take into account which changes or additional measures are feasible to match service requirements and deployment model capabilities.

<table>
<thead>
<tr>
<th>Question</th>
<th>Compliance Violation</th>
<th>Financial Loss</th>
<th>Reputational Impact</th>
<th>Maximum per Question (Row Max)</th>
</tr>
</thead>
<tbody>
<tr>
<td>How severe is the impact if the service is not available for an hour?</td>
<td>Low (1)</td>
<td>Low (1)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
</tr>
<tr>
<td>Impact if data of the last 24 hours are lost and cannot be recovered?</td>
<td>High (9)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>High (9)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Availability requirement overall rating (last column max)</td>
<td></td>
<td></td>
<td></td>
<td>High (9)</td>
</tr>
</tbody>
</table>
CONCLUSION
While the number of services that will be cloud-supported in the future will doubtless continue to increase, selecting the right cloud deployment model is not an easy matter, especially when taking into account the various information security challenges. The presented CSEM decomposes the inherent complexity into a sequence of structured and manageable steps that help to cope with this challenge.

As demonstrated, such assessments can be divided into two main parts: assessing the requirements of the service to be outsourced and evaluating the available cloud solutions for their appropriateness for the given task. The first part needs an individual C/I/A/T requirements assessment for each target service and can be performed, based on the provided questionnaire, with reasonable effort by the risk manager together with business, given that they know the concerned processes and systems well. However, the second task encompasses evaluating available cloud solutions regarding their C/I/A/T features. Here, the CSEM FoR, with its sample evaluation of four common cloud deployment models, can be used as a starting point. Putting both, the questionnaire and the FoR, together, the CSEM, with its systematic, six-step approach, enables professionals to efficiently provide comprehensive counseling during cloud service migration projects and identify suitable solutions. IT auditors may leverage the CSEM approach to assess cloud-deployed applications in a structured way.

It is a fairly safe bet to say that in the future, in many cases, the question will not be whether a cloud model should be used, but which cloud model. It is critical to be prepared.

ENDNOTES
2 Gartner, “Gartner Identifies Seven Major Projects CIOs Should Consider During the Next Three Years,” press release, 9 November 2010, www.gartner.com/newsroom/id/1465614
6 For example: Rosenberg, Jothy; Arthur Mateos; The Cloud at Your Service, Manning Publications, 2010
7 For example: Sosinsky, Barrie; Cloud Computing Bible, Wiley, 2011
10 The questionnaire is available upon request from the authors. Contact thomas-schaefer@onlinehome.de.
Electronic Documents Information Security Compliance

The increased use of technologies that allow electronic document storage and electronic communication with clients by governments and enterprises has led lawmakers and courts in many jurisdictions around the world to consider the legal status of such information and the legal effect of that communication. Legislators across the globe recognized the need for new laws to permit and ensure the admissibility of electronic information as evidence and, more so, to enable contracts to be concluded and administrative submissions and requests to be made in electronic form. Perhaps the most important of these is the United Nations Commission on International Trade (UNCITRAL) Model Law on Electronic Commerce.¹ In one form or another, this law has been enacted in at least 31 countries.² Other countries have adopted digital signature legislation, generally modeled on the UNCITRAL Model Law on Electronic Signatures, which also impacts use of electronic documents to establish business relationships and perform interactions with other entities and individuals.³

Certain legal requirements and obligations of institutions and legal entities need to be fulfilled to ensure the admissibility and reliability of electronic documents. According to the UNCITRAL Model Law on Electronic Commerce, “in assessing the evidential weight of a electronic document regard shall be had to the reliability of the manner in which the electronic document was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.”⁴

Failure to take appropriate information security measures regarding electronic documents might constitute a violation of legal obligations in some countries and result in fines. So, for example, under the Bosnia and Herzegovina Law on Electronic Documents,⁵ breaches, subject to fines of up to €7,500, include:

- Prevention verification of authenticity and integrity of electronic documents
- Archiving of electronic documents in such form and with such technologies and procedures that do not provide a reasonable guarantee of their authenticity and integrity for the entire storage time
- Application of information systems with inadequate protection of personal data in accordance with the provisions of the law governing the protection of personal data

COMPLIANCE

To demonstrate compliance with legal requirements relating to the preservation of the authenticity and integrity of electronic documents throughout the entire electronic document life cycle, organizations should establish a documented risk-based information security management system (ISMS) and maintain records to confirm compliance. To ensure good record-keeping practices are followed to avoid problems with records acceptance in the event of litigation, an organization should periodically assess its practices and procedures.⁷

“Consistent use of a risk management strategy and assessment process will show outside assessors (and courts of law) that due diligence was completed and justification for any specific direction in technology implementation was documented. Will it resolve all liability and risk? No, of course not. Will it show due diligence and risk analysis? Absolutely.”⁸

Protection of Vital Electronic Records

Each organization must analyze its own operations and records to determine what information is vital to its continued existence. Once vital electronic records have been identified, the remaining records can then be classified as important or useful. Identified vital records and information require special protection from potential loss. Typically, only 3-7 percent of an organization’s electronic records would be classified as vital.⁹
The record types listed in figure 1 are examples of what might be considered in each classification. It is the responsibility of each organization to determine the classification of the records and information for that organization.10

**Audit Trail**
When preparing electronic records for use as evidence, it is often necessary to detail the storage date of the information, the movement of the information from one medium to another and the evidence of the controlled operation of the records management system (RMS). These details are known as audit trail information. The audit trail consists of a historical record of all significant events associated with the RMS.11

Procedures for audit trails and any changes to the accepted procedures must be documented in an RMS procedures manual. Audit trails must contain sufficient and necessary information to provide evidence of the authenticity of stored records. The audit trail of an RMS shall consist of system-generated and operator-generated logs containing data about changes to the stored records. If the authenticity of stored records is questioned, the integrity of the audit trail may be fundamental in establishing the authenticity and, therefore, the evidentiary weight of the stored records.

**CONCLUSION**
The laws pertaining to electronic documents in most countries are not sector-specific. The enactment of these laws means that all organizations will have to take appropriate measures to protect document integrity while using electronic documents in their ordinary course of business. Failure to take these measures is no longer just lack of due professional care, but constitutes a violation of legal obligations and can result in fines.

Application of such laws requires knowledge from various fields, including familiarity with a number of regulations that are directly or indirectly related to its provisions. Additionally, management of IT and information security is a prerequisite for their proper utilization.

Electronic records processing systems designed and implemented in a fashion to ensure that records cannot be altered or modified without audit trails and/or history logging can produce accurate results. Such systems must follow a

---

**Figure 1—Sample Records Classification**

<table>
<thead>
<tr>
<th>Class</th>
<th>Definition</th>
<th>Example</th>
<th>Example Protection Method</th>
</tr>
</thead>
</table>
| Vital   | These records contain information essential to the continuation or survival of an organization during or immediately following a crisis. Such records are necessary to continue operations without delay under abnormal conditions. They contain information necessary to re-create an organization’s legal and financial status and to preserve the rights and obligations of stakeholders, including employees, customers, investors and citizens. Vital status should be assigned only for as long as records fulfill the stated requirements. Once they have fulfilled this role, they should be reclassified. | - Current accounts payable and accounts receivable  
- Current customer or client files  
- Research documentation  
- Current contracts and agreements  
- Unaudited financial records | - Backup tape stored offsite  
- Backup tape and backup microfilm stored offsite  
- Backup files from imaging server sent by electronic transmission to a remote electronic vault  
- Ledgers and transaction documentation stored in a standard record vault  
- Original records transferred to offsite protective storage and surrogate copies used for reference |
| Important | These records are necessary to the continued life of the business. They can be replaced or reproduced only at considerable cost in time and money. | - Ownership records for land, facilities, equipment and vehicles  
- Tax records | - Backup of imaging media stored offsite  
- Routine and planned dispersal |
| Useful  | These records are useful to the uninterrupted operation of the business. They are replaceable, but their loss could cause temporary inconvenience. | - Bank statements  
- Correspondence | - Routine dispersal |
well-documented business process demonstrating that the process used to create, store and access the records is reliable and contains appropriate levels of security for users and system administrators, preventing unauthorized access and/or records deletion/modification.

No matter how strong its data security policies and controls are, an organization will not really know the adequacy of its defenses unless it continually verifies that its defenses are sound, uncompromised and applied in a consistent manner. To achieve such assurance, internal audit has to play a far more substantial role in evaluating information security practices or implementation than is often the case today.

ENDNOTES
2 Montana, John C.; John R. Kain; Kathleen Nolan, Legal Obstacles to E-Mail Message Destruction, ARMA International Educational Foundation, 19 October 2003
4 Op cit, UNCITRAL, 1996
5 This act established a legal basis for administrative bodies, local authorities, business enterprises and individuals to accept and use electronic documents in their work and daily operations. The act is fully harmonized with related European Union (EU) legislation and current global best practice. Its adoption is in line with the directives of the European Union, under which Bosnia and Herzegovina must create all preconditions for electronic access to information and e-commerce.
7 AIIM International, AIIM TR31-2004, Legal Acceptance of Records Produced by Information Technology Systems, 2004
Writing Good Risk Statements

A fundamental part of an information systems (IS) audit and control professional’s job is to identify and analyse risk. Furthermore, risk factors need to be stated clearly and concisely to support effective management of risk. Thus, it is critical that IS audit and control professionals know how to write a good risk statement that is impactful and aligned to better practice.

A marker of a good quality risk statement is that it can answer the following questions:

- What could happen?
- Why could it happen?
- Why do we care?

Summarising risk identification and analysis in a statement is not a science and there is no specific formula to get it right; however, there is guidance provided in the ISO 31000:2009 Risk management—Principles and guidelines that can help to better articulate risk.

The key to writing a good risk statement is having a foundational understanding of risk components and their interrelationships. Understanding key risk-related terms and their definitions, as well as the business and its objectives, will result in more impactful risk articulation.

DEFINITIONS WITH AN EXAMPLE CASE

To illustrate the application of these definitions in practice, one can consider a fictional bank with an objective to “keep confidential customer information secure” that is implementing a change to a highly complex customer account management system that handles customer information.

The key definitions are:

- **Risk** is the effect of uncertainty on objectives.¹
- **An effect** is a deviation from the expected.² The effect in the example is the deviation from the expected condition of customer information being kept secure. Expected conditions are those conditions that are expected by the bank’s stated objectives and policies.
- **Uncertainty** is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.³ Uncertainty in the example is from not fully understanding the consequences of the change due to the customer account management system being highly complex and inherently difficult to understand. The greater the complexity of the at-risk area, the greater the inherent uncertainty. The objective in the example is for the bank to keep confidential customer information secure.
- **An event** is an occurrence or change of a particular set of circumstances and can have several causes.⁴ In the example, the event may appear to be the system change itself, but there is no direct effect on objectives if the change goes through without a problem. An event must have an effect on objectives. Data leakage related to problems with the change would be an event, as this directly affects the objective to keep confidential customer information secure.
- **A cause** is that which gives rise to any action, phenomenon or condition.⁵ It is important not to mix up the cause and the event. In the example, defective changes, such as encryption algorithms not encrypting data as expected, cause data leakage. Defective changes do not have a direct effect on the objective of safeguarding customer information in and of themselves, and so should not be seen as an event in this case, but rather a cause. Data leakage, on the other hand, does have a direct impact on objectives so it would not be a cause in this scenario. A risk statement can contain multiple causes when applicable.
- **A consequence** is the outcome of an event affecting objectives.⁶ This element of the risk statement is important because it highlights why one should care about the risk. It is crucial that this is relevant, plausible and, ideally, quantified to give this element meaning in real terms. A vague statement of “damage to reputation” is not enough. How will this damage to the organisation’s reputation impact the organisation? If the organisation is an effective monopoly, reputational damage...
may not be an issue. The consequence ideally needs to be quantified using industry research data, internal management information or known cause-and-effect relationships, such as known fixed fines levied by regulators or known customer impacts for instances of customer data leakage. A good example of this is the maximum fine of UK £500,000 that can be levied by the UK Information Commissioner's Office for confidential customer data leakage incidents or alternatively customer churn of 6.4 percent derived from industry research reports.

- **Likelihood** is the chance of something happening; risk is a combination of potential events and consequences along with the associated likelihood of occurrence. In the example, “something” refers to the combination of potential events and consequences. Likelihood can be reasonably estimated through frequency analysis of similar events in the industry, specific technology from internal organisation incident or issue databases and consultation with subject matter experts. So, considering the example, the risk analyst might look at the number of loss events in the past 12 months registered in an internal loss event database, an external database such as the Privacy Rights Clearinghouse, or a media scan, where causes related to poorly controlled changes are recorded. Looking at the frequency of these events over the total number of changes made would give a basic estimation of the likelihood of the event recurring.

Based on these definitions, a risk statement should look something like:

> [Event that has an effect on objectives] **caused by** [cause/s] **resulting in** [consequence/s].

An alternative two statement version is:

> [Event that has an effect on objectives] **caused by** [cause/s]. This may **result in** [consequence/s].

The latter version is better to use if the risk statement sentence would be too long and needs to be broken up to improve clarity. This might happen, for example, if there are a large number of key risk causes.

Taking the previous example to illustrate this, if the bank’s objective is to “keep confidential customer information secure” and the event is customer data leakage, corruption or unavailability caused by defective system changes, the risk statement could be:

Customer data leakage, corruption or unavailability **caused by** defective system changes **resulting in** financial fraud losses of UK £1 million and an Information Commissioner’s Office fine of UK £500,000, customer churn of 6.4 percent, and regulatory sanction by the Prudential Regulation Authority.

Data leakage, corruption and unavailability are information security failure events. That is, keeping information secure (the objective) has deviated from (the effect). The unauthorised, defective or unfit changes are the causes of this effect on objectives, while the consequences are defined in terms of what happens if the organisation fails to meet its objective.

**POINTS TO NOTE**

There are different levels of objectives. A clue to selecting the right level is to look at the objectives of the organisational unit for which you are undertaking risk assessments. For example, the IT function is required to protect information assets in its care, so protecting information is one of its objectives (this may also be reflected in policy statements). To highlight this, consider the following two risk statements:

1. Customer data leakage, corruption or unavailability caused by defective system changes resulting in financial fraud losses of UK £1 million and ICO fine of UK £500,000, customer churn of 6.4 percent, and regulatory sanction by the Prudential Regulation Authority.
2. Loss of market share caused by eroded customer confidence in the organisation’s information security resulting in net revenue reduction of UK £200 million and bank share value reduced by 12 percent.

- Refer to COBIT® 5 for Risk
  www.isaca.org/cobit
- Discuss and collaborate on risk management in the Knowledge Center.
  www.isaca.org/topic-risk-management
These two risk statements are valid depending on their context. The first is valid if the context relates to keeping customer information secure. The second is valid in the context of achieving the organisation’s business strategy. The first risk statement would mean more to those responsible for managing customer information systems security in that it tells them exactly what needs to be controlled (the system change process). The second statement might mean something to higher-level executives responsible for delivery of business strategy that includes maintaining market share, but these people will not generally be responsible for implementing and monitoring system change controls. The key message is to know the audience and tailor the risk statement to that audience.

It is important to not get bogged down trying to list every conceivable cause or consequence; instead, one should highlight the key causes and consequences only.

Likelihood (or probability) is a key element of risk. For risk to be risk, there needs to be that element of uncertainty. If the risk factor is 100-percent certain to happen, this is not a risk, but an issue. If the risk factor is impossible, it is irrelevant. For example, the possibility of data leakage due to defective system changes to the customer account management system is a risk. But, if this risk is certain to materialise, it is an issue that needs to be managed as such. If the risk under consideration is of a simultaneous meteor impact on two geographically distant data centres, this is close to impossible and would not be registered as a risk.

APPLICATION TO FINDINGS REPORTING

When writing up findings to report, use only the “[Event that has an effect on objectives] caused by [cause/s]” component of the risk statement for the title. If the title still will not fit, try to make it more concise. One may need to classify the causes and edit any noninstrumental causes to help clarify the finding’s title. The full risk statement should be included in the body of the finding being reported.

CONCLUSION

Risk can be more effectively understood and managed if it is clearly articulated. This can be achieved by remembering risk definitions while writing risk statements. Having an understanding of the objectives at risk is also key. The IS audit and control professional should create concise risk statements that are information-rich and relevant to the situation and the audience to ensure that the risk statements have an impact and support effective risk management.

ENDNOTES

2 Ibid.
3 Ibid.
4 Ibid.
6 Op cit, ISO, 2009
7 Ibid.
Most approaches to process audits are antiquated and far from best utilizing the auditor’s capabilities or the potential of existing enterprise resource planning (ERP) data. Instead, it would be ideal to start a process audit fieldwork project with the best information set available: complete models of actual processes conveniently displayed even on mobile devices, data analytics finished with high-risk business transactions clearly indicated, internal controls evaluated to the maximum extent and all results directly linked to the auditee’s financial statements.

To systematically build a better approach to process auditing in an ERP environment, it is important to understand the way process audits are carried out at present. A closer look at current audit practice reveals two major shortcomings:

1. For complex audit assignments such as process audits, primarily manual audit procedures are employed. The manual survey of as-is processes by interviews/inquiries or sample-based inspections of control evidence documentation are common examples. This circumstance is particularly surprising in light of the fact that almost all audit-relevant data are available in the entity’s IT environment. For audit purposes, IT tools are preponderantly used for single audit steps. For instance, IT-based data analyses are applied for substantive testing to identify conspicuous business transactions (e.g., SAS 99). However, in current practice, a comprehensive view on IT support is seldom taken, especially not for complex audit tasks like process audits.

2. Although business processes and IT are highly intertwined on the client side, auditors typically do not use an integrated audit approach. Processes and IT are audited separately by different auditors who are organized in different departments. Results are integrated but not before the reporting step of the assignment. All this happens even though an integrated approach for process and IT audit has been proven to be more efficient (saves time) and effective (a more comprehensive audit plan, more likely to identify risk exposures).

What deters auditors from overcoming these shortcomings with the help of IT? How is an IT-based, data-driven and integrated audit procedure composed to make the difference?

DATA-DRIVEN APPROACH TO PROCESS UNDERSTANDING

In the course of a process audit (figure 1), an auditor essentially has to answer four questions:

1. Which process (variants) does he/she have to audit (scoping)?
2. In which variants was the process enacted during the period under audit (walk-through)?
3. Which control means were effectively in place (internal controls [IC] testing)?
4. What is the overall audit result for the process (reporting)?

Phase 2, the walk-through, is the first potential area for automation. The domain of process mining provides a set of techniques to discover real processes by extracting knowledge from recordings of past process executions (e.g., SAS 99). However, in current practice, a comprehensive view on IT support is seldom taken, especially not for complex audit tasks like process audits.

Although business processes and IT are highly intertwined on the client side, auditors typically do not use an integrated audit approach. Processes and IT are audited separately by different auditors who are organized in different departments. Results are integrated but not before the reporting step of the assignment. All this happens even though an integrated approach for process and IT audit has been proven to be more efficient (saves time) and effective (a more comprehensive audit plan, more likely to identify risk exposures).

What deters auditors from overcoming these shortcomings with the help of IT? How is an IT-based, data-driven and integrated audit procedure composed to make the difference?
to human error and based on data that are independently recorded from the auditee.\textsuperscript{5, 6}

However, using traditional process mining techniques in ERP environments is still a challenge. Common ERP systems (e.g., SAP, Oracle, Microsoft) are not process-oriented.\textsuperscript{7} Data that relate to particular steps of a process execution are spread across several database tables without readily providing a process-oriented link (case identifier). Hence, process mining on ERP data demands comprehensive preprocessing.

Against this background, financial process mining (FPM) was developed. It uses links between financial documents to reconstruct single-process instances.\textsuperscript{8} These links stem from fundamental accounting principles (e.g., open-item accounting) and, therefore, are available in diverse types of ERP systems. With this, all documents belonging to a particular business transaction can be automatically identified. In this regard, a business transaction—for instance, the purchase of a specific raw material—comprises several documents, from a purchase order over the goods receipt and the invoice to the payment of the vendor. These documents can be easily mapped to well-defined activities in the purchase-to-pay (P2P) process.

Based on the full set of process instances executed throughout the period under audit, a complete process model is derived by applying common process-mining techniques. Such a process model helps to get a general understanding of what has actually happened in the auditee’s business processes. Attaching the frequency of occurrence to activities enables a convenient identification of standard process flows as well as outliers. Furthermore, a drill-down to single-process instances allows for a detailed analysis of conspicuous business transactions. \textbf{Figure 2} provides an example of a process model and a corresponding process instance for the P2P cycle. The process model is derived with the process-mining software Disco.\textsuperscript{9}

The financial-document-based mining of business processes provides another advantage for auditors. The financial perspective of a process is readily available on the process model and process instance levels. This allows for a detailed analysis of the impact each process activity, each process instance and, in aggregation, each process has on specific financial accounts. The right portion of \textbf{Figure 2} includes this financial perspective in the style of t-accounts, with which auditors and accountants are familiar.\textsuperscript{10} Such detailed information on the financial impact of processes enables a new way of materiality-based scoping. So far, auditors have been mostly forced to apply a “rule of thumb” when deciding which process variants to audit for particular accounts. For instance, in a case in which the liability accounts are identified as material, the P2P cycle is usually audited. However, it is not immediately apparent for the auditor which process variants exist for the P2P cycle and to what extent each variant contributes to the balance of the material accounts. With FPM, a process model can be derived that is based only on process instances touching the in-scope accounts above a specified amount. Until now, such a deep connection between financial statements and business processes was not available for auditors.\textsuperscript{11}

\textbf{Automatically Evaluating Internal Controls}

As a result, FPM establishes a detailed and pinpointed basis for process analysis, namely the end-to-end process instance, including a direct link to the financial statements. Based on such detailed information, several internal-control-related aspects can be reviewed immediately at the process and instance levels. The analysis of the process structure reveals conspicuous, unexpected or noncompliant business transactions. Deviations from a defined standard process or applicable regulatory requirements, as well as missing process activities (e.g., approval steps for each purchase order and/or invoice), incorrect ordering of activities (e.g., payment before an invoice is received) and segregation-of-duty conflicts can be easily identified. For instance, in the left portion of \textbf{Figure 2}, it is apparent that 42 goods receipts were posted without a corresponding purchase order. This should not be the case in a well-organized purchasing process. This kind of analysis can be performed either manually or automatically by applying conformance- and rule-based checking techniques.\textsuperscript{12, 13} In the aggregate, the auditor obtains a clear overview of what has actually happened in the process under audit.

Over and above this, current ERP systems and accounting information systems (AIS) offer a wide range of audit-relevant customizing settings, collectively referred to as application controls (ACs).\textsuperscript{14} Common examples for this type of control means are checks for duplicate invoices, the reconciliation of totals after processing a batch of payments or restricting/separating access to sensitive system functions.\textsuperscript{15, 16} ACs can be audited by directly reviewing the corresponding
customizing settings in the system. However, this review requires an in-depth knowledge of the particular ERP system and may involve a set of interlinked settings for a single AC. Hence, this review is often done by IT auditors and not by process auditors. As the corresponding settings are electronically stored in the systems, they can also be analyzed automatically. In academia, a few software solutions are discussed that operate independently from a particular ERP system and enable such an automated evaluation of ACs from an audit perspective. As result, these solutions provide a report that includes the current settings of relevant ACs; a description of the ACs; a risk estimation based on default values; and, in case of deviations, recommendations for improvement. Thereby, these solutions hide the technical details from the auditor. Figure 3 depicts such an automatically generated report on three ACs from a SAP ERP.

In addition to the current settings, ERP systems maintain a log of changes to relevant settings including the change date, old value and new value of the parameter. The analysis of this log allows reconstructing the AC settings for each point in time throughout the audit period.

INTEGRATING RESULTS OF IT AND PROCESS AUDIT

A good approach to leveraging the previous results (process model/process instances and internal controls analysis) is the seamless integration of process instances and process-dependent internal controls. The integrated business process model forms the focal point of a process audit. The automated approach for integration is based on the relationship between ACs and particular process activities in the form of functional modules in the ERP system (e.g., transaction codes in SAP ERP). For instance, a check for duplicate invoices is performed before or after process activities that involve invoice processing.
Figure 4 depicts the process model from figure 2 enriched with information on two ACs (double invoice check and payment block removal). Depending on the list of related process activities/functional modules, the nature of the control (preventive, detective) and the status of the AC settings (active, inactive), the ACs are added as a special process activity. In doing so, the structure of an enriched process model shows whether ACs were appropriately activated throughout the period under audit. For instance, in figure 4, there are business transactions for which the invoices were not checked for duplicates (all invoices that were created with the functional module MR01—Process Incoming Invoice). A drill-down displays the corresponding business transactions for a more detailed review. In contrast, for the remaining invoices (FB60—Enter Incoming Invoices) duplicates are prevented by an AC. In addition, for all invoices, the removal of a payment block during payment processing is prevented. In general, with the approach described previously, ACs as well as manual control means can be added to process instances or models.

Accordingly, with the enhanced process model, new process variants are derived enabling the auditor to better analyze process variants according to their risk and control scheme. The auditor is able to focus on business transactions that are less controlled and, therefore, are subject to a higher risk of (un)intended errors.

Again, these analyses on internal controls can be performed either manually or automatically by applying conformance- and rule-based checking techniques. Unmitigated risk, unaddressed control objectives or missing control means are available at the click of a button.

**Figure 3—Internal Controls Report**

<table>
<thead>
<tr>
<th>Status</th>
<th>Assessment</th>
<th>Test Title</th>
<th>Test Description</th>
<th>Default</th>
<th>Current</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OK</td>
<td>Check duplicate invoice</td>
<td>The rule checks if the system detects and blocks duplicate invoice posting.</td>
<td>“E”</td>
<td>“E”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Three-way match</td>
<td>The rule checks if a three-way match between PO, GR and INV is in place.</td>
<td>“W”</td>
<td>“E”</td>
<td>Message type for three-way match should be adjusted.</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Payment block removal</td>
<td>The rule checks if a removal of the block-flag without further approvals is prevented.</td>
<td>Null</td>
<td>“X”</td>
<td>The setting for payment block should be changed.</td>
</tr>
</tbody>
</table>

**Figure 4—Enriched Process Model**
SUBSTANTIALLY AUDIT ONLY THE INTERESTING STUFF
Automated analyses on multiple aggregation levels (process activity, process instance, process model, financial account) help to focus on the most relevant audit issues. Integrating various perspectives helps to draw a complete picture. To do so:
• Identify unusual process sequences in a process model.
• Analyze conformance to standard processes and compliance requirements.
• Detect insufficiently controlled process variants and process instances.
• Pinpoint actual segregation-of-duty conflicts on the process instance level.
• Filter on particular material financial accounts, divisions or departments.

Based on these individual indicators, an overall risk score can be computed for each process instance—and in aggregation for each process variant and even in total for a financial account or an arbitrary list of accounts. A drill-down back and forth allows for diving into details or setting a particular finding in its broader context. Compared to traditional solely document-based data analyses, such an integrated view drastically reduces the number of false-positives.

USE CASE EXAMPLE
At present, the described approach for IT-based process audits is implemented at the University of Hamburg (Germany) as a software prototype called App2Audit. Figure 5 gives a rough impression of the targeted user interface. The aim of the prototype is to show that for complex audit assignments, a comprehensive software support is feasible and auditors benefit from an integrated view on diverse data analyses.
CONCLUSION
As demonstrated, comprehensive IT support gives auditors the opportunity to better utilize their time for value-added and high-risk tasks.\textsuperscript{21, 22} In light of the increasing complexity of auditees’ business processes and the vast amount of audit-relevant data, it is crucial to be able to render audit assignments in an effective and efficient way. Of course, human auditors cannot completely be replaced by automated approaches, thus final audit assessments should undergo a professional judgment. However, in current audit practice there is significant room for improvement for an extended usage of IT support in the preparation phase of an audit. Auditors can leverage different IT-based analysis opportunities. As a result, such a comprehensive usage of IT may completely change the way audits are executed.

ENDNOTES
\begin{itemize}
\item[3] Ibid.
\item[9] Fluxicon, Disco, 2013, \url{http://fluxicon.com/disco/}
\item[15] Bellino, C.; J. Wells; S. Hunt; \textit{Global Technology Audit Guide (GTA) 8: Auditing Application Controls}, 2007
\item[16] ISACA, \textit{COBIT and Application Controls: A Management Guide}, 2009, \url{www.isaca.org}
\item[21] Op cit, Omoteso
\end{itemize}
Internal Audit’s Contribution to the Effectiveness of Information Security (Part 2)

Perceptions of Internal Auditors

In “Internal Audit’s Contribution to the Effectiveness of Information Security (Part 1): Perceptions of Information Security Professionals,” published in the ISACA Journal, volume 2, 2014, research results are presented from a study of information security professionals’ perceptions about the factors that affect the quality of the relationship between the internal audit and the information security functions and the outcomes associated with that relationship. The examination and evaluation of the internal auditors’ views on these issues is the focus here.

The findings reported here are from a web-based survey of internal auditors. As figure 1 shows, most respondents to the survey possessed the Certified Information Systems Auditor® (CISA®) certification and had more than 10 years of work experience. About half worked in large, public, for-profit organizations and the remainder worked for privately held or nonprofit enterprises. Slightly more than 40 percent of respondents worked in the financial services sector, with the remainder representing a wide variety of industries.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respondent gender:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Male</td>
<td>29</td>
<td>67%</td>
</tr>
<tr>
<td>• Female</td>
<td>14</td>
<td>33%</td>
</tr>
<tr>
<td>Respondent age:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Under 40</td>
<td>18</td>
<td>43%</td>
</tr>
<tr>
<td>• 40 or older</td>
<td>25</td>
<td>57%</td>
</tr>
<tr>
<td>Respondent certifications (could be multiple):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• CPA/CA</td>
<td>7</td>
<td>16%</td>
</tr>
<tr>
<td>• CISA</td>
<td>34</td>
<td>79%</td>
</tr>
<tr>
<td>• CISM®</td>
<td>8</td>
<td>19%</td>
</tr>
<tr>
<td>• CIA</td>
<td>6</td>
<td>14%</td>
</tr>
<tr>
<td>• CISSP</td>
<td>3</td>
<td>7%</td>
</tr>
<tr>
<td>• None</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>• Other (CRISC™, CGEIT®, etc.)</td>
<td>17</td>
<td>40%</td>
</tr>
<tr>
<td>Respondent total work experience (years):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 10 or less</td>
<td>11</td>
<td>26%</td>
</tr>
<tr>
<td>• 11-20</td>
<td>18</td>
<td>43%</td>
</tr>
<tr>
<td>• More than 20</td>
<td>13</td>
<td>31%</td>
</tr>
<tr>
<td>(Note: One person did not respond to this question.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respondent work experience with current employer (years):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 10 or less</td>
<td>30</td>
<td>67%</td>
</tr>
<tr>
<td>• More than 20</td>
<td>13</td>
<td>33%</td>
</tr>
<tr>
<td>Nature of organization:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Publicly traded for-profit</td>
<td>21</td>
<td>49%</td>
</tr>
<tr>
<td>• Privately held for-profit</td>
<td>14</td>
<td>33%</td>
</tr>
<tr>
<td>• Nonprofit</td>
<td>8</td>
<td>18%</td>
</tr>
<tr>
<td>Industry:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Government</td>
<td>3</td>
<td>7%</td>
</tr>
<tr>
<td>• Manufacturing</td>
<td>1</td>
<td>2%</td>
</tr>
<tr>
<td>• Financial services</td>
<td>18</td>
<td>42%</td>
</tr>
<tr>
<td>• Technology</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>• Health care, education and other professional services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mining and construction</td>
<td>3</td>
<td>7%</td>
</tr>
<tr>
<td>• Other</td>
<td>5</td>
<td>11%</td>
</tr>
</tbody>
</table>

Do you have something to say about this article? Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.
FACTORS AFFECTING THE RELATIONSHIP BETWEEN INTERNAL AUDIT AND INFORMATION SECURITY

The part 1 article reported that information security professionals considered two factors to be important drivers of the quality of their relationship with the internal audit function: their perceptions about the level of internal audit’s information security knowledge and the frequency of interaction (audit review). The survey of internal auditors collected information about certifications as a way of measuring their information security knowledge. Statistical analysis did not show a significant connection between such objective measures and the perceived quality of the relationship between the two functions. This may be due to the fact that the overwhelming majority of respondents possessed the CISA and also had more than 10 years of work experience. Thus, there was little variation in knowledge across respondents.

Figure 2 shows that internal auditors, like information security professionals, believe that it is important to frequently review different components of information security. However, the specific aspects of security being reviewed have different outcomes. More frequent reviews of the aspects of information security that involve interactions between the information security function and other parts of the organization (identity and access management [IAM] controls, backup procedures, security policies, and change management) have a positive effect on the overall quality of the relationship between the internal audit and information security functions and also lead to a subsequent increase in the number of audit findings. More frequent review of the technical aspects of information security (encryption, firewalls, logging and business continuity/disaster recovery) also results in more audit findings, but does not affect the quality of the relationship between the audit and security functions.

These results make sense. The survey of information security professionals (reported in part 1 of this series) found that the quality of the relationship between the internal audit and information security functions was positively related to information security professionals’ perceptions about the value added by internal audit. The interviews with information security professionals revealed that they perceived one of the biggest benefits resulting from a good relationship with internal audit was support for desired information security initiatives.

“I think the partnership kind of helps with that escalation. [The internal auditor] was able to take that [data privacy issues] to his one-on-one meeting with the CEO and then, in very short order, policies were changed.”1 In other words, information security professionals saw internal audit as a potential ally or partner when interacting with end users and management. The four areas for which more frequent audit reviews resulted in better relationships all deal with aspects of the information security program that involve areas outside the information security function.

Identity and access controls involve end-user behaviors. Backup procedures are typically performed by IT staff or are sometimes the responsibility of end users; thus, in many instances, those procedures are not performed by information security professionals. Security policies should be designed with input from end users and management, but their functioning is dependent on individuals outside of information security. Change management affects many functions and is usually the responsibility of business process owners, and again, is outside of the direct responsibility of information security. Therefore, it appears that the quality of the relationship between internal audit and information security improves when internal auditors focus on the areas in which information security professionals perceive that they must need support to implement their initiatives.

In contrast, responsibility for the other four areas is primarily internal to the information security function. Firewall configuration, review and operation are the responsibility of information security. Similarly, logging is a task assigned to information security as are decisions about the strength and nature of encryption. Finally, while disaster recovery and business continuity plans do use input from various business executives and senior management, the development and the testing of these plans is usually assigned to information security personnel. Thus, audit reviews of these four areas are primarily a binary relationship between the auditor and the information security function. The fact that the frequency of such reviews has no effect on the quality of the relationship is not surprising. Indeed, it is good news that it is not negative, indicating that at least internal audit’s review of these more technical aspects of information security does not create an adversarial relationship.

Figure 3 shows internal auditors’ and information security professionals’ responses to questions about how often they reviewed eight aspects of information security on a five-point scale with higher scores representing more frequent reviews. The two sets of data come from different surveys, with respondents belonging to different organizations. Thus, they cannot be directly matched. However, comparison of the two sets of responses yields two interesting patterns.

First, the relative rank ordering is quite similar: What auditors say they do matches what information security professionals think auditors do. Second, for all eight topics, information security professionals’ scores are lower than those of internal auditors. The latter suggests that either information security professionals may not be fully aware of the extent of internal auditors’ activities related to information security or that the perceptions about what constitutes a review are different. Because information security professionals and auditors agree that an increased frequency of audit review improves the quality of the relationship between the two functions, this discrepancy represents a communications gap that needs to be addressed.

### BENEFITS FROM A GOOD RELATIONSHIP BETWEEN INTERNAL AUDIT AND INFORMATION SECURITY

The part 1 article reported that information security professionals believe that a positive relationship with internal audit improves both their perceptions about the value of internal audit findings and also improves overall effectiveness of information security by making it easier to get top management to support efforts to increase employees’ compliance with policies and the institution of improved security measures. In contrast, Figure 2 shows that internal auditors did not think that the quality of their relationship with information security directly affected outcomes, as measured by the number of incidents or audit findings. From one perspective, this can be seen as good news in that the quality of the relationship with the auditee does not affect audit findings. This may also be good news in that it may reflect the independence of internal audit in reviewing information security. However, it also indicates that respondents did not think that a better relationship with information security helped improve audit efficiency or effectiveness because the auditee, instead of trying to hide information, was forthcoming about higher risk areas in need of remediation.

Auditors did, however, think that the frequency of audit reviews of information security affected audit findings. The results show that increasing the frequency of audit reviews results in an increased number of audit findings.

One explanation for these results is that the four most frequently reviewed aspects of information security are primarily people- and process-driven and involve interaction

---

### Figure 3—Areas Reviewed and the Frequency of the Review

<table>
<thead>
<tr>
<th>Security Topic</th>
<th>Internal Audit</th>
<th>Information Security</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Review Areas</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Encryption policies (including key management)</td>
<td>3.77 (4.0)</td>
<td>2.72 (3.0)</td>
<td>1-5</td>
</tr>
<tr>
<td>• Business continuity and disaster recovery</td>
<td>3.44 (3.0)</td>
<td>2.72 (3.0)</td>
<td>1-5</td>
</tr>
<tr>
<td>• Logging and system monitoring</td>
<td>3.26 (3.0)</td>
<td>2.56 (3.0)</td>
<td>1-5</td>
</tr>
<tr>
<td>• Firewalls and other network access devices</td>
<td>2.88 (3.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Interaction Review Areas</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Identity and access management</td>
<td>4.07 (4.0)</td>
<td>3.17 (3.0)</td>
<td>1-5</td>
</tr>
<tr>
<td>• Change management controls</td>
<td>4.02 (4.0)</td>
<td>3.00 (3.0)</td>
<td>1-5</td>
</tr>
<tr>
<td>• Security policies</td>
<td>3.88 (4.0)</td>
<td>3.28 (3.5)</td>
<td>1-5</td>
</tr>
<tr>
<td>• Backup procedures</td>
<td>3.49 (4.0)</td>
<td>3.00 (3.0)</td>
<td>1-5</td>
</tr>
</tbody>
</table>

Note: One being not at all; five being often
with people and functions outside the information security function. Thus, they are amenable to continuous improvement. Once areas for improvement are identified and remediation efforts implemented, subsequent reviews can dig deeper to find additional ways to further improve security. The same argument applies to audit reviews of the other four more technical topics that less directly involve employees outside the information security function.

Security is a moving target. Once defenders mitigate existing vulnerabilities, attackers find new methods to try to compromise the system. In addition, systems and business processes continually change. Change always creates the possibility for new vulnerabilities that must be discovered and addressed.

Auditors were also asked about the current level and trends in the number of security incidents and audit findings related to security at their employer. Figure 4 shows that, overall, internal auditors thought their employers were doing a satisfactory job on information security, but that there is room for improvement (mean responses to all four questions are above the midpoint, but well below the maximum). Examining the professional literature reveals that other internal auditors have similar perceptions about information security.2,3

In both surveys, respondents were asked to assess top management’s level of support for information security. Figure 5 shows the questions asked and the results. The first four questions ask about management’s current level of support, and the last four questions ask about the trend in that support. The results demonstrate that both information security professionals and internal auditors see the need for increased management support for information security initiatives. From the perspective of the three lines of defense,4 this result is additional confirmation that even without direct involvement, top management must play a supportive role for information security efforts to be effective.

### Figure 4—Effectiveness of Information Security

<table>
<thead>
<tr>
<th>Effectiveness of Information Security</th>
<th>Mean (Median)</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents (past year)</td>
<td>5.40 (6.00)</td>
<td>1-7</td>
</tr>
<tr>
<td>Trend in incidents (past three years)</td>
<td>3.42 (4.00)</td>
<td>1-6</td>
</tr>
<tr>
<td>Audit findings related to information security (past year)</td>
<td>4.30 (4.00)</td>
<td>1-7</td>
</tr>
<tr>
<td>Trend in audit findings (past three years)</td>
<td>3.30 (3.00)</td>
<td>1-6</td>
</tr>
</tbody>
</table>

Note: Higher scores are better. Responses for incidents and audit findings in past year ranged from more than 25 (score of 1) to zero (score of 7), in increments of five. Responses to the trend questions ranged from significantly increased (score of 1) to significantly decreased (score of 5) and did not have any findings or incidents (score of 6).

### Figure 5—Top Management Support

<table>
<thead>
<tr>
<th>Top Management Support for Information Security</th>
<th>Mean (Median)</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>In my organization, top management provides adequate resources for information security.*</td>
<td>3.33 (4.00)</td>
<td>1-5</td>
</tr>
<tr>
<td>In my organization, top management regularly communicates with employees about the importance of information security.*</td>
<td>3.21 (4.00)</td>
<td>1-5</td>
</tr>
<tr>
<td>In my organization, top management believes that information security is an important issue.*</td>
<td>3.79 (4.00)</td>
<td>1-5</td>
</tr>
<tr>
<td>In my organization, top management is more proactive as opposed to reactive with respect to information security issues.*</td>
<td>3.05 (3.00)</td>
<td>1-5</td>
</tr>
<tr>
<td>Considering the past three years, I think top management’s commitment to providing adequate resources for information security has….**</td>
<td>3.56 (4.00)</td>
<td>1-5</td>
</tr>
<tr>
<td>Considering the past three years, I think top management’s communication of the importance of information security issues has….**</td>
<td>3.45 (3.00)</td>
<td>1-5</td>
</tr>
<tr>
<td>Considering the past three years, I think top management’s view of the importance of information security has….**</td>
<td>3.51 (4.00)</td>
<td>1-5</td>
</tr>
<tr>
<td>Considering the past three years, I think top management’s anticipation of information security issues has….**</td>
<td>3.43 (3.00)</td>
<td>1-5</td>
</tr>
</tbody>
</table>

* Responses to these questions range from 1 (strongly disagree) to 5 (strongly agree).
** Responses to these questions range from 1 (significantly decreased) to 5 (significantly increased).
Yet in practice, these two functions do not always have a harmonious relationship. To further understand the factors affecting this relationship and the benefits accruing to organizations with positive relationships, multiple studies were conducted. Part 1 in this series of articles reported information security professionals’ perspective on these issues and part 2 provides internal auditors’ views. The studies indicate two important conclusions.

First, information security professionals and internal auditors agree that more frequent interaction between the two functions improves the quality of their relationship. Furthermore, there are organizational benefits to more frequent interaction. There is room for improvement. Both information security professionals and internal auditors report that many areas of information security are not reviewed as often as they could be. One reason may be the lack of resources.

Second, both information security professionals and internal auditors agree that top management could do more to support the organization’s information security efforts. This result is consistent with professional and academic literature and emphasizes the importance of top management in the overall effectiveness of organizational control. This may be particularly important in the areas of information security that must rely on individuals outside the information security department for compliance and improvement.

Finally, a conclusion from the part 1 article is worth reinforcing: Information security personnel place importance on the knowledge that internal auditors have about information security.

ENDNOTES
2 Ross, Steven J.; “Just Okay Practice,” ISACA Journal, vol. 2, 2013, p. 4-5. This article indicates that organizations should strive not to be like everyone else, but to implement the strongest security.
5 ISACA, COBIT 5, USA, 2013, p. 29 and 80, www.isaca.org/cobit
6 ISACA, COBIT 5 Implementation, USA, 2012, p. 72, www.isaca.org/cobit
ACROSS
1. Sophisticated cyberattack on Google in 2010, Operation _____
4. It was classified in 2010 as “the world’s most advanced malware”
8. Name given to a kind of statistical chart
9. Fine-___, honed
13. See 22 down
15. Completely
16. ___ant, point of view
17. City in Italia
19. Locates the source
20. Deviation from the normal: It is something big data can detect using longer and broader analysis of data.
24. Intense
26. Soft white cheese
27. Computer shortcut
29. Coding
30. Unprocessed, as data
32. Prevent
35. Kilowatts per hour, abbr.
36. Analyzed
37. Computer science expert who demonstrated that the intrusion detection problem is NP-Hard, Paul _____
39. Job function
40. Branch of computer science that deals with writing programs that solve problems, abbr.
41. Customer service caller
43. Temporal focus of most current intrusion detection systems (2 words)
46. Fail to retain
48. “State of the art” malware introduced in 2012
49. Guilt acknowledgment, with mea
50. Programming language
51. Kind of file
52. Remove viruses from a system
53. Spooled

DOWN
1. Acronym for sophisticated and enduring threats
2. ___ command
3. Very advanced malware introduced in 2012-13 (2 words)
4. Most widely used approach to intrusion detection is ___ based
5. Drink with lemon and ice
6. Confidentiality agreement, for short
7. Keep score
10. Very
11. Timescale section
12. ___ totaling software, can be used to check for correctness and security of data in a trusted image
14. Investigate
18. Yours truly
21. Form of address
22. Name for a remote data center used to recover from a cyberattack (goes with 13 across)
23. Assange action
25. Word of choice
27. Plan out in detail
28. Bear a reciprocal or mutual connection
31. “Ethical” computer hacker (2 words)
33. The makers of PDFs
34. ___-accompli
37. Marine pronoun
38. Evil program
42. CD ___
44. Swiss mathematician
45. An exact copy, in computing
47. Observed
48. Acronym for a specific device for capturing and archiving network traffic
49. In early 2014, ISACA announced its program for this ethical aspect of corporate activity, abbr.

(Answers on page 58)
1. SCADA systems are smart, intelligent control systems that acquire inputs from a variety of sensors and, in many instances, respond to the system in real time.

2. Control systems can tolerate occasional failures, insecure sites and little separation among intranets, and have a lifetime of three to five years.

3. An ideal SCADA security framework should have characteristics that include meeting the availability, risk management and performance requirements of SCADA systems.

4. Most of the industries where SCADA systems are in use are heavily regulated. A well-designed compliance framework allows an organization to meets its compliance requirements.

5. The foremost priority for SCADA systems is to ensure the confidentiality of system data.

6. A report by the US Patent and Trademark Office published in 2010 estimated US $5.06 billion in value added, or 3.4 percent of US gross domestic product (GDP) generated, by IP-intensive industries in the US.

7. Data loss prevention (DLP) technology solutions focus on accidental or malicious data losses, primarily from external sources.

8. DLP solutions should be considered as part of an overall information security mechanism and data protection strategy.

9. Events triggered from DLP policies provide useful insight on where, when and how the sensitive data are stored and handled within the organization.

10. COBIT® 5 goes beyond “old style” frameworks that are based on domains, checklists, control objectives and measures.

11. The COBIT 5 and framework describes seven categories of enablers including processes and information.

12. Governance runs the organization, while management sets policy, exercises oversight and strategically guides the organization.

13. Although migrating to COBIT 5 brings other benefits, it does not help with compliance with EU accreditation criteria.

14. 4G LTE is expected to exceed US $340 billion in service revenues by 2017.

15. Risk management can manage only external attacks and cannot manage inherent security risk and vulnerabilities.

16. Aside from the high-bandwidth user traffic, signalling traffic on LTE is estimated to be 40 percent higher per LTE subscriber than on 3G networks.

17. Tokenization strings are surrogates used to uniquely identify a piece of data and contain no information beyond the token.

18. Before a token is generated, it is not necessary to decide whether the token will be used once or several times.
**ISACA Journal**  
**CPE Quiz**  
**Based on Volume 1—Data Privacy**

**Quiz #154 Answer Form**

(Please print or type)

Name _____________________________________________

__________________________________________________

Address ____________________________________________

__________________________________________________

__________________________________________________

CISA, CISM, CGEIT or CRISC # ____________________________

---

**Quiz #154**

**True or False**

**MALAVIYA ARTICLE**

1. _______

2. _______

3. _______

4. _______

5. _______

**ARCIDIACONO ARTICLE**

10. _______

11. _______

12. _______

13. _______

14. _______

**KUMARESAN ARTICLE**

6. _______

7. _______

8. _______

9. _______

**BHASKER ARTICLE**

15. _______

16. _______

17. _______

18. _______

**BEISSEL ARTICLE**

17. _______

18. _______

---

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

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

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

You are responsible for submitting your credit hours at year-end for CPE credits. A passing score of 75 percent will earn one hour of CISA, CISM, CGEIT or CRISC CPE credit.

---

**Answers—Crossword by Myles Mellor**  
See page 56 for the puzzle.
ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

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

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

ITAF™, 2nd Edition (www.isaca.org/itaf) provides a framework for multiple levels of guidance:

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

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

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

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

Please note that the guidelines are being revised and comments from public exposure are being addressed. The new guidelines are scheduled to be issued in the third quarter of 2014.

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

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

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

Editor
Deborah Oetjen

Senior Editorial Manager
Jennifer Hajigorgiou
publication@isaca.org

Contributing Editors
Sally Chan, CEGIT, CMA, ACIS
Kamal Khan, CISA, CISSP, CITP, MBCS
Vasant Raval, DBA, CISA
Steven J. Ross, CISA, CBCP, CISSP
Tommie Singleton, Ph.D., CISA,
CCEIT, CPA
B. Ganapathi Subramaniam, CISA, CIA,
CISSP, SSCP, CCNA, CCSA, BS 7799 LA
Smita Totade, Ph.D., CISA, CISM, CEGIT, CRISC

Advertising
media@isaca.org

Media Relations
news@isaca.org

Editorial Reviewers
Matt Allman, CISA, CISM, CGEIT, CRISC
Goutama Bachtiair, BCP, BCP, HPCP
Brian Barnier, CEGIT, CRISC
Linda Betz, CISA
Pascal A. Bizarro, CISA
Jerome Capriossi, CISA
Cassandra Chasnis, CISA
Ashwin K. Chaudary, CISA, CISM, CGEIT, CRISC
Reynaldo J. de la Fuente, CISA, CISM, CRISC
Christos Dimitriadias, Ph.D., CISA, CISM
Ken Doughty, CISA, CRISC, CBP
Nikesh L Dubey, CISA, CISM, CRISC, CISSP
Robert Findlay
Jack Freund, CISA, CISM, CRISC, CPP,
CISSP, PMP
Sailesh Gadia, CISA
Robin Generous, CISA, CPA
Anuj Goel, Ph.D., CISA, CGEIT, CRISC, CISSP
Manish Gupta, CISA, CISM, CRISC, CISSP
Jeffrey Hare, CISA, CPA, CIA
Jocelyn Howard, CISA, CISSP, CISSP
Francisco Ignal, CEGIT, CRISC
Jennifer Insore, CISSP
Timothy James, CISA, CRISC
Khwaja Faisal Javed, CISA, CRISC, CBCP,
ISMS LA
Keni Lemme-Moretti, CRISC
Romulo Lompata, CISA, CGEIT, CRISC
Juan Macias, CISA, CRISC
Larry Marks, CISA, CGEIT, CRISC
Norman Marks
David Earl Mills, CISA, CGEIT, CRISC, MCSE
Robert Moeller, CISA, CISSP, CPA, CSQE
Aureo Monteiro Tavares Da Silva, CISA, CISM, CGEIT
Ramu Muthiah, CISM, ITIL, PMP
Gretchen Myers, CISSP
Ezekiel Dementio J. Navarro, CPA
Mathew Nicho, CEH, RWSP, SAP
Daniel Paula, CISA, CRISC, CISSP, PMP
Pak Lok Poon, Ph.D., CISA, CSQA, MIEEE
John Pouey, CISA, CISM, CRISC, CIA
Steve Primost, CISM
Haif Ramachandru, CIGEIT, TGAF
Parvathi Ramesh, CISA, CA
David Ramirez, CISA, CISM
Antonio Ramos Garcia, CISA, CISM, CRISC,
CDPP, ITIL
Ron Roy, CISA, CRP

LouiSa Saunier, CISP, PMP, Six Sigma
Green Belt
Nrupak D. Shah, CISM, CSK, CEH, ECSC ITIL
Sanddeep Sharma
Johannes Tekle, CISA, CFSA, CIA
Robert W. Theriot Jr., CISA, CRISC
Iliai Vadjon, CISA
Sadir Vanderfoot Sr., CISA, CISM, CCNA,
CCSA, NCSC
Ellis Wong, CISA, CRISC, CFE, CISSP

ISACA Board of Directors (2013–2014)

International President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS,
FCPA, FIA

Vice President
Allan Boardman, CISA, CISM, CGEIT, CRISC,
ACA, CA (SA), CISSP

Vice President
Juan Luis Canselle, CISA, CISM, CRISC

Vice President
Ramesh Gallego, CISM, CGEIT, CCSK, CISSP,
SCPM, Six Sigma Black Belt

Vice President
Theresa Grafenberg, CISA, CGEIT, CRISC,
CGAP, CGMA, CIA, CPA

Vice President
Vittal Raj, CISA, CISM, CGEIT, CFE, CIA,
CISSP, FCA

Vice President
Jeff Spivey, CRISC, CPP

Vice President
Marc Vael, CISA, CISM, CGEIT, CRISP, ITIL

Past International President, 2012–2013
Greg Grocholski, CISA

Past International President, 2011–2012
Kenneth L. Vander Wal, CISA, CPA

Director
Christos Dimitriadias, Ph.D., CISA, CISM, CRISC

Director
Kristen McCabe, CISA

Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC

Acting Chief Executive Officer
Ron Hale, Ph. D., CISM
BOOKSTORE
RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

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

New Books…
www.isaca.org/newbooks

Vendor Management: Using CobiT5 *
178 pages—CBSVM
Member $35.00 | NonMember $60.00

eBook—WCBSVM
Member FREE | NonMember $60.00

Computer Forensics InfoSec Pro Guide
512 Pages—34MCF
Member $40.00 | NonMember $50.00

Cloud Computing—Assessing the Risks
306 pages—17ITCC
Member $40.00 | NonMember $50.00

Cyber Attacks: Protecting National Infrastructure, Student Edition
336 pages—11EL2
Member $70.00 | NonMember $80.00

Featured…
www.isaca.org/featuredbooks

COBIT5: Enabling Information *
90 pages—CB5EI
Member $35.00 | NonMember $135.00

eBook—WCB5EI
Member FREE | NonMember $135.00

Executive’s Guide to IT Governance: Improving Systems
Processes with Secure Management, CobiT, and ITIL
416 pages—101WEG
Member $75.00 | NonMember $85.00

Crisp Practice Question Database 2014–12 Month Subscription *
XMXCR14-12M
Member $185.00 | Nonmember $225.00

Security Strategies in Windows Platforms and Applications,
2nd Edition
396 pages—3JBSS2
Member $102.00 | Nonmember $112.00

Securing Mobile Devices Using CobiT5 for Information Security *
100 pages—CB5SMD
Member $35.00 | Nonmember $75.00

eBook—WCB5SMD
Member FREE | Nonmember $75.00

System Forensics, Investigation, and Response, Second Edition
318 pages—2JBSF2
Member $102.00 | Nonmember $112.00

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

We are constantly expanding. Check out our new books and eBooks!
https://www.isaca.org/bookstore/Pages/New-Arrivals.aspx
Vendor Management: Using COBIT 5*

by ISACA

Vendors constitute an important part of an enterprise’s external environment. The increased use of outsourcing and cloud computing implies that vendors are taking on an increasingly fundamental role in the operations of an enterprise.

As the scope, scale and complexity of vendor relationships and services increase, the risk related to them and the importance of effective vendor management increase proportionately. Managing external vendors should be a key competency for every enterprise and can lead to optimally mitigated risk and significant benefits.

This publication describes the vendor management process and its activities and then presents the most common threats, risk and mitigation actions. A detailed case study is provided to show the potential consequences of faulty vendor management. Practical sample templates and checklists are also provided to help during implementation of the concepts presented in this publication. 2014, 178 pages

Print Format—CB5VM  Member $35.00  Nonmember $60.00  eBook—WCB5VM  Member FREE  Nonmember $60.00

Computer Forensics InfoSec Pro Guide

by David Cowen

Find out how to excel in the field of computer forensics investigations. Learn what it takes to transition from an IT professional to a computer forensic examiner in the private sector.

Written by a Certified Information Systems Security Professional, Computer Forensics: InfoSec Pro Guide is filled with real-world case studies that demonstrate the concepts covered in the book. You’ll learn how to set up a forensics lab, select hardware and software, choose forensic imaging procedures, test your tools, capture evidence from different sources, follow a sound investigative process, safely store evidence, and verify your findings. Best practices for documenting your results, preparing reports, and presenting evidence in court are also covered in this detailed resource. 2012, 512 Pages

Print Format—34MCF  Member $40.00  Nonmember $50.00

Cloud Computing—Assessing the Risks

by Jared Carstensten, Bernard Golden and JP Morgenthal

Using jargon-free language and relevant examples, analogies and diagrams, it is an up-to-date, clear and comprehensive guide the security, governance, risk, and compliance elements of Cloud Computing. Written by three internationally renowned experts, this book discusses the primary concerns of most businesses leaders—the security and risk elements of the Cloud. But ‘security and risk’ are just two elements of Cloud Computing, and this book focuses on all the critical components of a successful cloud programme including: compliance, risk, reliability, availability, areas of responsibility, Cloud Computing borders, legalities, digital forensics and business continuity. This book covers them all. 2013, 306 pages

Print Format—17ITCC  Member $40.00  Nonmember $50.00

Cyber Attacks: Protecting National Infrastructure, Student Edition

by E. Amoroso

This textbook offers a technical, architectural, and management approach to solving the problems of protecting national infrastructure and includes practical and empirically-based guidance for students wishing to become security engineers, network operators, software designers, technology managers, application developers, Chief Security Officers, etc.. This approach includes controversial themes such as the deliberate use of deception to trap intruders. In short, it serves as an attractive framework for a new national strategy for cyber security. Each principle is presented as a separate security strategy, along with pages of compelling examples that demonstrate use of the principle. A specific set of criteria requirements allows students to understand how any organization, such as a government agency, integrates the principles into their local environment. 2012, 336 pages

Print Format—11EL2  Member $70.00  Nonmember $80.00

* Published by ISACA and ITGI  ISACA member complimentary download www.isaca.org/downloads  All prices are listed in US Dollars and are subject to change
**NEW/FEATURED BOOKS**

**CISA Review Manual 2014**

*by ISACA*

The CISA® Review Manual 2014 is a comprehensive reference guide designed to help individuals prepare for the CISA exam and understand the roles and responsibilities of an information systems (IS) auditor. The manual has been enhanced over the past editions and represents the most current, comprehensive, peer-reviewed IS audit, assurance, security, and control resource available worldwide. The 2014 manual is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

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

2014, 434 pages

Print Format—CRM14

- Member $105.00
- Nonmember $135.00

**COBIT 5: Enabling Information**

*by ISACA*

Enterprises are experiencing increasing difficulty in maintaining control of their data to comply with legal and regulatory requirements. COBIT 5: Enabling Information is a reference guide that provides a structured way of thinking about information governance and management issues in any type of organization. This structure can be applied throughout the life cycle of information, from conception and design, through building information systems, securing information, using and providing assurance over information, and to the disposal of information. 2013, 90 pages

Print Format—CB5EI

- Member $35.00
- Nonmember $135.00

Ebook—WCB5EI

- Member FREE
- Nonmember $135.00

**Security Strategies in Windows Platforms and Applications, 2nd Edition**

*by Michael G. Solomon*

More than 90 percent of individuals, students, educators, businesses, organizations, and governments use Microsoft Windows, which has experienced frequent attacks against its well-publicized vulnerabilities. Revised and updated to keep pace with this ever changing field, Security Strategies in Windows Platforms and Applications, Second Edition focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. Particular emphasis is placed on Windows XP, Vista, and 7 on the desktop, and Windows Server 2003 and 2008 versions. It highlights how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. The book also includes a resource for readers desiring more information on Microsoft Windows OS hardening, application security, and incident management. With its accessible writing style, and step-by-step examples, this must-have resource will ensure readers are educated on the latest Windows security. 2014, 396 pages

Print Format—3JBSS2

- Member $102.00
- Nonmember $112.00

**Executive’s Guide to IT Governance: Improving Systems Processes with Secure Management, COBIT, and ITIL**

*by Robert R Moeller*

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

- Written by Robert Moeller, an authority in auditing and IT governance
- Practical, no-nonsense framework for identifying, planning, delivering, and supporting IT services to your business
- Helps you identify current strengths and weaknesses of your enterprise IT governance processes
- Explores how to introduce effective IT governance principles with other enterprise GRC initiatives
- Other titles by Robert Moeller: IT Audit, Control, and Security and Brink’s Modern Internal Auditing: A Common Body of Knowledge

2013, 416 pages

Print Format—101WEG

- Member $75.00
- Nonmember $85.00

* Published by ISACA and ITGI

ISACA member complimentary download www.isaca.org/downloads All prices are listed in US Dollars and are subject to change
Securing Mobile Devices Using COBIT 5 for Information Security *
by ISACA

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

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

The main purpose of applying COBIT 5 to mobile device security is to establish a uniform management framework and to give guidance on planning, implementing and maintaining comprehensive security for mobile devices in the context of enterprises. The secondary purpose is to provide guidance on how to embed security for mobile devices in a corporate governance, risk management and compliance (GRC) strategy using COBIT 5 as the overarching framework for GRC. 2012, 100 pages

System Forensics, Investigation, and Response, Second Edition
by Chuck Easttom

Computer crimes call for forensics specialists, people who know how to find and follow the evidence. System Forensics, Investigation, and Response, Second Edition begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field. 2014, 318 pages

CRISC Practice Question Database 2014—12 month subscription
by ISACA

The CRISC Practice Question Database—12 Month Subscription is a comprehensive 400-question pool of items that combine the questions from the CRISC Review Questions, Answers & Explanations Manual 2013 with those from the 2013 and 2014 editions of the CRISC Review Questions, Answers & Explanations Manual Supplement.

The database is available via the web, allowing our CRISC Candidates to log in at home, at work or anywhere they have Internet connectivity. The database is updated annually.

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.

* Published by ISACA and ITGI  ❙ ISACA member complimentary download www.isaca.org/downloads  All prices are listed in US Dollars and are subject to change.
Getting an ISACA® certification doesn’t just say you’re well read or well connected. It announces that you have the expertise and insight to speak with authority. The credibility that it adds lets you create value for your enterprise. Your certification is more than a credential, it’s a platform that can elevate your career.

Register at www.isaca.org/Sept14-Jv3

“I’M RECOGNIZED FOR MY CERTIFICATION.
I’M VALUED FOR WHAT I DO WITH IT.”

— KETAN DHOLAKIA, CISM, CRISC
MANAGING PARTNER, MACLEAR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2007

Getting an ISACA® certification doesn’t just say you’re well read or well connected. It announces that you have the expertise and insight to speak with authority. The credibility that it adds lets you create value for your enterprise. Your certification is more than a credential, it’s a platform that can elevate your career.

Register at www.isaca.org/Sept14-Jv3

UPCOMING EXAM DATE:
6 September 2014*
CISA and CISM only

Early registration deadline: 11 June 2014
Final registration deadline: 21 July 2014
Register early for an upcoming exam and save US $50!

*CISA and CISM only

*Held in select locations
Regis University's College of Professional Studies offers a graduate certificate as well as a master's degree in Information Assurance. With both programs, you have the option to take classes online or on campus. Our School of Computer and Information Sciences is also designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency.

### INFORMATION ASSURANCE PROGRAMS

**GRADUATE CERTIFICATE**
- Can be completed in less than a year
- Four classes (12 credit hours) - choose the courses that most interest you

**MASTER'S DEGREE**
- Two year program
- Specialize in cyber security or policy management

The curriculum is modeled on the guidelines and recommendations provided by:
- The Committee on National Security Systems (CNSS) 4000 training standards
- The (ISC)² Ten Domains of Knowledge
- ISACA

Classes can be taken on campus or completely online.

---

**Regis University** is an accredited, 130-year-old Jesuit institution in Denver, CO. Regis has been recognized as a national leader in education for adults and is committed to programs that are accessible and affordable. U.S. News & World Report has ranked Regis University as a Top University in the West for 19 consecutive years.