The IS Audit Transformation

Featured articles:
Auditing Oracle Databases Using CAATs
Auditing Cyberinsurance Policy
Internal Audit’s Contribution to the Effectiveness of Information Security
And more...
“MY CERTIFICATION OPENED NEW DOORS.
NOW I EASILY MOVE BETWEEN BUSINESS AND TECHNOLOGY.”

— TIMO HEIKKINEN, CISA, CGEIT
SENIOR AUDIT SPECIALIST, NORDEA HELSINKI, FINLAND ISACA MEMBER SINCE 1999

EXPAND YOUR POSSIBILITIES
Earning my ISACA certifications helped me gain the competence and experience that moved my career forward and eventually helped me reach my current position. My certification opened doors—and not just with IT. It gave me a link to the business side as well, expanding my level of responsibility, but also creating more possibilities.

Register at www.isaca.org/register14-Jv2

UPCOMING EXAM DATE: 14 June 2014
Final Registration Deadline: 11 April 2014
Register online and save US $75!
Let TeamMate CM 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.

Now Includes COBIT Content

To learn more call 888-830-5559 visit TeamMateSolutions.com/CM
VOLUME 2, 2014

Columns

4
Steven J. Ross, CISA, CISSP, MBCP

6
Information Security Matters: Shedding Tiers
Steven J. Ross, CISA, CISSP, MBCP

8
The Network
Ketan Dholakia, CISM, CRISC, CISSP

11
Information Ethics: The Piracy of Privacy
Vasant Raval, DBA, CISA, ACMA

14
IS Audit Basics: Risk to Entities Regarding Data Breaches
Tommie Singleton, CISA, CGEIT, CPA

Features

17
Book Review: IT Strategic and Operational Controls
Reviewed by Maria Patricia Prandini, CISA, CRISC
(Este libro también está disponible en español)

18
COBIT 5 Processes From a Systems Management Perspective
Myles Suer, Chane Cullens and Don Brancato

25
Auditing Oracle Databases Using CAATs
Ian Cooke, CISA, CFE, CGEIT-F, ITIL-F, Six Sigma Green Belt

29
Auditing Cyberinsurance Policy
Jide Olakunle, CISA, CISM, CISSP

33
Critical Information Systems Processes
Tugba Yildirim, CISA, CGEIT, CRISC, and Bilgin Metin, Ph.D.

37
The Effect of the COSO 2013 Update on IS Professionals
John H. White, Ph.D., CISA, CPA

42
Internal Audit’s Contribution to the Effectiveness of Information Security (Part 1)
Pau John Steinbart, Robyn Raschke, Graham Gal and William N. Billa, Ph.D., CPA

48
Why Computer Ethics Matters to Computer Auditing
Wanbil W. Lee, DBA

53
Vimal Mani, CISA, CISSP

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 1 April 2014.

The A to I Ways to Launch an IT Program or Information Security Project
Key Mak, CISM, CAP, CISSP, ITIL, PMP, Security Plus, ECMP

Communicating IT Governance—Does It Matter?
Giuliano Pozza

Security Policy—Keys to Successful Communication
James Baird, CISM, CISSP, ISO 27001 LI, ITIL (F)

Reinspecting Password, Account Lockout and Audit Policies
M. Faisal Naqvi, CISA, AMBCI, CISSP, ISO 27000 A, ISO 27000 M

COBIT 5 Processes From a Systems Management Perspective
Myles Suer, Chane Cullens and Don Brancato

Auditing Oracle Databases Using CAATs
Ian Cooke, CISA, CFE, CGEIT-F, ITIL-F, Six Sigma Green Belt

Auditing Cyberinsurance Policy
Jide Olakunle, CISA, CISM, CISSP

Critical Information Systems Processes
Tugba Yildirim, CISA, CGEIT, CRISC, and Bilgin Metin, Ph.D.

The Effect of the COSO 2013 Update on IS Professionals
John H. White, Ph.D., CISA, CPA

Internal Audit’s Contribution to the Effectiveness of Information Security (Part 1)
Pau John Steinbart, Robyn Raschke, Graham Gal and William N. Billa, Ph.D., CPA

Why Computer Ethics Matters to Computer Auditing
Wanbil W. Lee, DBA

Vimal Mani, CISA, CISSP

Read more from these Journal authors...

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

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

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

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

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

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.

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
www.isaca.org
Save time and money at Capella University

The knowledge you gained for your IT certifications—including CISSP®, CISA®, CISM®, and more—can help you earn college credit toward a Capella bachelor’s or master’s IT program, saving you time and money on your degree.

Online degrees in key IT fields

Further your career—explore Capella bachelor’s, master’s, and doctoral degrees in:

- Information Assurance and Security
- Project Management
- Network Technology
- And more

Many Capella IT programs have earned national recognitions and designations from several organizations, including:

ACCREDITATION:
Capella University is accredited by The Higher Learning Commission and is a member of the North Central Association of Colleges and Schools (NCA), www.ncahlc.org.

WASHINGTON RESIDENTS MAY RECEIVE CREDIT THROUGH CAPPELLA’S PRIOR LEARNING ASSESSMENT ONLY IN THE BACHELOR’S AND MBA PROGRAMS.

Capella’s BS in IT program is accredited by the Computing Accreditation Commission of ABET, http://www.abet.org.

The following program specializations are accredited by the Project Management Institute (PMI®) Global Accreditation Center for Project Management (PMI-GAC): BS in Information Technology – Project Management, BS in Business – Project Management, MS in Information Technology – Project Management, MBA – Project Management.

Capella University has been designated as a NSA/DHS national Center of Excellence for Information Assurance Education (CAEIAE) for the academic years 2012–2017.
Looking Back: Information Security Matters

This column recently reached its 15th anniversary. That means I have written more than 90 articles for the ISACA Journal, which I must admit catches me by surprise when I add them all up. Over the years, I have solicited feedback from the Journal’s readers and I have been very gratified by the dialogues that have been established. There were only a few rotten tomatoes thrown my way and many more responses that I found challenging and thought provoking. And a few that just said they liked what I had written.

IDEAS FOR TOPICS
I have often been asked, “Where do you come up with ideas for all the articles?” It really has been easy. Most of the time, I just talk about my job and the projects I am working on at the time. I have been fortunate to have had some interesting work to do, which resulted in pieces that talked about matters such as establishing security functions, managing user identities, recovering from disasters and building secure data centers.

When my own work did not provide topics, I could always count on the newspaper for ideas. There is always something newsworthy about information security, risk management and disaster recovery. In the past few years, I have been writing a lot about cyberthreats, ranging from industrial espionage to all-out warfare. I consider this the most important question of our time… or at least the one we as security professionals can address. We cannot solve income inequality or world hunger, but we can do something about protecting information from criminals, terrorists and hostile governments.

Where I could, I have drawn on my own experiences. While I have never been the victim of a cybercrime, unless a few viruses along the way can be included, I have used my experience in writing about some disasters I have lived through and helped my clients navigate. In particular, there were two articles in the early 2000s on the destruction of the World Trade Center, across the street from where my office was at the time.

Finally, I have enjoyed sharing my viewpoints on information security trends. My first column looked at public key infrastructure (PKI) with a more skeptical eye than was fashionable at the time. As I understand it, that one had some impact among the readership. I wrote about such matters as the vanishing security perimeter, the security of instant messaging and the cloud before they were common topics elsewhere. (Or maybe they were written about and I just missed the publications.)

CONVERSATIONS WITH THE WORLD
I have viewed each article as a conversation with security professionals around the world. I have always tried to make the articles I write entertaining, as well as (so I hope) relevant to fellow professionals. I suppose my favorite bit of fun in this regard was a column that began with “I am sitting in a bar in Berlin… .”

I suspect I am the only security commentator to have included references to Mel Gibson, Sandra Bullock and Paris Hilton in my articles. It was not all Hollywood, of course. I have had occasion, in discussing information security, to quote Plato, Aristotle, Shakespeare, Keynes and Robert Burns. It is important to me never to talk down to those who read my pieces; I assume a certain level of culture, learning and intelligence on your part and have never been shown to be misguided in that regard.

RELEVANCE OVER TIME
It amazes me, looking back, how relevant some of the articles remain after a decade or more. Digital signatures, security architecture, privacy, incident management and computer viruses were subjects of articles in 1999. I am not sure I would say the same things today and I know I would not say them the same way, but those are all still very timely topics.

The perennial nature of these subjects should not surprise me, though. When reduced to its elements, information security is really very simple: Keep information safely in the hands of...
those who should have it and out of the hands of everyone else. However, achieving that goal is a great deal more complex. Information security is somewhat kaleidoscopic in that just when you think you can see the picture, it changes. The bad guys get smarter, the technology evolves, the business becomes more encompassing and the components of information security interact in ways that were never previously anticipated.

Information security professionals are faced with decisions that go well beyond the technology of protection: How does one create a culture of security? Does security of information fit within the laws in the places where the information is stored and used? What is the relationship between information security and risk management? Is information security the same thing in different countries and cultures around the world? I have enjoyed the opportunity to probe questions like these in the pages of the Journal.

Some of you may know that I was president of ISACA in its early years. I have little interest in attending board meetings or involving myself in the administration of what is now a vibrant, global organization with more than 100,000 members. I have great loyalty to ISACA and I prefer to make my contribution to its welfare by writing my column. It has been my privilege to have the pages of the ISACA Journal in which to share my viewpoints and ideas. I make no pretense that I have provided any direct guidance as to how security professionals and IT auditors should do their jobs. I hope that I have provoked some thoughts, opened a few eyes and maybe even started a few arguments. It has been fun for me and while I do not promise to be writing Information Security Matters 15 years hence, I will continue writing as long as people still want to read what I have to say.
Let me belabor the obvious. Organizations everywhere realize that they need to back up their critical data and make arrangements to run their critical application systems in the event of a disruption in their data centers. So, not to put too fine a point on it, critical is covered. Critical is not the subject of this article.1

THE MYTH OF TIER TWO

What concerns me here is everything else, the noncritical data and systems, which I will lump under the rubric of “Tier Two.” Over the years, I have heard many IT managers (and many information security professionals, for that matter) say, “We’ll take care of the critical systems and figure out what to do with the rest when the time comes.” T’aint so, my friends, t’aint so.2 I would like to challenge that entire way of thinking. There is no such thing as Tier Two.

There is no definitive way to ascertain what is critical and what is not based on the perceptions of the users of information systems or their developers. At best, criticality is a determination made by individuals with a prejudicial interest in what they consider to be important. While certain systems and their associated data may be of obvious importance to a department or an organization as a whole, it does not follow that that which is less evident is not vital to the organization’s welfare. In most corporations and government agencies I have dealt with, information systems are a reflection of complex organizational structures with many interrelated parts. Those managers uninterested in certain applications may not understand the consequences of the absence of seemingly unimportant applications to other functions on which they are knowingly or unknowingly reliant. It is scant comfort that the hole may be in someone else’s part of the boat.

Thus, the user who has—or who seems to have—the greatest knowledge has the greatest influence over criticality decisions. Managers who are less forceful have less knowledge of how their systems actually work, or managers who just happen to miss the meeting may find that their systems have been considered Tier Two.

(CRITICALITY, COST AND COMPLEXITY

In my experience, many criticality decisions are based more on budgets than on the actual importance of systems. Because many IT functions charge back their costs, business managers have an incentive to downplay the consequences of the unavailability of their information systems. It is not inexpensive to replicate data in real time, maintain alternate equipment that would be used only in emergencies and establish telecommunication links to multiple data centers. Thus, there is a reason for some managers to say that their systems are Tier Two, knowing full well that they will insist on instant recovery should there ever be a system failure, without having to pay for recoverability every year in advance of an outage.

Adding to the murkiness of Tier Two determinations is that in many cases, application owners do not understand all the interactions among systems and data. Sadly, many application developers do not know all the interactions of their systems either. I have found that the result is shock and dismay when a critical component is missing at the time of a data center disruption—closely followed by a mad scramble to elevate Tier-Two systems to the top rank.

Systems and databases have become so large and complex that no one can accurately predict what is essential to an organization’s well-being. The 80-20 rule does not apply. A great deal more than 20 percent of all systems are necessary for an organization to function—not function at its peak, just to function tolerably well.

THE UNCERTAINTY PRINCIPLE

Organizations can accept that not everything is critical, or even that everything might be critical to someone, sometime. But it is extremely difficult to determine what is critical and what is Tier Two. Even that which is clearly a Tier-Two system must have some importance to an organization; otherwise, why was the system developed and the data captured? The problem is that it is nearly impossible to know the difference in advance. The Uncertainty Principal in play here may not be much of a deal by Werner Heisenberg’s3 standards, but it certainly
makes information security, business continuity and data management difficult.

Thus, the conundrum for management is what to do with Tier-Two systems and data. One might say, “Treat everything as though it were critical, and then nothing will be missed.” The one who might say that surely never had to justify a budget. (This approach may actually be a valid one where lives are at stake, e.g., in hospitals or in the military, but it can hardly be a general theory of data management.) While the criticality, or lack thereof, may be uncertain, the cost of protecting all the information resources equally is very clear indeed.

It does, to my mind, make sense to take the opposite approach: Treat nothing as though it were noncritical. Organizations should employ an integrated solution to data and system availability in such a way that an organization’s information portfolio is protected in a consolidated, consistent fashion, with no data element left behind.

DISASTER RECOVERY AS A SERVICE
That all sounds very egalitarian, but what does it mean in practical terms?
• Those applications and data judged to be critical should be backed up and recovered within the constraints of an organization’s risk tolerance and budget.
• All data, not just those deemed critical, must be backed up regularly and stored offsite. There is nothing inherently wrong with using physical tape, but it does necessitate tape drives at a recovery site, which add both time and expense to a recovery effort.
• The recovery of all data and applications must be tested. It is insufficient to figure out how to recover data after a disruption.
• This implies that there must be an equipped site in which recovery tests may be run. It need not be the same site where data and applications will be recovered if the need ever arises, although that would be preferable.
• There must be people assigned to recovering all data and applications. Following a significant data center outage, most staff will be consumed with the recovery of critical data and applications; some people need to be reserved for the recovery of everything else. To me, this suggests a contingent outsourcing solution that would come into effect only when needed.

Fortunately, meeting these requirements does not necessitate an investment in real estate and massive amounts of equipment. Much today can be accomplished using the cloud as a vehicle for data backup and recovery testing. While this is hardly a zero-cost solution, it may well bring the timely availability of all data within the financial constraints of many companies.

Disaster Recovery as a Service (DRaaS) has been much talked about for at least the past five years. Well, at least I have been talking about it, but it was always in the future tense, because DRaaS has only recently become viable—technically and economically. It may not be the best single solution just yet for enterprisewide IT recoverability, but it may offer hope to downtrodden, neglected data and applications. Tier Two is dead. Long live all data for all applications.

ENDNOTES
1 Nor is it about sensitivity. However, I believe that the same point could be made about the need to treat the confidentiality and integrity of data, especially the so-called “public information” that organizations make no effort to secure. It constantly amazes me how much information I am able to obtain about companies and their people from publicly available sources. I will take up confidentiality and integrity in a later installment of this column.
2 Jen Hajigergiou, one of the editors of this column, tells me that the ISACA Journal reaches a global audience, many of whom do not understand Americanisms. In this spirit, I offer the translation: “It is not so, my friends, it is not so.” It loses something in translation.
3 Werner Heisenberg was a German physicist who stated, in laymen’s terms, that we cannot simultaneously know the position and momentum of a subatomic particle. In nonlayman’s terms, he wrote \( \sigma_x \sigma_p \geq \hbar/2 \). For this, he won the Nobel Prize.
Ketan Dholakia, CISM, CRISC, CISSP

Q: What do you see as the biggest risk factors being addressed by governance, risk management or security professionals? How can organizations protect themselves?

A: Many of our customers seem to be struggling with third-party or vendor risk management. One of the reasons for this is because many organizations do not have processes in place to ensure that the vendor can meet the customer’s regulatory requirements. To be effective with vendor management, a thorough vetting process has to be implemented using automation to filter out high-risk vendors. Automation is necessary as there can be hundreds of vendors that supply to a customer, and, without automation, it is humanly impossible to manage the risk posed.

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

A: I have been in the GRC field for several years and I started out in this field by transitioning from managing IT vulnerabilities and determining the controls in place to mitigate the threat. As I was progressing through my career, it was evident that the business saw me as “just another IT guy making a big deal about risk.” To change this, I looked to certification.

The Certified Information Security Manager® (CISM®) certification was the most beneficial for me. I was a member of ISACA and decided to take the CISM exam. CISM exam training provided me with an understanding of how to articulate and walk a business person through the impact that risk can have on the business, using language the average business person can understand.

Today, at Maclear, the first thing we do when hiring new team members is ensure that they have at least a Certified Information Systems Auditor® (CISA®) certification—it gives us the confidence to know that the potential team member understands risk and is comfortable explaining it to the business.

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

A: My biggest career challenge has been in convincing a very large client to implement a governance, risk and compliance (GRC) strategy effectively. The client’s risk appetite did not meet its risk strategy. The risk professionals were well qualified and understood risk at a tactical level for their business unit, but did not understand the strategic direction toward which the company wanted to go. Communicating the strategy and having senior management work across the business units, we were able to build a GRC program that leveraged risk and controls across all business units so that there was a common source of data and understanding. Three years into this endeavor the strategy has been successfully implemented.

Q: What will be the biggest compliance challenge in 2014? How should it be faced?

A: I believe the biggest challenges facing compliance are building awareness and providing training for compliance and risk managers for some of the regulatory changes and updates. For example, as PCI 3.0 starts to get established, companies will have to change their approach to be more risk-based in their assessments and will require a thorough understanding of risk and compliance, not just an understanding of vulnerabilities and threats. Training and awareness will be required to meet these challenges.
My Favorite Blogs:
- Maclear’s GRC blog
- Forrester
- GRC 20/20

On My Desk Right Now:
- My computer attached to 2 screens
- My iPad
- A lot of to-do items organized by priority

When I’m Not at Work:
I love to watch movies with my family and have hundreds of books on my iPad that travel with me everywhere.

My No. 1 Piece of Advice for Risk and Compliance Professionals:
Understand the strategy that your company is trying to implement and make sure that the risk appetite meets that strategy, doing so via open communication channels across all business units and business processes.

My Three Goals for 2014:
1. Hire several people in various roles with the best talent I can find.
2. Build new, and enhance our existing, partnerships in EMEA.
3. Improve marketing of Maclear.

My Favorite ISACA Benefit:
- Chapter meetings
- ISACA Bookstore
- eLibrary
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.
The Piracy of Privacy

Following US Federal Judge Richard Leon’s ruling that the US National Security Agency (NSA)’s bulk collection of telephone metadata is likely unconstitutional, the Wall Street Journal ran an opinion piece, that read in part:

"The reality of the information age is that we all have less expectation of privacy. No one who makes calls and emails on a smartphone, visits an e-commerce web site, uses a credit card, drives with an Easy Pass or otherwise benefits from modern technology can truly believe that he is not entrusting data to third parties about personal behavior."

2013 was especially dotted by significant shake-ups in the field of information privacy, beginning with Edward Snowden’s disclosure of vast numbers of NSA documents. “When one considers the global uptake of information trade, it is not unreasonable to expect that informational privacy will be to this century what liberty was in the time of John Stuart Mill.” More recent happenings include German Chancellor Angela Merkel’s complaint that the US government tapped her cell phone, an open letter from certain tech companies to US President Barack Obama suggesting a review of NSA’s data surveillance programs, the appearance of the NSA director before a congressional committee, CBS News’ 60 minutes coverage of the NSA story, and previously mentioned Judge Leon’s ruling that the NSA practices regarding telephony metadata are likely unconstitutional.

Intent in furnishing data is central to the issue of privacy. The question is: What purpose on hand drives the need to share data? Our consent, or agreeing to provide data, is the first layer of protection of privacy. Accordingly, data can be classified as transactional (driven by contract) or voluntary (driven by consent of the provider). Contractual sharing of data is now well established and expectations of privacy surrounding such data have matured over time. What is causing uninformed debate about privacy is the nature and context of voluntarily supplied personal information.

The growth in voluntarily supplied information has been, and will continue to be, exponential. Information infrastructures (e.g., Google, Facebook, Twitter, LinkedIn) are emerging daily and becoming popular in a short period of time. In our desire to seek services of various kinds—for efficiency, productivity, profit or just fun—we sort of agree to terms and conditions that we may not have even read or, if read, not comprehended fully. One might say that this, too, is contractual sharing of data. Yes, while that is true, the contract refers to no direct exchange for consideration between the company and the patron, but rather for the use of the infrastructure, which results in trillions of data—data that the owner of the infrastructure controls, aggregates and uses for its own economic gain.

Transactional data have a definite cycle; voluntary data seem to fade into perpetuity. The intentions behind the former are usually tacitly articulated and apply within the realm of the agreeing parties. In contrast, voluntary data are generally timeless, could be “sliced and diced” using data mining, and can be further masked and shared for economic gain of the infrastructure owner and its customers.

**SOFT VOLUNTEERISM**

Soft volunteerism refers to the act of volunteering information on the part of a user when, in fact, one does not necessarily want or mean to do so. It is not so much consent to share data, but rather lack of dissent in sharing data. Passivity or inertia on the part of the provider plays an important role in one’s attraction to soft volunteerism. Immediate perceived benefits of seeking the services and, thus, benefiting from them outweigh anything that the user vaguely understands as the costs of doing so under the terms and conditions signed by the user.

Before clicking the “I agree” button on an agreement to use, how often have you paused and analyzed the contents of the agreement? The agreement is generally long, filled with...
legal ease and you feel like you are wasting time in getting to the services provided by the company that just popped the agreement on your screen. According to the prospect theory of decision-making behavior, losses are weighted more heavily than gains. And here you are, delaying the immediate benefits of using digital signatures from Co-Sign or the latest version of Adobe Acrobat. And we fall into the vulnerability of allowing an apparently harmless agreement to come in the way of doing want we want to do.

According to a 2009 survey conducted by Harris Interactive Inc., on behalf of Microsoft and the National Cyber Security Alliance, about one out of five people has given personal information on a web site that may not have been a secure site without knowing if someone was tracking the personal information or login information as it was typed. People willingly share personal information when they are nudged to do so. The perceived benefits seem to outweigh any remotely noticed costs of volunteering the information.

Over time, as the avalanche of such actions continues to precipitate, it becomes second nature to experiment with the excess of arguably free services. We may still adorn the normative value of privacy, but privacy, in fact, continues to decline. We voluntarily place into our cars wireless devices from our auto insurance company that track our driving habits, and we walk around with an active cell phone that announces our position, time and potential interests.

WHAT DRIVES SOFT VOLUNTEERISM?
Claiming to know our fallibilities better than we do, soft paternalists seek to aid us in making “correct” decisions through persuasion; they guide us toward the alternatives that we would have chosen had we been exercising willpower and foresight. Companies and institutions merely organize the context in which people make decisions. A form of social engineering of people’s decision making toward a particular outcome, it preserves the possibility of choice. Indeed, it grants the choice, but with an overwhelming urge to lean toward the recommended choice, nudging people toward more disclosure while preserving the illusion of free choice.

In part, this apparently seamless data gathering process is fully enveloped within a technological framework. As part of our daily life, the process has little visibility, if any. Its ubiquitous nature makes it a part of our routine; it is easy to neither control nor challenge its presence. Soft volunteerism is sourced in mandatory volunteerism and, as defined by Gary Marx, is disingenuous communication that seeks to create the impression that one is volunteering when that really is not the case. Here are some examples:
• Retail store loyalty card
• Ownership and use of mobile electronic devices
• Credit card ownership and use

Even normal inquiries with a provider begin with: “This call may be monitored for quality assurance purposes.” Of course, we are not going to hang up; our focus is on seeking a resolution for the question hovering in our mind. We do not say, “Well, I do not agree to the recording of this conversation.” And of course, the company is nudging us toward a complacent “OK.” Absence of dissent overtakes the explicit presence of consent.

FOUR PREMISES
In searching for an appropriate threshold for consent in privacy, Ian Kerr and colleagues focus on the following four requirements:
1. The subject must have knowingly consented to the collection, use or disclosure of personal information.
2. Consent must be obtained in a meaningful way, generally requiring that organizations communicate the purposes for collection, so that the person will reasonably know and understand how the information will be collected, used or disclosed.
3. Organizations must create a higher threshold for consent by contemplating different forms of consent depending on the nature of information and its sensitivity.
4. In a principal-agent relationship, consent is dynamic and ongoing. It is implied all the time that the patron grants the privilege to the provider and is only good as long as the consent is not withdrawn.

As Kerr and his colleagues point out, a legal definition of consent is hard to find. The common law context suggests that consent is a “freely given agreement.” An agreement, contractual or by choice, implies a particular aim or object. While it is clear that the force of laws and regulations is necessary, in the end, what equally matters is the behavior of the user. Concepts and paradigms such as bounded rationality
and prospect theory point to the vulnerability of human users in exercising consent. If that is where the failure occurs, privacy issues will only propagate, not get better.

Finally, remember that privacy solutions embedded in the technology to empower users to protect their privacy are only as good as the motivation, knowledge and determination of the user. Not all users are equally technology savvy; not all users consider it worth their time to navigate through privacy monitors in a gadget to feel safe. And generally, all users are creatures of bounded rationality. Despite Apple and Google, for example, giving them more tools to control on their own, not much difference on the privacy landscape is likely.

SOFT VOLUNTEERISM TO SOFT SURVEILLANCE

Soft volunteerism nudges people to share more information. This results in a huge pool of data across companies and institutions. If hard surveillance, such as the use of camera watching over a parking lot, remains concretely vivid, soft surveillance remains buried in the technology, allowing it to explore freely on available data and metadata. The NSA's reach of networks could become wider and stronger. Consequently, people would lose trust in their providers, such as Facebook, and the loss of trust would translate into a lack of prosperity for the provider. This is where the motivation for the open letter by technology companies to President Obama can be contextualized. Technology companies want to protect their collection of voluntary data.

GOING FORWARD: IS PRIVACY A MIRAGE?

I wonder: Is privacy now a mirage? With volumes of data emerging, work and home boundaries fading, and devices becoming more pervasive, is a viable defense of privacy possible? Or, is the situation going to continue to worsen on this ground? Because companies like Facebook thrive on data that users provide for safe storage and proper use, is it likely that the Facebooks of the world will fight for personal privacy and innovative solutions to protect privacy? For now, it seems like a business model that simply focuses on privacy protection may be inadequate for the financial world.

ENDNOTES

1 According to a Pew research survey, 59 percent of Internet users do not believe it is possible to be completely anonymous online, while 37 percent of them believe it is possible. See Pew Research Center, “Anonymity, Privacy, and Security Online,” Pew Research Center’s Internet & American Life Project survey, September 2013.


7 Subsequently, in a separate hearing of a petition filed by the American Civil Liberties Union, US District Judge William Pauley upheld the legality of the NSA’s data-collection program. The Wall Street Journal, 28 December 2013


12 Op cit, Kerr. Most of the analysis presented by Kerr, et al., is based on the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA).
With the expansion of technology, especially the Internet, organizations have reaped many benefits. But these advancements come with some risk and threats, both to individuals and organizations. One of those threats is referred to as cybercrime, where bad guys do not wield guns and force to rob you, but use technology, stealth and cunning. One popular crime among cybercriminals is identity theft, which has become rampant. Costs of cybercrime in 2011 were an estimated US $1.52 billion in the US alone and US $221 billion globally. These criminals find a bonanza if they can successfully perpetrate a data breach in which they break into a system and database to steal personally identifiable information (PII) (e.g., addresses, social security numbers, financial account numbers), or better yet, data on credit/debit cards (a more direct way to perpetrate identity theft) for a large number of individuals. The recent data breach at Target is an example of such a crime.

**THE PROBLEM**

Even large, sophisticated organizations, such as Target, can have their systems penetrated and lose thousands, even millions, of people’s PII or data on credit/debit cards. There are safety measures that can help prevent this crime, or at least detect it early. But the truth is, many organizations are susceptible and do not know it.

In 2011, 174 million data records were stolen, in 885 different incidents. There were five attacks in 2011 in the US in which more than 10 million identities (PII) were stolen, at a cost of US $194 per capita. In 2012, the Ponemon Institute surveyed 56 organizations about the cost of cybersecurity, and results show the average cost of a data breach for those organizations was US $8.9 million. The same survey found that those entities experienced 102 successful attacks per week.

Organizations of all sizes are at risk. PC World says that data breach is a fairly common occurrence among companies of all sizes. In addition, Symantec’s 2013 Internet Security Threat Report says that 50 percent of all targeted malicious attacks in 2012 were aimed at entities with fewer than 2,500 employees, and the largest growth area was entities with fewer than 250 employees (51 percent of all attacks).

**CASE STUDY**

A good example is a recent data breach conducted on the Department of Revenue for the state of South Carolina (USA) and its data records in those systems. According to reports, about 3.6 million records were compromised in the data breach. The cybercriminals got Social Security numbers and other PII that can be used to perpetrate identity theft crimes. Thieves also accessed data on 387,000 credit/debit cards. Stolen records contained data from 1998 to present. Fortunately, the state used encryption on recent credit/debit cards, and only 16,000 records were unencrypted. However, cybercriminals are tech-savvy and there is a chance that they could take the time to break the encryption on those records.

The cybercriminal attacked the systems of South Carolina in August 2012 from a non-US Internet address and again in September 2012—this time gaining access to tax returns back to 1998. The attack went unnoticed until 10 October 2012, when the US Secret Service electronic crimes task force detected the crime. It took 10 days for South Carolina to lock down its systems from the intruder and secure its data. To date, no arrests have been made nor has the intruder been publicly identified. It is important to note that South Carolina did not discover the crime itself—there was outside detection. Thus, it is possible the crime would have gone undetected for much longer.

According to South Carolina Governor Nikki Haley, the crime was “creative,” bringing up an important point about data breaches and similar cybercrimes. Cybercriminals, as stated previously, are tech-savvy and, therefore, are fully capable...
of conducting sophisticated, crafty and creative attacks to steal data. A second point, cybercriminals often target their victims specifically. Third, often these attacks are associated with cybergangs that live in countries external to where the perpetrated organizations reside and that may act as safe havens for the cybercriminal. Data breach and resulting identity theft are the new international crime wave.

THE RISK
There are a number of risk factors that might be proprietary to a particular entity. The following are the more common risk factors (albeit the list is not exhaustive):

- Resources to conduct IT repairs, mitigation activities
- Costs associated with protecting PII of customers
- Loss of public image and relations

Obviously, the initial costs are associated with mitigating the vulnerability (loophole) that allowed the breach to occur. IT professionals have to figure out how the cybercriminal got into the organization's system, how to patch it and how to prevent it from happening again. Remember, it took South Carolina 10 days to do all of that. These costs likely include technologies and other purchases as well as the time of many professionals. Sometimes, a consultant or subject matter expert (SME) may be needed to fix the loophole.

Monetary costs related to customers typically involve the organization providing credit monitoring, usually for one year, and sometimes an insurance policy, often for as much as US $1 million, to cover future fraud based on stolen PII. Think about an organization that has 3.6 million such customers/clients and calculate the total costs of these two provisions.

Then, there is the effect of a publicized data breach on the reputation and public image of the victim organization. While it is difficult to put a specific monetary figure to this situation, almost everyone would agree there is some level of cost in this intangible circumstance. It appears Target has suffered some of that loss in its recent data breach.10

Finally, there can be legal fees. If individuals sue the victim organization for not protecting their PII, the victim has to pay to defend itself because it is a victim of a cybercrime—a paradox to say the least. Settlement costs can be significant, and if the case goes to court and the organization loses, there may be stiff costs associated with the court’s decision.

CHANGES IN LEGAL ENVIRONMENT
Executives need to understand that the risk is not just that their organization can become a victim of a data breach or may end up in court. The risk goes beyond that. There is a new expansion of legal risk.

Over the last few years, about 46 US states have passed a security (data) breach law.11 On 25 August 2013, the new breach notification regulation of the European Union (EU) came into force for electronic communication service (ECS) entities.12 Businesses in the US that fall victim to a data breach may also be found guilty of a violation of one or more state security breach laws. A few years ago, Choicepoint.com had a breach that cost it millions of dollars in fines and mandatory security audits for years.

In June 2012, the US federal government crafted a bill and is attempting to pass a federal security breach law similar to those enacted by those 46 states. The bill, which should ultimately replace state laws, contains language to specifically define a breach and set a national standard in the US for data breach notification to the victim’s clients. It would also set maximum damages the victim would have to pay its clients.

But more than the pending US federal law is the legal risk of existing laws and the way courts are interpreting them. Until a couple of years ago, courts dismissed a lot of claims of damages from data breaches similar to the one in South Carolina. Victims had to show specific damages and often the data would have been stolen, but the cybercriminals had not used any of the data...yet.

Now judges are allowing class-action suits related to data breaches. They are also considering the fact that there is a lag between the theft of PII and the use of PII to conduct identity theft crimes that do involve monetary damages, but not until weeks or months after the theft. Now judges consider lawsuits that can show a real possibility of future damages. Organizations will need to make sure their insurance is adequate to handle this rare, but possible, event.

Although it is impossible to prevent all data breach attacks, the courts have taken a stance on reasonable protection. The metric for that reasonableness is best practices in cybersecurity to protect against a data breach. That is, the more the entity has adopted those best practices, the less likely the court is to settle on behalf of the plaintiff or the lower the settlement. Conversely, the less the defendant has employed best practices, the more likely the judge or court is to rule in favor of plaintiffs and award higher settlements.
According to a study by Temple University Beasley School of Law (Philadelphia, Pennsylvania, USA), in the case of a lawsuit associated with a data breach, the average settlement award is US $2,500 per plaintiff and the average attorney fees are US $1.2 million. As can easily be seen, the potential legal costs are a significant risk that no executive wants to have to address as the result of a data breach. These costs are additional to the ones mentioned in the last section.

SOLUTION

IT auditors need to be informed and capable of assisting organizations in preventing data breaches, as much as possible. That prevention must start with an evaluation of the risk associated with a data breach. If an organization maintains PII of individuals who are basically customers, then the higher the number of such customers, the higher the inherent risk. In the previously discussed case of South Carolina, the initial risk assessment is quite large, with millions of customers. In such cases, the IT auditor must assist management in evaluating its level of security over PII. It could be that the entity has sufficiently addressed the risk by employing the necessary best practices, but a security audit by the IT auditor should help make a relatively definitive assessment. But if the entity has not done an assessment, it is likely to be quite vulnerable and susceptible to large costs of a data breach, and it is likely they have not employed a sufficient level of best practices. In this process, the organization should assess the need for the assistance of an IT auditor knowledgeable about data breaches.

CONCLUSION

IT auditors need to be aware of the basics regarding data breaches. This begins with a risk assessment based on size, assets that are high-profile targets and having security controls in place. It also includes a basic understanding of the best practices in security: vulnerabilities assessment, patching them, weaknesses in a perimeter and encryption. These special skills, knowledge and abilities are needed more than ever.

Entities that maintain large databases of individuals and their PII should be prepared for a data breach by doing due diligence, as defined by cybersecurity professionals. That includes such preparation as ensuring that an adequate level of best practices have been employed, and an incident response plan is in place to handle all of the aspects of risk and costs mentioned herein. IT auditors should be key resources to accomplish these tasks.

ENDNOTES

7 Op cit, Symantec, p. 4
8 Most of the facts on the case study were taken from Bonner, P.; “S.C. Taxpayers’ Social Security Numbers, Credit Cards Hacked,” Journal of Accountancy, 1 November 2012, www.journalofaccountancy.com/News/20126778.htm
11 The only US states without a data breach law are Alabama, Kentucky, New Mexico and South Dakota. Puerto Rico and Washington DC also have data breach laws.
From an organization’s point of view, the best technology is worthless when it is not appropriately implemented. In fact, systems or devices that are not well deployed could quickly transform the benefits for which they were acquired into potential risk factors. Therefore, taking control of technology, both from the strategic and operational perspective, is essential to guarantee successful implementation. This is the focus of *IT Strategic and Operational Controls*, by John Kyriazoglou, which is also available in Spanish ([www.isaca.org/bookstore](http://www.isaca.org/bookstore)).

From the first chapter, the author challenges the reader, offering an analogy between IT and medication. Like medicine, IT reinforces the organization, allowing for the solution of real problems. However, when not strictly used, medicine can cause damage, provoke unexpected results or even have catastrophic consequences.

From here, IT controls are defined as specific actions based on procedures, policies and practices aimed at the fulfillment of organizational goals. As stated by the author, IT controls define an appropriate operational environment for IT, essentially infrastructure and systems, and ensure the adequate accomplishment of day-to-day activities.

Based on this definition, Kyriazoglou lays out 10 chapters, starting with a generic review of the organization and management of IT controls. He also covers issues related to specific fields, such as software and applications and security controls, among others. Controls related to audit and consulting services are also analyzed.

The book includes an appendix with several examples of policies, a code of ethics, IT forms and methodologies, as well as review questions for every chapter and some practical cases and useful recommendations. The book also offers a complete listing of books, articles and Internet links intended to provide the reader more insight.

**EDITOR’S NOTE**

*IT Strategic and Operational Controls* is available from the ISACA Bookstore. For more information, see the ISACA Bookstore Supplement in this Journal, visit [www.isaca.org/bookstore](http://www.isaca.org/bookstore), email bookstore@isaca.org or telephone +1.847.660.5650. Learn more about and discuss controls monitoring in the Knowledge Center ([www.isaca.org/topic-controls-monitoring](http://www.isaca.org/topic-controls-monitoring)).
COBIT 5 Processes From a Systems Management Perspective

COBIT® 5 establishes a governance layer and does a good job of capturing stakeholder needs, driving enterprise, IT and enabler goals. COBIT 5 fosters the use of balanced scorecards and goal cascades to help IT leaders show that IT is managing its ship for the good of the enterprise. This includes its metric recommendations for enterprise and IT goals.

COBIT® relates process to a life cycle of plan, design, build, operate, monitor and update. How do COBIT’s 13 Align, Plan and Organize (APO) processes; 10 Build, Acquire and Implement (BAI) processes; six Deliver, Service and Support (DSS) processes; and three Monitor, Evaluate and Assess (MEA) processes relate to one another? IT’s primary goal is business services delivery; as important as it is to define each of these processes, it is also important to understand how these processes relate to one another to optimize IT’s ability to deliver the right service at the right time for the right price. For example, the management of service requests and incidents, and the management of change and change transition and acceptance are intimately interrelated. Poor change management dramatically impacts the quality of the service request and incident processes.1

Systems thinking offers an answer to many of these issues:

In systems thinking, we must consciously recognize that everything we do has affected and does affect everything else we have done or will do. Systems thinking involves us moving away from seeing single or isolated elements, structures, functions and events to seeing the processes by which they interrelate to one another…. It is this process of diagnosis and discovery that will ultimately give us a practical guide to finding systems solutions to our systems’ problems. As leaders, we really do not deal with problems today—we deal with messes of problems which require more holistic or systems solutions.2

This quote represents IT today. IT managers do not deal with isolated problems. They deal with messes of problems. IT leaders need to recognize that the quality of solutions definition processes determines the quality of requirements created, the issues that are discovered in the build, the bugs that are found in quality testing and the number of incidents that are in service delivery. All of these are related.

The quality at each stage is determined by the confluence of people, process and technology (figure 1). Together, these make answering most of the aforementioned issues difficult at best. For this reason, a systems viewpoint is a valuable way to view the COBIT processes as interrelating and providing data for successful process layers. Further, IT management is a system of systems or, at the very least, a system of processes.

All COBIT components can be viewed as a single system or as interconnected value streams.3

VIEWING IT AS A CORPORATE VALUE CHAIN

Viewing IT as a corporate value chain requires that everything IT does be synthesized into a set of core value-added functions. Figure 2 is a view of this value chain.
The primary activities that IT performs—the places where it adds value—can be summarized into three activities:
1. Automation of business capabilities
2. Management of those capabilities once they have gone into production

HP has identified four value streams (Figure 3) that cover the core process of the COBIT 5 process reference model and, even more important, how these value streams relate to the organization and to each other to create an end-to-end IT management system.

Enjoying this article?

• Read Configuration Management: Using COBIT 5. www.isaca.org/configuration-management
• Learn more about, discuss and collaborate on information security management and COBIT 5 in the Knowledge Center. www.isaca.org/knowledgecenter

3. Servicing of end-user requests and issues relating to subscribing to business capabilities, dispatching people to fix client issues and instantiating business capabilities—services and applications

Figure 2—IT Value Chain

Figure 3—Value Streams Across the Service Life Cycle
A key element of this is the notion of a conceptual model feeding a logical model, which, in turn, feeds a physical service model. Once strategic demand enters the planned portfolio, a conceptual service model needs to be developed against which requirements can be constructed and built. This includes drafting a proposed solution that reflects enterprise needs/expectations and the laying out of service warranty expectations. Next, a logical service model that describes what the components of the service are and, in turn, relates the model to existing capabilities needs to be developed. This should then be followed by an actual service model. By starting the service modeling early, it can drive up reuse of capabilities, technology and knowledge. In the end, agility increases while cost and risk are reduced.

**STRATEGY TO PORTFOLIO LINKAGES**

Strategy to portfolio (**figure 4**) defines how well the IT portfolio of services matches the enterprise’s business strategy. IT leaders must recognize that they are not in the IT business, but rather the business of their firm—e.g., banking, insurance, manufacturing. The strategy-to-portfolio value stream is concerned with the quality of management of the portfolio, the innovation that is being produced for the portfolio, the quality of new solutions being identified, the management of instantiation within programs and projects, and the effectiveness and efficiency of spend for services and innovation.

Strategy to portfolio includes COBIT 5 processes/activities for APO02 (strategy), APO03 (enterprise architecture), APO04 (innovation) and APO05 (portfolio). In this value stream, enterprise architecture drives the current state of the portfolio and all proposed additions to the portfolio. Additions are captured as innovation proposals/contracts representing demand and then integrated as demand management. These are then added as development (to be procured) items to the proposed portfolio. While not explicitly called out, goals are captured here in the form of proposals—a separate process manages the capture, reconciliation and realization of benefits. The enterprise architect’s role involves applying standards and governance; using COBIT, the enterprise architect is able to measure the variance between the anticipated future state and the ongoing processes to get there.

In this integrated form, the key elements identified by COBIT 5 are viewed as one system and include:

- Defining the strategic plan and road map where initiatives are prioritized by enterprise need
- Selecting opportunities and solutions that are aligned to business strategy
- Ensuring that the established budgets are transparent to monitor implementation and use of innovation
- Identifying opportunities, risk and constraints for IT to enhance the business
- Collecting data to enable effective IT-related risk identification, analysis and reporting

The key COBIT processes directly linked to strategy to portfolio are:

- **APO02 Manage strategy**
- **APO03 Manage enterprise architecture**
- **APO04 Manage innovation**
- **APO08 Manage relationships**
- **APO12 Manage risk**
- **APO13 Manage security**
REQUIREMENTS TO DEPLOYMENT

The requirements-to-deploy value stream (figure 5) describes how well IT manages development and delivery—the delivery of strategic demand. This value chain is concerned with the quality of the requirements process, the predictability of programs and projects, the end-to-end quality delivered, the change process, and the use and measurement of performance against service agreements. Here, service designers create/negotiate service level agreements (SLAs)/operational level agreements (OLAs) that evolve as the client and application mature over time.

The requirements-to-deploy value stream includes the COBIT 5 processes of BAI01 (programs and project), BAI02 (requirements), APO09 (service agreements), APO11 (quality), BAI07 (change acceptance and transitioning), and BAI06 (changes). Here, requirements are captured at the same time as a project is initiated. Part of assuming that a quality level is part of the project is the establishment of a planned service agreement in what the IT Infrastructure Library (ITIL) calls the service design phase. When this phase is completed, a deployment package is created and change acceptance and transitioning begins; this results in a change being created (i.e., a ticket).

Again, in this integrated form, the key elements identified by COBIT 5 are viewed as one system and include:

- Integrating quality management into solutions for development and service delivery
- Collecting and analyzing risk data
- Developing and maintaining a project plan
- Defining and maintaining business and technical requirements

---

**Figure 5—Requirement to Deploy**

```
[Diagram showing the requirements-to-deploy value stream with nodes for Requirement Management, Defect Management, Project Delivery Management, Test Management, Build Management, Service Design Management, Release Management, Deployment Management, and Change Management.]
```
• Designing, building and testing solution components
• Documenting, tracking, performing and reporting on change

The key COBIT processes directly linked to a requirement to deploy are:
• APO11 Manage quality
• APO12 Manage risk
• APO13 Manage security
• BAI01 Manage programs and projects
• BAI02 Manage requirements definition
• BAI03 Manage solutions identification and build
• BAI04 Manage availability and capacity
• BAI06 Manage changes
• BAI07 Manage change acceptance and transitioning

REQUEST TO FULFILL
The request-to-fulfill value stream (figure 6) focuses on how well IT manages its overarching request and fulfillment activities. This is clearly operational demand. The request-to-fulfill value stream aims to “increase user productivity and minimize disruptions through quick resolution of user queries.”4 As a process, it touches multiple IT disciplines including, but not limited to:
• Service requests
• Change management
• Asset management
• Configuration management
• Supplier management (including cloud supplier management)

Request to fulfill is built upon service requests and change processes, but adds functions to complete the end-to-end processes. As indicated in figure 6, request to fulfill establishes the notion of a catalog and the notion of financial consumption in the form of subscription management, billing/chargeback and usage management. This is a choice IT organizations need to make; the current best practice is for it to be included. At this phase, the notion of service leasing should be envisioned, and its complement and elasticity allowed to evolve: As services are requested, they either fall into disuse or are abandoned altogether as business/mission capability changes (i.e., business agility). IT must ensure efficiency by keeping systems highly utilized.

There are also items that have been added here that are not explicit in COBIT 5. These include catalog management, subscription management and usage management. These support the rights aspects of asset management/software compliance and the implications of request, budgeting and actual usage. In this integrated form, the key elements are already identified by COBIT 5, but here it is viewed as one system and includes:
• Monitoring supplier performance and compliance
• Organizing, identifying, classifying and using knowledge
• Managing data for the asset life cycle
• Managing user identity and logical access

The key COBIT processes directly linked to request to fulfill are:
• APO10 Manage suppliers
• APO12 Manage risk
• APO13 Manage security
• BAI06 Manage changes
• BAI08 Manage knowledge
• BAI09 Manage assets
• DSS05 Manage security services
DETECT TO CORRECT

The detect-to-correct value stream (figure 7) concerns how well the IT organization prevents services and the supporting infrastructure from breaking down or degrading and how well it manages issues or events when the inevitable happens—something breaks. Simply put, this value chain aims to, as COBIT 5 suggests, increase user productivity and minimize disruptions. The detect-to-correct value stream touches many IT activity categories, including:

- Capacity
- Availability
- Operations
- Incident
- Knowledge
- Problem
- Quality (CSI)
- Security

The goal is clearly process optimization. Instead of viewing each area as discrete processes, they are viewed as part of one system that aims to ensure that services perform as agreed and that issues are routinely and holistically resolved. This process considers asset management and configuration management as a single process.

In this integrated form, the key elements identified by COBIT 5 are viewed as one system and include:

- Documenting, tracking, performing and reporting on change
- Monitoring internal and external IT services
- Identifying, investigating, resolving and closing events, incidents and problems
- Monitoring for security-related issues
- Monitoring, collecting and analyzing performance and conformance data

The key COBIT processes directly linked to detect to correct are:

- APO12 Manage risk
- APO13 Manage security
- BAI06 Manage changes
- DSS01 Manage operations
- DSS02 Manage service requests and incidents
- DSS03 Manage problems
- DSS05 Manage security services
- MEA01 Monitor, evaluate and assess performance and conformance

OVERARCHING VIEW

The previously described streams have been put together into one flow that shows all the linkages among the processes and how the processes touch one another (figure 8).

CONCLUSION

Every IT approach has a unique viewpoint on helping IT be more agile and efficient at meeting the needs of the business. The IT value chain viewpoint, which focuses on the data linkages across the service life cycle, complements the COBIT viewpoint of governance and management. This article has described a systems approach to COBIT 5, using COBIT 5 as the overarching system. Conscious recognition is given to the concept that everything done in IT management has affected and does affect everything else in IT management. The goal is to provide an understanding of the challenges in IT management.
and the importance of how everything touches and affects one another. Clearly, the people, process and technology elements of the IT management system cannot be viewed in isolation. The value streams of strategy to portfolio, requirement to deploy, request to fulfill and detect to correct align to support a singular value chain that supports business capability. The system has to improve to improve any one part.

**ENDNOTES**

1 Based on a private case study of a major US financial institution. Multiple additional sources.
2 Haines, Stephen G.; *Strategic and Systems Thinking*, 2007
3 Michael Porter pioneered the value chain strategy several years ago as a mechanism to evaluate business competitive advantage. According to Porter, a value chain is the interlinking activities that a firm performs to deliver a valuable product or service to the marketplace.
Auditing Oracle Databases Using CAATs

There are a variety of commercial security tools available to audit Oracle databases. However, there are instances when their application is not practical:

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

One approach is to audit Oracle databases using computer-assisted audit techniques (CAATs) in conjunction with information taken directly from the Oracle database.

ORACLE DATABASES

Oracle databases contain metadata or data about data. This is contained in the data dictionary and database views.

The data dictionary provides information about every object in the database, including Oracle database users, their privileges, roles and auditing information.

The contents of the data dictionary can be queried through Oracle database views. These views display the underlying table data in a useful manner. Some views are accessible to all database users, whereas others are restricted to DBAs. These views (prefixed with ‘DBA_’) show all relevant information in the database, including the information stored in the data dictionary. A full list of DBA views, along with more detailed explanations, may be found in the Oracle Database Reference.

The Oracle database also maintains dynamic performance views. As their name suggests, they are continuously updated with performance information while a database is open and in use. Dynamic views are named beginning with ‘V$’.

with explanations, may be found in the Oracle database reference.

SQL*Plus is a query tool included in every Oracle database installation. It enables one to query the database using Structured Query Language (SQL), formatting the output as desired and writing the results to file (if required).

OUTPUTTING ORACLE DATABASE VIEWS

Using the formatting and configuration options in Figure 1, Oracle query output, including those from views, can be directed to comma-separated values (CSV) text file(s).
**Figure 2** gives an idea of what a script would look like (a full Oracle script can be downloaded from the ISACA® Knowledge Center). Once generated, these scripts can be handed over to the DBA to be run over the required database(s). One CSV file will be produced for each view.

```sql
SET LINES 10000
SET TRIMSPOOL ON
SET PAGESIZE 10000
SET TIMING OFF
SET ECHO OFF
SET FEEDBACK OFF
SET COLSEP " , "
SET UNDERLINE OFF
SET NEWPAGE 0

-- Get a list of profiles on the system
SPOOL dba_profiles.txt
SELECT * FROM dba_profiles;
SPOOL OFF

-- Get a list of all users on the database
SPOOL dba_users.txt
SELECT * FROM dba_users;
SPOOL OFF

-- Parameter file contains commas
SET COLSEP " , "

-- Get a list of parameters
SPOOL v$parameter.txt
SELECT *
FROM v$parameter;
SPOOL OFF
```

These files can then be imported into CAATs tools, such as the following, for analysis and comparison.

**ANALYSING ORACLE DATABASE VIEWS**

These files can then be imported into CAATs tools, such as the following, for analysis and comparison.

**DBA_PROFILES**

The entity being audited should have a policy on how its passwords are configured. In Oracle databases, password configurations are reflected in the database profile (DBA_PROFILES) view. A profile is a named set of resource limits and password parameters that restricts database usage and instance resources for a user. That is, a given profile is attached to a user account, controlling, for example, the number of failed login attempts, password lifetime or password reuse for that user.

As noted previously, this view can be output to a CSV file (see figure 2). A sample output from the DBA_PROFILES CSV file can be seen in figure 3, in which the first line shows the Oracle field names. These field names relate to the defined layout for the DBA_PROFILES view (figure 4). The layout for this view and all Oracle database views is available in the Oracle Database Reference.

<table>
<thead>
<tr>
<th>Column</th>
<th>Data Type</th>
<th>Null</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE</td>
<td>VARCHAR2(30)</td>
<td>NOT NULL</td>
<td>Profile name</td>
</tr>
<tr>
<td>RESOURCE_NAME</td>
<td>VARCHAR2(32)</td>
<td>NOT NULL</td>
<td>Indicates whether the resource profile is a KERNEL or a PASSWORD parameter</td>
</tr>
<tr>
<td>RESOURCE_TYPE</td>
<td>VARCHAR2(8)</td>
<td></td>
<td>Indicates the limit placed on this resource for this profile</td>
</tr>
<tr>
<td>LIMIT</td>
<td>VARCHAR2(40)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All common CAATs tools (and, indeed, Microsoft Excel and Microsoft Access) allow for importing CSV files. Once the DBA_PROFILES have been imported into the CAATs tool, they can be analysed for compliance to the entity’s standards. These standards could be based upon ISACA’s Oracle Audit/Assurance Program and ICQ, the Defense Information System Agency’s Security Technical Implementation Guide, the Center for Internet Security benchmarks, or a document developed by the entity.
The key concept is that once the entity has one database analysed and knows it to be compliant to relevant standards, it can use that as a master profile, configuring its CAATs tool to compare the profiles of interest across all of its Oracle databases. This can be done by joining on the fields profile and resource (or simply on resource), displaying all records where the limit is not equal. For example, the failed login attempts may differ across a sample of databases. In this manner, the entity can quickly flag noncompliant profiles for follow-up and review.

If required, the entity can also periodically repeat reviews of the Oracle profiles. This would allow it to track changes and could be used as part of a continuous monitoring audit programme.

V$PARAMETER
The entity being audited should also have a policy on how its Oracle databases are configured. Much of this configuration is reflected in Oracle initialisation parameters, which can be retrieved from the V$PARAMETER view. Examples of parameters include those for enabling the auditing of operations issued by privileged users, such as DBAs, or whether case-sensitive passwords are required.

There are approximately 260 Oracle initialisation parameters and a full list may be found in the Oracle Database Reference. However, a key concept of this approach is that not all the parameters of interest for all databases need to be reviewed. Again, once one database is known to be compliant to the standards, it can be used as a master in the CAATs tool to compare the parameters of interest across all of the databases. This can be done by joining on the field name (from the V$PARAMETER layout) and displaying all records where the value is not equal. As above, in this manner noncompliant configurations can be quickly flagged for follow up and review.

DBA_USERS
DBA_USERS describes all users of the Oracle database. This includes username, account status and, in Oracle databases up to and including 10.2.0.5, the password hash.

The password is up to 30-characters long with all characters converted to uppercase before the hashing is performed. Furthermore there is no real “salt”—the algorithm simply uses the username. This means that the username password combinations sys/temp1 and system/p1 have the same password hash. Furthermore, a username installed with the same password on different Oracle databases will have the same password hash. This is often the case when the default value is accepted during database installation. Default passwords pose a real and common risk to Oracle database installations.

The threat is so common that a list of default Oracle password hashes is maintained online. This is maintained in various formats, including CSV and Excel, that can be imported easily into the CAATs tool. This list of default password hashes can then be compared against DBA_USERS (joining on the field password) across all of the entity’s databases—anywhere the password hashes match indicates the use of a default password. These should be reviewed immediately.

DBA_USERS can also be compared to other sources of information, for example, the entity’s payroll to flag leavers and movers. (Note: From Oracle 11g, the new view DBA_USERS_WITH_DEFPWD displays all users who are still using their default passwords.)

Other Views
As there are hundreds of Oracle views, it is not possible to discuss them all in this article. Those mentioned are for illustrative purposes. The view(s) used depends on the purpose of the audit, but could also include:

• Any of the views described in ISACA’s Oracle Audit/Assurance Program and ICO
• DBA_ROLES, which lists all the roles that have been defined in the database. It could be reviewed to ensure that the roles are appropriate and password-protected, where applicable.
• DBA_ROLE_PRIVS, which identifies the roles granted to users or other roles. This could be reviewed to ensure that the role privileges granted to users are appropriate and under the principle of least privilege.
• DBA_SYS_PRIVS, which lists all systems privileges granted to users or roles. This could be reviewed to ensure that the system privileges granted to users are appropriate and under the principle of least privilege.
• DBA_TAB_PRIVS, which lists all table privileges granted to users or roles. This could be reviewed to ensure that the table privileges granted to users are appropriate and under the principle of least privilege.
DBA_OBJ_AUDIT_OPTS, which lists the auditing options on all objects. This could be reviewed to ensure that the auditing enabled is appropriate for the sensitivity of the data in the database.

DBA_PRIV_AUDIT_OPTS, which captures granting of system privileges. This could be reviewed to ensure that system privileges are only granted to appropriate users under the principle of least privilege.

DBA_STMT_AUDIT_OPTS, which captures issued statements. This could be reviewed to ensure that statements were issued by appropriate users and under the principle of least privilege.

DBA_DB_LINKS, which lists information about connections to other databases. This could be reviewed to ensure that connections to other databases are private and granted under the principle of least privilege.

V$VERSION, which lists version and status information for component Oracle products. This could be reviewed to ensure that the current version installed is fully supported.

V$LICENSE, which lists database licence information. This could be reviewed to ensure that the audited entity is in compliance with all Oracle licensing requirements.

A full list of Oracle views along with more detailed explanations may be found in the Oracle Database Reference. However, the key point is that any of the views may be output to CSV files and imported into a CAATs tool. These may then be:

- Compared to other Oracle databases, including a master that is known to be compliant to the standards
- Compared to development, test or quality assurance versions of the production database (useful for change control)
- Compared to other sources of data. This can include data from internal or external entities.

CONCLUSION

CAATs are a valuable tool for auditing Oracle databases. With the proposed CAATs, there are little or no set-up costs, because frequently the organisation is already using CAATs software. Furthermore, the approach allows external consultants and geographically dispersed companies to request that queries be run by the local DBA without the need to compromise the administrator password. The DBA of the audited entity can also review the SQL being run over the database to ensure that it will have no effect on the production environment.

Once the queries are run, they can be securely emailed or otherwise transferred for analysis. Query results can be compared against known compliant databases to highlight areas of audit concern. Query results can also be compared against preproduction databases and other sources of data, such as the company payroll. Finally, the entire process can be repeated and used as part of a continuous monitoring and/or audit.

ENDNOTES

2 Oracle, Oracle Database Reference 11g Release 2 (11.2), http://docs.oracle.com/cd/E11882_01/server.112/e25515.pdf
3 ISACA, Knowledge Center, www.isaca.org/Groups/Professional-English/oracle-database/GroupDocuments/Oracle.SQL
4 Op cit, Oracle, p. 17-3
8 Op cit, Oracle, p. 1-4
9 Op cit, Oracle, p. 8-52
12 Op cit, Oracle, p. 5-49
13 Op cit, ISACA, 2009
14 Op cit, Oracle
The importance of information technology to an organization’s productivity, profitability and processes is increasing exponentially. There is unprecedented reliance on the IT infrastructure to leverage product design, marketing and reporting; handle management of information; and enhance service deliverables. As dependence on IT systems increases, the associated risk increases.

In recent years, as the result of increased system interconnectivity, government and private facilities transitioning from paper to electronic data storage, enhanced traffic in e-channel trading platforms, and improved technology products (e.g., cloud services), the cyberincident has become one of the most reported types of IT security breaches. The impact, frequency and magnitude of cyberincidents have reached an all-time high; in business continuity planning for cyberincidents, the notion of if has turned to when these incidents will occur. In the first quarter of 2013, five of the major US banks suffered denial-of-service (DoS) attacks; Twitter, Facebook, Microsoft and Apple systems were hacked; and in South Korea, financial institutions’ and media houses’ systems were crashed by hackers.

The financial and reputation cost associated with cyberattacks is high. Organizations should implement risk management strategies to help delay, deny, destroy and document cyberattacks. Risk management objectives are to protect assets, conserve resources and improve the quality of decision making. Risk management strategies include risk acceptance (taking on risk and making budgetary provisions for the expected loss), risk mitigation (implementing strategies to contain risk and the effects), risk avoidance (eliminating risk by avoiding processes, events or actions that create risk) and risk transfer (transferring the liability arising from risk to third parties).

Cyberinsurance policies are one product developed to cater to the transfer of risk emanating from cyberactivities. In 2012, cyberinsurance premiums in the US rose from US $800 million to more than US $1 billion. The market is expected to grow an additional 25 percent within the next five years. As the market continues to grow, the role of information systems (IS) professionals in identifying cyberexposure, enumerating preventive techniques and determining security gaps will become more critical. The adoption of cyberinsurance as the strategy for risk transfer by many organizations has created another frontier for IS auditors to explore and review. For effective and efficient auditing of a cyberinsurance policy’s adequacy, completeness and appropriateness, IS auditors need to understand cyberinsurance intricacies and complexities.

**REASONS FOR CYBERINSURANCE**

Preventive, detective and corrective controls implemented by an organization cannot completely eliminate cyberincidents. Cyberinsurance is a way to handle the residual risk. It is an insurance product used to protect organizations from Internet-based risk as well as that of other related IT activities, tools and processes. Gone are the days when organizations that suffer a cyberattack keep the information secret; now, industry regulators and media act as enforcers of transparency. The US Securities and Exchange Commission CF Disclosure Guidance mandates that companies report the material risk associated with specific data breaches or other cyberincidents; companies must disclose the financial cost, legal cost and document control in place to guide against future recurrence. Hackers are becoming more forthcoming, using YouTube, Twitter and other social media to disclose their exploits and compromised data. The competition for news by 24-hour cable networks also ensures that all news is reported.

Governments and various industry regulators have also intensified pressure on businesses to protect personal data, using significant fines for any breaches. In the US, 46 states have enacted legislation that mandates that businesses notify customers of data breaches. US federal laws such
as the Graham-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA), the European Data Protection Directive (2003), the Japanese Personal Identifiable Information Law (2005), and other international privacy laws also hold organizations liable for a customer data breach.

In 2011, one question in the PricewaterhouseCoopers Global State of Information Security Survey was, “Does your organization have an insurance policy that protects it from theft or misuse of electronic data, consumer records, etc.?” Of the 12,840 worldwide respondents, 46 percent answered yes.3 There is not only an increase in reliance on cyberinsurance policies as a risk transfer strategy, but also in acceptance of the product by organizations.

TYPES OF CYBERINSURANCE
The most common types of cyberinsurance are first-party risk exposures and third-party risk exposures. First-party coverage insures against damage to and costs incurred directly by the insured organization in responding to cyberbreaches and cyberattacks. Figure 1 describes the types of exposure covered by first-party insurance.

Third-party coverage insures against liability, damages, attorney fees, costs and expenses incurred in responding to allegations against an insured company made by third parties arising from cyberattacks and cyberbreaches. Figure 2 shows some types of exposure covered by third-party insurance.

<table>
<thead>
<tr>
<th>Risk Exposure</th>
<th>Description</th>
<th>Attack Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss or damage to IT asset</td>
<td>This covers damage to IT infrastructure, damaged software or data loss. It covers the cost incurred to restore or replace the asset.</td>
<td>Virus attack, injection attack, malware attack, web site defacement, destruction of network hardware</td>
</tr>
<tr>
<td>Business interruption/denial</td>
<td>This covers income loss from interruption or denial of usage of network resources for a particular point in time.</td>
<td>DoS, restriction of URL access, theft of IP or trademark, cyberattack</td>
</tr>
<tr>
<td>Reputation loss</td>
<td>This covers losses incurred from loss of intellectual property, loss of customer patronage or damage to the organization’s goodwill.</td>
<td>Phishing email, web site defacement</td>
</tr>
<tr>
<td>Electronic theft</td>
<td>This covers the direct loss of money in the cyberworld.</td>
<td>Cross-site scripting, Trojan horse</td>
</tr>
<tr>
<td>Cyberextortion</td>
<td>This covers the cost of payments associated with threats to destroy a network or release private information.</td>
<td>Cyberbullying</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Exposure</th>
<th>Description</th>
<th>Type of Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis services cost</td>
<td>This includes costs associated with investigation, notification, credit monitoring and associated reputation damage.</td>
<td>Malware attack, credit card data compromise, data breach</td>
</tr>
<tr>
<td>Cost of legal damages</td>
<td>This includes defense costs, settlement of liability and civil liabilities.</td>
<td>Violation of regulations</td>
</tr>
<tr>
<td>Fines</td>
<td>These include awards and fines resulting from an investigation or enforcement by a regulator associated with security or privacy liability.</td>
<td>Data breach resulting from exposure of customers’ medical records</td>
</tr>
<tr>
<td>Third-party asset loss</td>
<td>This includes liability for damage to, or corruption of, third-party assets or data loss.</td>
<td>Malware, virus attacks using the insured firm as the platform to launch, botnet</td>
</tr>
</tbody>
</table>

CYBERINSURANCE POLICY AUDIT OBJECTIVES
To perform an audit in an effective and efficient manner, the auditor must understand the objective of the exercise. Some of the objectives of cyberinsurance audits include:
- Verifying the effectiveness of the risk management process
- Determining that adequate procedures have been developed to identify and analyze risk, implementing processes to decrease exposure, and monitoring progress
- Ensuring that cyberinsurance coverage is adequate to compensate for identified risk
- Determining that the cyberinsurance policy covers all critical IT infrastructure
- Verifying the existence and adequacy of procedures for reporting incidents and making claims
The auditing of cyberinsurance policies can be divided into two major components:

1. **Condition precedent to the cyberinsurance policy**
   - The IS auditor must understand the business, critical assets and IT infrastructure in order to properly audit the cybersecurity policy. The auditor should use this baseline knowledge to review the condition that necessitated the purchase of the cyberinsurance policy. The following are issues IS auditors should consider:
     - **Review the network diagram and the business process flow chart.** The network diagram shows the sequence of steps to depict the IT infrastructure and to identify critical processes that need to be protected. The network diagram should be updated regularly.
     - **Check whether the organization’s risk management framework identifies and classifies all IT assets according to their criticality to the business.** All assets must be ranked according to their importance. The IS auditor should check the completeness of the asset documentation, ensuring that all critical assets are documented, ranked and continuously reviewed as processes change.
     - **Verify whether risk management strategies are updated periodically and reflect the current business and IT infrastructure.** In this era of zero-day exploits, defense mechanisms should be reviewed daily.
     - **Evaluate the adequacy of IT security strategies.** The IS auditor should review IT security, tools and processes for adequacy. Preventive controls are the first step to a secure system.
     - **Review the IS incident report within a specific period.** The incident report will enable the IS auditor to understand the historical trend of attack, targeted systems and channel of attack.

     The IS auditor understands that the objective of cyberinsurance is to relieve the insured of the financial losses these cyberactivities bring. Concurrent with obtaining the cyberinsurance policy, the IS auditor should take the following steps:
     - **Obtain the sample proposal form submitted by the organization to the insurance provider to evaluate the completeness and truthfulness of the data therein.** The proposal form documents the nature, size and complexities of the network, data structure, security system in place and the entire IT infrastructure. The insurance company uses the information in the proposal form to determine premiums and make other insurance decisions. In the event of a claim, the policy may be declared null and void if it is discovered that the organization deliberately or mistakenly omitted critical information in the questionnaire. The IS auditor should verify the truthfulness of detail in the proposal form, and management should be notified of any inaccurate answers.
     - **Obtain copies of the insurance policies, and review them for adequacy of coverage and assurance that all critical areas have been included in the policy.** If the policy does not cover all systems that are critical and prone to incident based on the organization’s past security incidents or industry trend, the auditor should analyze the impact and notify management. An example of this would be an online retailer that stores customers’ critical credit card data in third-party cloud storage, but fails to cover the asset in a cyberinsurance contract. The retailer has limited control over the security of the cloud operations, but has complete responsibility to ensure the security of customers’ data.
     - **Validate the security measures that are in place.** Prior to issuing an insurance policy, the organization must submit a security status in the proposal form. The IS auditor should test the existing control for adequacy. Management should be promptly notified of any security gaps.
     - **Examine the incident reporting documentation.** The IS auditor should ensure that the adequacy of the reporting incident is in tandem with the cyberinsurance policy.
     - **Interview IT employees to verify whether cyberinsurance policies and procedures have been communicated to the appropriate personnel.** Employees should have adequate knowledge of the cyberinsurance policy, reportable incidents and steps to be taken in the event of a covered incident. A successful claim is dependent on the actions taken within a few minutes of the insured incident.

2. **Condition concurrent with the cyberinsurance policy**
   - The IS auditor understands that the objective of cyberinsurance is to relieve the insured of the financial losses these cyberactivities bring. Concurrent with obtaining the cyberinsurance policy, the IS auditor should take the following steps:
     - **Discuss and collaborate on audit tools and techniques and cybersecurity in the Knowledge Center.**
     - **www.isaca.org/knowledgecenter**
• Determine how material changes in the IT infrastructure are communicated to the carrier, and obtain a copy of the physical assets covered in the policy to compare with the present assets. Any exceptions noted should be reported for action.

• Select a sample of claims or covered incidents from previous years to determine any remedial action that can be implemented to reduce the risk of incidents. Any reported increase in incidents should be investigated and resources diverted as appropriate.

CONCLUSION
Cyberattacks and the resulting security breaches are part of the rapidly expanding security threats organizations face. The frequency, nature and cost of cyberincidents are growing at an alarming rate. IS auditors must ensure that the organization adequately protects itself and safeguards critical data. IS auditors must plan for cyberinsurance policy audits as part of risk management reviews or as a stand-alone review.

Cyberinsurance is not a mandatory requirement, but as more organizations adopt this strategy to transfer risk, IS auditors must understand the processes and test the insurance policy for completeness, adequacy and integrity.

ENDNOTES
Organizations maintain their operations with the help of processes that differ according to their organizational structure, business objectives and working styles. A process determines and manages numerous linked activities within an organization to help ensure that the organization functions effectively. It is “an activity or set of activities using resources, and managed in order to enable the transformation of inputs into outputs.”1 Furthermore, processes for managing IT operations should be formed because IT is a part of every business process.

The processes described in this article were identified as critical from the viewpoint of using confidential information in business operations. These processes have been chosen by taking into account the requirements of well-known IT frameworks and standards that provide a general understanding of the processes that need to be established within organizations. COBIT®, the Project Management Body of Knowledge (PMBOK), the Capability Maturity Model Integration (CMMI), the IT Infrastructure Library (ITIL), ISO 27001, The Open Group Architecture Framework (TOGAF) and ISO 9001:2008 were considered in preparation of these critical processes. The chosen processes are also included in the Certified in Risk and Information Systems Control (CRISC) Review Manual.

In COBIT® 5, the concept of critical IT processes is stressed and required in processes DSS01.02 (integration of critical internal IT management processes with those of outsourced service providers) and MEA01 (percent of critical processes monitored). In MEA02, the percent of critical business processes covered by risk assessment is defined as a process performance metric.2, 3

While these methods often differ based on the organization’s approach to problem solving and its targeted audience, the most important common issues were taken into consideration in order to develop this list of critical IS processes (figure 1).

### Figure 1—Presence of Critical Processes in Key Frameworks/Standards

<table>
<thead>
<tr>
<th>IS Process Name</th>
<th>COBIT</th>
<th>PMBOK</th>
<th>CMMI</th>
<th>ITIL</th>
<th>ISO 270001</th>
<th>TOGAF</th>
<th>ISO 9001:2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determining the IT strategy</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Project and program management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Change management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Third-party service management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Continuous service assurance</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Information security management</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Configuration management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Problem management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Data management</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Physical environment management</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>IT operations management</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

(+) Related process is included in the standard/framework.  
(-) Related process is not included in the standard/framework.

---

2. Tugba Yildirim, CISA, CGEIT, CRISC, works in the information systems (IS) control and audit function at Bank Asya, Turkey, where she specializes in IS control design, testing, monitoring and governance. Yildirim’s background includes IS, instructional technology and management of IS education. She can be reached at tugbametu@gmail.com.
3. Bilgin Metin, Ph.D., has more than 15 years of experience in the IT sector. Metin is an assistant professor in the Management Information Systems Department at Bogazici University (Istanbul, Turkey). He can be reached at bilgin.metin@boun.edu.tr.
DETERMINING IT STRATEGY
Strategy is the first step in determining the organization’s direction, and “technology has become so embedded in the internal functions and the external value propositions of modern organizations that it is impossible to execute strategy in any organization without it.” The IT strategy should be in line with the organization’s objectives in order to support the business in achieving its strategic goals. There should be a clear strategy for information transfer from organization management to IT management, and mechanisms should be in place to align with these strategies. There should be no discrepancies between the organization and IT strategy; any discrepancies here would conflict with the aim of advancing strategic goals. A strategy plan should be developed and regularly updated for compliance with changing business needs and objectives. This process should also comply with any new competitive changes in the environment and should provide for updating the strategy according to these changes to catch up with the evolving environment.

THE PROJECT AND PROGRAM MANAGEMENT PROCESS
Business objectives can be achieved only by following the business strategy. “If IT is to deliver the services that a business needs now and in the future, it has to be managed by the business as a whole.” This can be done by allocating resources and budget in line with business priorities. Doing the right projects with the right prioritization is significant; therefore, project and program management plays a crucial role. Project planning, relationships among projects, resource planning and project budgeting should be established according to business priorities. In addition, requirements planning, risk management, testing, quality management and stakeholder approval phases have critical importance on the project’s success. Project success should be reviewed to ensure that value is delivered to the organization.

THE CHANGE MANAGEMENT PROCESS
Since business environments undergo rapid changes, organizations are expected to adapt and, thus, must reevaluate business goals and direction. This makes the change management process crucial since keeping up with these changes carries new risk and opportunities to the organization. “Competitive pressures, rising expectations from global customers and the emergence of newer technologies, especially in the area of telecommunication, have accelerated the process of change management.” In order to manage changes to take advantage of opportunities in business and to minimize the related risk, the change management process should involve a number of phases: monitoring and taking change requests, prioritizing them, evaluating the change impact, taking the appropriate stakeholder approvals, tracking the status of the changes to ensure that they are done as planned, and reporting.

THE THIRD-PARTY SERVICE MANAGEMENT PROCESS
As organizations focus on their primary service area, they may get some outsource support for their operations. This is common in IT since IT is an integral part of business operation support. Third-party services directly affect the organization’s business operations, and management of these services is significant. Every detail about the service requirements, roles and responsibilities, communications, legal obligations, payment, support, and cancellation should be determined and written into the contract. This process should also include compliance monitoring of third-party contracts. “Properly constituted organizations have the capacity to enter into contracts with one another, and many legal endeavors go into working out the terms of the contract, as well as assessing how its terms are complied with during the duration of the contract.”

THE CONTINUOUS SERVICE ASSURANCE PROCESS
“The confidentiality, integrity and availability of information systems must be ensured to protect the business from the risk relating to IT.” Organizations may face some disruptions such as natural disasters or service outages. Organizations should take precautions so that these disruptions are not reflected on their customers and service continues. This process determines critical business processes and ensures the continuous backup to an alternative site away from the risk associated with the main site.

Roles and responsibilities are important in the event of a disruption; all critical personnel should know how to act. Manuals and communication information should be
in place at the staff members’ homes and at the alternative site. Continuity should be periodically tested to ensure its applicability. The business continuity plan should be documented clearly and updated periodically. This process is significant since organizations are expected to serve the customer continuously and to cope with such disruptions.

THE INFORMATION SECURITY MANAGEMENT PROCESS
Information is the most important asset of the organizations; it is indispensable to its operation. There are remarkable issues to consider in using IT as a support for business operations. IT assets should be protected against vulnerabilities and incidents in order to minimize the business impact of damaged security. Information systems security management essentially belongs to risk management, handling the threat of attacks on the system and dealing with the threat posed by vulnerabilities.

This process should include determining security roles and responsibilities, information security rules, procedures, policies, and standards. Monitoring noncompliance to security policies and related rules and periodically testing to ensure the safety of information systems should be established in the organization. Corrective and improvement actions should be maintained to ensure that risk is minimized. Security management should be performed effectively to ensure the protection of information assets and continuity of services. To accomplish this difficult task in today’s risky technology environment, new risk factors and threats should be continuously reviewed and appropriate mechanisms should be established rapidly.

THE CONFIGURATION MANAGEMENT PROCESS
Providing for system availability, production issue management and recovery from erroneous operations is important for business continuity, safety and customer satisfaction. The configuration management process aims to accurately and completely configure inventory. Backing up the configuration information is a part of this process as it helps return business to its original or previous state when a problem occurs. Integrity of these configurations should be monitored and tested periodically as part of this process.

THE PROBLEM MANAGEMENT PROCESS
It is common to face problems in ongoing business operations related to IT. Organizations establish problem management processes to return to normal operation of business activities as soon as they can. Recognizing the problem, communicating the problem to appropriate parties, conducting a root-cause analysis, determining the solution, undertaking the appropriate stakeholder approval for solutions, resolving the problem and monitoring the status of the problem are important stages of the process. Documentation and reporting for knowledge sharing are also significant for this process in order to accelerate the resolution of known problems.

Periodic analysis of the problems encountered can result in process improvements that can improve the organization’s ability to perform business activities.

THE DATA MANAGEMENT PROCESS
An entity’s information assets constitute a significant portion of the entity’s market value, making this a key enterprise asset that needs to be governed effectively. Business operation’s quality is strictly related to the timeliness, availability and quality of business data. Accuracy, consistency, completeness, confidentiality, integrity and availability are desired characteristics of data for business use. To accomplish this task, it is important to establish a data management process.

This process should involve determining the data storage and retention requirements with business management, establishing and maintaining a media library, protecting data, backing up data, and restoring and disposing of data and sensitive media.

THE PHYSICAL ENVIRONMENT MANAGEMENT PROCESS
Physical facilities should be managed to protect computer and related equipment. Appropriate physical conditions should be selected for business continuity. Computer and related equipment should operate effectively in the selected environment. Establishing and maintaining this process could help organizations to minimize damage to the physical facilities and, therefore, minimize interruption to business operations. Protection of the physical facilities includes...
protecting physical facility staff. This process also reduces the organization’s resource allocation for maintenance.

THE IT OPERATIONS MANAGEMENT PROCESS
Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware.12 This process is crucial since operating policies and procedures need to be defined and standardized to help safeguard the continuation of business activities. Performance monitoring for infrastructure and related technology should be established, and information mechanisms for the detected events should be set up. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.13

CONCLUSION
Determining critical IS processes is crucial in order for organizations to prioritize their efforts toward achieving business objectives. Perhaps the most important improvement will be the extension of the domain and range of these processes from the IT arena into corporate operations.

When classifying the scope of operations, the domain of these critical processes could be decomposed; the components of the domain might facilitate the application of these processes in the everyday life of a business. A possible partition may be the three pillars: organizational, regulation and technical, which were first defined as pillars of IT and later generalized to pillars of operations.14, 15

These critical information processes can also be used as a reference for MEA01 and MEA02 processes in COBIT 5 to prioritize critical information systems processes.

ACKNOWLEDGEMENTS
The authors would like to thank Katalin Szenes, Ph.D., Obuda University, for her valuable comments.

ENDNOTES
2 Business objectives can be achieved only by following the business strategy. ISACA, COBIT 5, 2012, www.isaca.org/cobit
3 In COBIT® 4.1, the concept of critical IT processes is stressed and required under many control objectives, including PO4.11 (importance of segregation of duties), PO7.5 (dependence upon individuals for critical processes) and ME2.2 (managerial oversight for critical processes).
9 Op cit, ISACA, 2012
12 Op cit, ISACA 2012
13 Ibid.
The Effect of the COSO 2013 Update on IS Professionals

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the Internal Control—Integrated Framework in 1992. In the more than 20 years since, the framework has become the accepted general internal control framework of the US Securities and Exchange Commission (SEC), American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), Financial Executives International (FEI), and many other professional organizations and standard setters. Because of intervening changes in business models and best practices since 1992, such as economic globalization, electronic commerce, outsourcing and the pervasive use of IT, COSO initiated a project in 2010 to update the 1992 framework. After appropriate due process, including review and input from the internal control (IC) community, this project culminated in May 2013 with the publication of the revised framework.

IT professionals must be aware of the recent, important changes in the COSO framework and especially how/why these changes are pertinent when using ISACA® standards and framework documents such as the ISACA Code of Professional Ethics, IT Assurance Framework® (ITAF®), and COBIT® 5.

Both the 1992 and 2013 frameworks are structured around three categories of enterprise objectives and five components of an IC system to mitigate the risk to achieving those objectives. This objectives/components framework can be applied at any/all levels of the enterprise structure—all the way from the entity (highest) level down through the cascading levels of division, operating unit and, finally, the individual process (lowest) level.

THE 1992 FRAMEWORK
COSO depicts the 1992 framework as a three-dimensional cube with the three axes representing enterprise objectives, IC components and enterprise levels (figure 1). The slices on each axis of the cube intersect each of the slices on the other axes and, thus, the framework components apply to each enterprise objective and level. The five components of the IC framework do not represent a list of the actual controls as many users interpret. Individual controls are not specified by COSO (although individual controls are mentioned in the many examples contained in the document), and, in practice, a single individual control usually supports multiple components.

Since the 1992 and 2013 frameworks incorporate the same fundamental model of three objectives and five components, it is important to completely comprehend this structure so one can apply it in practice.

Figure 2 offers a Unified Modeling Language (UML)-structured classifier diagram and is presented here as an alternate model of an organization and its IC system. It presents another view that shows the presence of risk and eludes the various levels of the organization. A UML-structured class diagram (also known as a UML...
composite structure diagram) depicts the structure of a class as consisting of (i.e., encapsulating) internal parts that may be connected via relationships (the lines in figure 2) to each other and/or to the outside environment. The parts internal to the main class rectangle may also be modeled as a subordinate class rectangle with its own internal part structure, so the diagram can show structure of the whole system as multiple levels of internal parts for a view of increasing amounts of structural detail. The number of levels of detailed parts to show in a structured class diagram is chosen by the presenter as a trade-off between detail and complexity.

Figure 2—UML Structured Class: Organization With Internal Parts

In figure 2, the organization (a class depicted by the large outside rectangle) is shown as composed of three internal parts: objectives, risk to achieving those objectives and an IC system connected to the risk through some type of interface (represented by the lollipop and socket). The objectives part has its own internal parts consisting of three COSO-defined enterprise objective types involving operations, reporting and compliance. The IC system part also has its own internal parts, consisting of five COSO-defined components. Figure 2’s risk part does not show any lower-level internal parts, even though they exist, because additional detail about risk is not the primary topic here.

Comparing figures 1 and 2, one can see that figure 1 does not show risk in its structure. Figure 2 does show risk, but does not depict enterprise levels in its structure. Even though figures 1 and 2 depict different views of an organization and its IC system and have some differences in structure, an analysis and comparison of the two figures shows that their different structures can be reconciled and that they show alternative views of the same thing: an organization and its system of IC. UML-structured classifiers are used here to model various objects and concepts in the revised 2013 COSO framework.

Many practitioners find the 1992 framework difficult to apply in practice due to:
• The complex interaction and relationships among objectives, risk, components and levels, as shown in figures 1 and 2
• The generic, conceptual (as opposed to precise) definitions/descriptions of the five components and how they relate to actual, individual internal controls in practice
• The absence of a list of specific controls to use in typical practice situations
• The limited and dated discussion of IS/IT risk and controls

Many IC framework users look for a simple checklist of standard, recommended controls, and instead, the 1992 framework presents an abstract and conceptual discussion.

THE 2013 FRAMEWORK

The 2013 framework keeps the same three-objective and five-component structure as 1992, but adds depth (more detailed structure) and clarity (easier to use in practice). The 2013 framework differs from 1992 at the more detailed lower levels of structure for the reporting objective and for each of the five components. The 2013 framework also clarifies the definition of control deficiencies and effective (vs. ineffective) system of IC. IT and its effect on risk and control is discussed frequently and in depth throughout the 2013 framework.

The three enterprise objectives from 1992 have been preserved, but the reporting objective definition and discussion is expanded in significant ways in the 2013 update.
The framework now includes internal reporting (in addition to external) and nonfinancial reporting (in addition to financial). These expansions greatly increase the scope of the framework guidance. Figure 3 presents a UML-structured class diagram of the 2013 reporting objective with four internal parts made from combinations of internal/external and financial/nonfinancial reporting.

This addition to the reporting objective is a major revision and clarification of the 1992 framework and is very important to IS/IT professionals. The 1992 reporting objective was generally interpreted as covering only external financial reporting, which is only one of the four subobjectives (parts) in the 2013 framework, as shown in figure 3.

Figure 3—2013 Framework Reporting Objective With Internal Parts

### REPORTING OBJECTIVE

<table>
<thead>
<tr>
<th>Internal</th>
<th>Financial</th>
<th>External</th>
<th>Financial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Nonfinancial</td>
<td>External</td>
<td>Nonfinancial</td>
</tr>
</tbody>
</table>

### 2013 PRINCIPLES AND POINTS OF FOCUS

Perhaps the major enhancement and clarifying change in 2013 is the introduction and integration of control principles and related points of focus into the five components. In the discussion of the five components in the 1992 framework, many fundamental concepts of IC were covered in a somewhat difficult-to-summarize discussion. In the 2013 framework, these concepts have been formalized and enumerated into 17 principles that are associated with (listed under) the five components. The following is a list of the five components and abbreviated descriptions of the associated 17 principles:

- **Control environment component:**
  1. The organization demonstrates a commitment to integrity and ethical values.
  2. The governing body (board of directors [BoD]) demonstrates independence from management and exercises oversight of IC.
  3. Management establishes, with BoD oversight, the organizational structure and assigns authority and responsibility for IC.

4. The organization demonstrates a commitment to attract, develop and retain competent employees.

5. The organization holds employees accountable for IC responsibilities.

- **Risk assessment component:**
  6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risk to those objectives.
  7. The organization identifies risk to the achievement of its objectives and analyzes risk to determine the risk response.
  8. The organization considers the potential for fraud when assessing risk.
  9. The organization considers the impact of changes in the external environment and within its own business model that could impact the system of IC.

- **Control activities component:**
  10. The organization selects and develops control activities to mitigate risk to achieving objectives.
  11. The organization selects and develops IT general control (ITGC) activities.
  12. The organization deploys control activities utilizing policies and procedures.

- **Information and communication component:**
  13. The organization obtains or generates and uses relevant and quality information to support the functioning of IC.

14. The organization internally communicates the information, including objectives and responsibilities concerning IC.

15. The organization externally communicates regarding matters affecting the functioning of IC.

- **Monitoring activities component**
  16. The organization selects, develops and performs ongoing and/or separate evaluations (i.e., audits, assessments, assurances) to ascertain whether components of IC, including the principles embedded in the components, are present and functioning.
Each of the three second-level internal parts (representing 2013 principles 10, 11 and 12) in Figure 4 has internal third-level parts of its own, which are the focus points defined for principles 10, 11 and 12. These focus points are shown inside each principle part, as a bullet. Figure 4 does not list all of the focus points for principles 10, 11 and 12. The last three focus points in principle 11 identify the three categories of ITGCs defined by the 2013 framework.

These principles and focus points make management’s and/or the auditor’s assessment of IC, when utilizing the 2013 framework, a more logical, inductive-based analysis.
implementation of and compliance with appropriate standards of control and risk management.” Item 5 states that they must “maintain competency in their respected fields…and only perform assignments where…they have the necessary skills, knowledge and competence.” Thus, COSO, because of its reputation/status as the most widely accepted IC framework and recent revisions, making it more applicable to IS/IT, becomes required reading and comprehension for many ISACA members and certification holders.

**ITAF and the 2013 Framework**

ITAF is a comprehensive and good-practice-setting reference model that establishes standards and guidelines to address IS audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements. *ITAF, 2nd Edition* was released in July 2013 with new IS audit standards and guidelines that reference internal controls in multiple places. Here are just two examples:

- **IS Audit Standard 1008, Criteria,** discusses criteria against which the IS auditor should assess the subject matter. It states that the criteria should be widely accepted and that it is preferable to use criteria published by relevant authoritative bodies.
- **IS Audit Standard 1205, Materiality,** discusses audit risk and assessment of internal controls and their importance in an IS assurance engagement.

The 2013 COSO framework, with its conceptual discussions of risk, control activities, monitoring activities and 17 principles of internal control, should be used as the overall IC framework from which to plan, monitor and assess IC when applying the assurance standards and guidelines found in ITAF.

**COBIT and the 2013 Framework**

COBIT 5 is a business framework for the governance and management of enterprise IT (GEIT). It aligns with other standards and frameworks (such as COSO) to use as an overall and complete enterprise IT integrator using its models of goals cascade and interconnected enablers.

COBIT 5 defines an enabler as a factor that determines whether management of enterprise IT will achieve its objectives. The 2013 COSO framework also defines enterprise objectives and describes an IC system structured with components, principles and focus points that together can assure the achievement of objectives. These components, principles and focus points of the 2013 COSO framework can also be considered enablers of IC. Thus, COBIT 5 and COSO 2013 are conceptually similar, presenting different, but compatible views of IC, and can be used in combination to ensure the accomplishment of enterprise objectives through IT. The 2013 COSO framework is a more general/generic view of overall IC, while COBIT is a more detailed view of GEIT and includes IC arrangements. When used together, COBIT and the COSO framework form a superior tool, as compared to using either one independently.

IC arrangements in COBIT 5 are too numerous to mention here, since it is a comprehensive GEIT framework. Two important IC examples from the COBIT 5 process enabler model are as follows:

- **Process practice DSS06.02, Operate business process activities and related controls to ensure that information processing is valid, complete, accurate, timely and secure.**
- **Process practice MEA02.01, Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.**

**CONCLUSIONS**

The COSO *Internal Control—Integrated Framework* now includes internal and nonfinancial reporting in the reporting objectives covered by IC, and also includes IT general controls as a primary consideration (principal 11) of all IC systems. Thus, it is more applicable and useful to IT professionals than the 1992 version. IS/IT professionals should seek competence in understanding and applying the 2013 content to the governance, management and assurance of enterprise IT, and should, therefore, include the COSO 2013 framework in their schedule of future continuing education.

**ENDNOTES**

3 ISACA, Code of Professional Ethics, www.isaca.org/ethics
4 ISACA, IT Assurance Framework (ITAF), www.isaca.org/itaf
5 ISACA, COBIT 5, 2012, www.isaca.org/cobit
6 UML defines a class as a thing of importance in a system. A class has structure and behavior and an IC system is a class composed of many internal parts that are classes themselves.
7 The IS audit standards in *ITAF, 2nd Edition* became effective on 1 November 2013.
The internal audit and information security functions should play complementary roles in an organization’s information security program. The information security function should focus on the design and implementation of the security plan, while internal audit should assess and evaluate the functioning of the plan’s components.\(^1\)\(^,\)\(^2\) Yet, in practice, the relationship between the two functions is not always positive.

At its worst, the relationship can become so adversarial that it impairs effective governance, as exemplified by one information systems (IS) manager: “…It has been a game of cat and mouse. The auditors are trying to catch IT doing something and IT is trying to prevent audit from finding out.”\(^3\) In part, this may reflect the general friction between the accounting and IS functions.\(^4\) But, it also likely reflects the tension that exists among the information security function and other compliance-oriented groups (e.g., records management\(^5\) within the organization.

What causes friction between the internal audit and information security functions? What actions can management take to improve that relationship? What are the benefits, if any, of having a better relationship between internal audit and information security?

A multistage research program was undertaken to answer these questions. First, in-depth interviews with both internal audit and information security professionals at four organizations were conducted.\(^6\) Then, the insights from those interviews were used to design two survey-based studies. The first survey collected data from IS professionals across a variety of industries,\(^7\) the results of which are analyzed here, and the other collected data from internal auditors, the results of which will be analyzed in part 2.\(^8\) Figure 1 shows the characteristics of the information security professionals who completed the survey.

**FACTORS AFFECTING THE INTERNAL AUDIT TO INFORMATION SECURITY RELATIONSHIP**

Figure 2 illustrates the three factors that information security professionals describe as important drivers of the quality of the relationship between the internal audit and information security functions:

1. The perceived role of internal audit
2. The organization’s structure
3. The communication approach
2. Perceptions about internal audit’s level of information security expertise
3. The frequency with which internal audit reviews various aspects of information security

The importance of internal audit’s perceived level of information security expertise and the frequency of audit reviews were corroborated in a follow-up survey study.

Perceived Role of Internal Audit
In the interviews, information security professionals indicated that how internal auditors approached the review of information security profoundly affected the quality of the relationship. At one extreme, the auditors could be perceived as “the police” who were out to catch mistakes; at the other extreme, they could be viewed as consultants or advisors. Not surprisingly, the two examples had markedly different effects on the quality of the relationship. When auditors were viewed as “the police,” the relationship was formal, reserved and even adversarial; but, when auditors were perceived more as advisors and consultants, the relationship was more open and positive. The latter view was most clearly explained by the information security manager who provided the comment about the “cat-and-mouse” game quoted earlier, who said: “We can leverage each other’s expertise and position in the organization to make things happen. Many times the IT department will tend to almost hide things from audit because they do not want to get a black eye and we don’t have that issue here so much…we have the same goals.”

An information systems professional at another institution expressed a similar comment, saying, “[Our relationship is] exceptionally strong to the point that we’ve just realized we have a codependent relationship. It’s been very positive.” These positive comments are related to the issue of trust. As the information security manager interviewed who talked about the typical “cat-and-mouse” relationship said, “I trust that [the internal auditor is] not out to catch anybody doing anything. He’s out to identify and reduce risk.” However, when attempting to build a good relationship, auditors must be careful not to imperil their objectivity and independence. Moreover, it may be almost inevitable that when auditors are the bearers of bad news in the form of audit findings, they will be viewed as compliance monitors or “the police.” Indeed, respondents to the survey indicated that they saw internal auditors as both monitors and advisors. Consequently, this may be why the survey results did not find a statistically significant relationship between perceptions of audit’s role and the quality of the IT-to-audit relationship. However, the interview data support the argument that auditors should strive not to be perceived as enforcement officers.

---

**Figure 2—Determinants and Outcomes of Relationship Between Internal Audit and Information Security**

- Perceived Role of Internal Audit
- Internal Audit’s Level of Information Security Knowledge
- Frequency of Audit Reviews of Information Security
- Perceived Value Added by Internal Audit
- Relationship Quality (Audit-Information Security)
- Information Security Effectiveness
Not surprisingly, the key factor may be the attitudes of the heads of both functions. As one information security manager stated, “… the executive auditor gets along with our vice president of IT really well, and they understand—again, they don’t just look at one task, they see the whole picture. That’s the most important thing from the workforce point of view. When they see that demonstrated up high, that’s how they follow suit. They watch this, and then they know that’s the expectation and it’s pretty effortless here. People partner and just get along well with the same goal in mind. It shows.”

To capture the information security participants’ view of the role of internal audit in their organizations, participants were asked to rate internal audit’s role in three categories as shown in figure 3.

As indicated in figure 2, participants did not perceive the role of internal audit to significantly impact the overall relationship between information security and internal audit. However, the perception of internal audit’s technical expertise has a significant impact on the quality of the relationship.

In the interviews, IS professionals repeatedly made comments about the importance of internal auditors possessing technical knowledge. For example, one respondent commented, “We’ve actually been very fortunate to hire a very competent IT internal auditor, intimately familiar with ITGC… That’s been really positive. And he’s very technical so that’s a big advantage. Many auditors that I have worked with in the past are not as technical. When [the internal auditor] goes on vacation, I sure am glad to have him return.”

In contrast, the chief information security officer (CISO) at another institution where internal audit did not have much technical skill said, “We see them and we have a very good working relationship with internal audit. However, their focus is typically auditing business processes. You know, ‘are things being done right in payroll?’, and ‘are we handling travel vouchers right?’” Although the CISO stated that the relationship was positive, the overall tenor of the interview indicated that it was really more a case of being nonadversarial than collaborative.

Respondents to the survey corroborated the importance of internal audit possessing strong technical skills, in particular, knowledge about information security. The survey instrument asked information security professionals whether they thought that internal auditors in their organization were “knowledgeable about information security” and whether they kept their “knowledge about information security current” (see figure 4). Higher scores on these two questions were significantly related to more positive views about the quality of the relationship between the two functions.

Taken together, the interviews and the survey clearly indicate that auditors’ technical expertise fosters a good relationship with the auditee (information security).

Frequency of Audit Reviews of Information Security
It is hard to develop a good relationship unless there is fairly frequent interaction. In the context of the relationship between the internal audit and information security functions, the most likely form of interaction involves audit reviews.
However, audit reviews of information security are affected by internal audit’s level of technical expertise, making it difficult to distinguish between the frequency of review and expertise factors in the interviews. For example, the previously quoted CISO who stated that he had a positive relationship with internal audit, but that they focused on business processes (e.g., fraud prevention), also indicated that he did not think the internal auditors in his organization possessed much technical expertise (and the auditor interviewed at that same organization agreed).

In addition to questions about internal audit’s level of information security expertise, the survey instrument also asked questions about the frequency of internal audit reviews of eight aspects of information security (figure 5).

<table>
<thead>
<tr>
<th>Information Security Topics</th>
<th>Mean (Median)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity and disaster recovery</td>
<td>2.72 (3.0)</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>3.17 (3.0)</td>
</tr>
<tr>
<td>Logging and system monitoring</td>
<td>3.00 (3.0)</td>
</tr>
<tr>
<td>Firewalls and other network access devices</td>
<td>2.56 (3.0)</td>
</tr>
<tr>
<td>Encryption policies (including key management)</td>
<td>2.28 (2.0)</td>
</tr>
<tr>
<td>Backup procedures</td>
<td>2.72 (3.0)</td>
</tr>
<tr>
<td>Change management controls</td>
<td>3.00 (3.0)</td>
</tr>
<tr>
<td>Security policies</td>
<td>3.28 (3.5)</td>
</tr>
</tbody>
</table>

Mean and median responses for all aspects were three on a scale of one to five, with one being “not at all” and five representing “often.” The responses ranged across the entire spectrum. Statistical analysis revealed that there was a significant positive relationship between frequency of audit reviews of those eight areas and the overall quality of the relationship between the information security and internal audit functions. Therefore, more frequent interaction in the form of audit reviews improves the relationship. However, the mean and median scores indicate that there is room for further improvement.

**Benefits from a Good Relationship Between Internal Audit and Information Security**

Some of the factors that affect the relationship between the internal audit and information security functions have been discussed. Those factors are clearly items that can be improved by managerial action, for example:

- The leaders of both functions can make an effort to develop a positive relationship.
- Additional resources can be invested to increase internal audit’s technical expertise in matters related to information security.
- Increases in the audit budget can enable more frequent audit reviews of information security.

Nevertheless, such investments are worthwhile only if improving the quality of the relationship between internal audit and information security produces tangible benefits. Figure 2 indicates that it does—better relationships improve perceptions about internal audit’s value as well as the overall effectiveness of information security.

**Perceived Value-Add from Internal Audit**

In the interviews, information security professionals indicated that a positive relationship improved their perceptions about the value added by internal audit. One reason is that information security professionals believe a good relationship with internal audit makes it easier for them to persuade employees and management to support information security initiatives. For example, one CISO stated, “The relationship with internal audit has been very positive…a real big benefit to us achieving a lot of the goals we have from an information security perspective.” The CISO goes on to explain that he feels he can use the audit findings to his advantage, “…and we are going to begin reinforcing the importance of change control. And more importantly, the importance of completed documentation as part of change control for the deployment of new services; and we are going to strongly reinforce through internal audit reports.” The information security manager at another organization described the benefits of a good relationship in obtaining compliance, “If I am just being the IT network police, and I have to get [the internal auditor] and he goes in there with a suit and says ‘here is why you do not want to do this,’ they just usually put their tails between their legs.”

Figure 6 shows the questions used to evaluate the quality of the relationship between internal audit and information security. As with the other questions in the survey, responses ranged from strongly disagree (1) to strongly agree (5).
The higher respondents rated the quality of the relationship between the internal audit and information security functions, the more they agreed with questions about whether the information security professional thought that internal audit findings/reports provided useful information to the information security function and whether internal audit’s capability to review information was being fully utilized.

**Figure 6—Perceived Quality of the Relationship Between Internal Audit and Information Security**

Respondents were asked to respond on a scale from “strongly agree” to “strongly disagree” to the following statements:

1. In my organization, there is little friction between internal audit and information security.
2. In my organization, the relationship between internal audit and information security staff is close and personal.
3. In my organization, there is a good working relationship between internal audit and information security.

**Figure 7—Perceptions of the Value Added by Internal Audit**

Respondents were asked to respond on a scale from “strongly agree” to “strongly disagree” to the following statements:

1. In my organization, internal audit findings/reports provide useful information to the information security function.
2. In my organization, internal audit findings/reports provide useful information to top management about the effectiveness of information security. (Dropped from final model)
3. In my organization, internal audit capability to review information security is fully utilized now.
4. In my organization, internal audit could be more involved in reviewing information security.
5. In my organization, internal audit should be more involved in reviewing information security.

**PERCEIVED EFFECTIVENESS OF INFORMATION SECURITY**

In the interviews, information security professionals expressed a belief that a positive relationship between internal audit and information security functions enabled them to enlist the support and clout of internal audit for information security initiatives. In turn, implementation of those initiatives would improve the overall effectiveness of the organization’s information security. For example, more support from internal audit enabled better change management controls. The results of the survey study corroborated that belief in the benefits of a positive relationship.

Respondents were asked about the trend (questions are shown in figure 8) over the past three years in the number of information security incidents that either interrupted operations or resulted in financial loss, the number of audit findings that related to information security, and the overall effectiveness of their organization’s information security efforts. The results showed that the higher a respondent rated the quality of the relationship between the information security and internal audit functions, the more positive their answers were to those three outcome measures. Thus, information security professionals believe that a good relationship with internal audit improves an organization’s information security.

**Figure 8—Effectiveness of Information Security**

Respondents were asked to respond on a scale from “strongly agree” to “strongly disagree” to the following statements:

1. Over the past three years, in my organization the number of information security incidents that have either interrupted operations or resulted in financial loss has declined.
2. Over the past three years, in my organization the overall effectiveness of information security has increased.
3. Over the past three years, in my organization the number of internal audit findings that relate to information security has decreased.

**CONCLUSION**

COBIT® 5 acknowledges the importance of cross-functional collaboration to achieving effective governance and management of enterprise IT (GEIT). In particular, the internal audit and information security functions can synergistically work together to optimize the overall effectiveness of information security.

Yet in practice, these two functions do not always have a harmonious relationship. Therefore, a multistudy program of research was conducted to investigate the factors that affect the quality of the relationship between these two important functions and the benefits associated with having a positive relationship. This article reported the perspectives of information security professionals about those issues.

A subsequent article will look at these questions from the viewpoint of internal auditors and is planned for publication in volume 3, 2014, of the ISACA Journal.
ENDNOTES


6 Op cit, Steinbart et al., 2012


9 Op cit, Steinbart et al., 2012

10 Ibid.

11 Ibid.


14 Op cit, Steinbart et al., 2012

15 Ibid.

16 Ibid.

17 Ibid.


19 Institute of Internal Auditors, Change and Patch Management Controls: Critical for Organizational Success 2nd Edition, USA, 2005

20 ISACA, COBIT 5, USA, 2013, p. 29 and 80, www.isaca.org/cobit

21 ISACA, COBIT 5 Implementation, USA, 2012, p. 72, www.isaca.org/cobit
Why Computer Ethics Matters to Computer Auditing

Unethical use of the computer\(^1\) is harmful to all—perpetrators and victims—and more than likely backfires on those who make use of computer facilities for unethical exploits. Failing to identify ethical issues surrounding the computer or neglecting these issues runs the risk of adverse consequences, and, especially in the case of computer auditing, it means a dangerously incomplete audit decision.

“Hardware, software and people are all sources of difficulties; people [the computer users] who appear to be cognizant of the risks involved [being] the most troublesome.”\(^2\) It is fair to say that people are the major source of risk and any decision to abuse or not to abuse depends entirely on a person’s sense of morality. Furthermore, “People need something to awaken their sense of responsibility because information regarding computing risks and safe practices does little to significantly change behavior.”\(^3\) Computer ethics is that “something,” and the connection between computers and ethics is obvious.

Computer auditing aims to discourage, detect and prevent information risk by enforcing compliance and governance rules and standards, whereas computer ethics attempts to minimize this risk by warning people of the potential adverse consequences of unethical actions. This integrated aim in risk aversion unites computer ethics and computers.

An audit decision without ethical consideration will lead to intangible, adverse consequences in the short and long term. Information systems (IS) auditors should regard the neglect of ethical issues associated with the use of information systems as a different type of risk that could be averted through a daily, routine check—a different kind of antirisk mechanism (compared with the other established antirisk routine countermeasures, e.g., password, cryptographic algorithms, antivirus software). IS auditors could also make use of the concept behind computer ethics to perform a dual function: a change agent function that can persuade rectifying behaviors/attitudes and an incubator function that can cultivate trusting relationships with the clients and maintaining a professional reputation in the industry.

CONNECTING THE COMPUTER AND ETHICS

Computer ethics has been given different labels including cyberethics, information ethics and, one of the more noticeable recent terms, sociotechnical computer ethics. The latter is attributed to the three recommendations in response to the three mistakes of science, technology and society.\(^4\) In this article, “computer ethics” is chosen for the reason that the core issues involved are rooted in the computer no matter how sophisticated and complicated the modern facilities, e.g., the Internet, social media.

Like ethics, computer ethics may mean different things to different people. In one often quoted definition, “Computer ethics is the analysis of the nature and social impact of information and communication technology, and the corresponding formulation and justification of policies for the ethical use of such technology.”\(^5\) In this article, it is taken to mean ethics in cyberspace.\(^6\) This simple definition implies that computer ethics is concerned with issues of ethical consequences arising out of using the computer and its peripherals, particularly the Internet, and that, while many of the threats are not possible without the computer, the computer becomes the culprit (or an instrument) and the victim (or a target).

The uniqueness of this relatively new field has been hotly debated and widely reported in

---

\(^{1}\)ISACA JOURNAL, VOLUME 2, 2014

---

Wanbil W. Lee, DBA, is principal director of Wanbil & Associates, president of The Computer Ethics Society and adjunct professor in computing at the Hong Kong Polytechnic University (Kowloon, Hong Kong). He has devoted more than five decades to serving the field of computing in the banking, government and academic sectors through various roles in Australasia and Hong Kong. His current teaching and research interests focus on ethical computing and information security. He is a member of several learned societies and sits on committees/boards of some of these bodies, editorial boards, and advisory committees of the Hong Kong government.

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

Go directly to the article:
The uniqueness camp argues that things such as software, web sites and online video games never existed before the arrival of the computer and these new things created new ethical dilemmas that are beyond the existing ethical rules or standards and justify the creation of a branch of applied ethics.

CONNECTING COMPUTER ETHICS AND COMPUTER AUDITING

Of the several implications that computer ethics has for computer auditing, computer ethics supplies the rules and regulations derived from the ethical principles and theories in an attempt to prevent/minimize abuse in cyberspace, while computer auditing primarily offers preventive and, to some extent, detective techniques, aimed at ensuring compliance with rules and regulation governance. This shows the common interest and different objective between computer ethics and computer auditing.

Moreover, failing to identify or excluding the ethical issues surrounding the computer (when performing risk assessment), despite sound cost and benefit justification, is a different type of risk (vis-a-vis the risk arising out of access control malfunction, identity theft and so on) as it will lead to potentially adverse consequences, such as loss of trust or collapse of business. For example, in assessing softlifting (illegal copying of software for personal use) or unauthorized access to sensitive information, the IS auditor should consider the damage due to personal use of sensitive information, not just concentrate on technical access control mechanisms. Considering the consequence in total may yield a different evaluation of the damage. This difference may be attributed to the exclusion of the cost for losing the confidence of the data owners (internal and external clients) and impairing the provider-client relationship, as well as payment for compensation and expenses for legal proceedings. Ethics should, therefore, be taken as an additional type of risk that IS auditors should check every day. Checking for potential ethical issues by performing an ethical analysis, for example, may reveal risk that may lead to ethical consequences, but may otherwise be missed in the traditional antirisk checks and audits. The fact that an ethical analysis adds a step or steps to the routine makes computer ethics a different kind of antirisk mechanism as alluded to earlier.

The variety, frequency and incidence of abuses are still increasing, despite the extant antirisk mechanisms, computer laws, and even computer auditing and information governance. This increase in abuse arguably can be attributed to several major reasons. The first is that computer-related risk is, as alluded to earlier, treated as a technical issue, missing out on its managerial, sociotechnical aspects. The second is that new tools will be rendered impotent by their inherent limitations, external factors, unexpected changes and the ever-lurking predators, no sooner than these new tools become available. The third is that the law is useful as a reference framework for remedy and can be a forceful deterrent to prevent abusive acts by virtue of its power to punish, but it is by nature too slow to combat the rapidly developing acts of wrongdoing because creating new laws is a complex and lengthy process and because people are, in general, reluctant to proceed with legal action or they opt for legal action only as a last resort. The last is that the audit-based mechanism is limited as a deterrent, the audit tools are empowered to detect deviation from a set policy of performance, and the audit tools check and verify that compliance is properly enforced and the results are consistent with the set standard, but in physical, cost-benefit terms only.

As revealed in an exploratory study, which ran an annual survey from 2006 to 2012, knowledge of ethics tends to yield an effect of reducing people’s inclination toward abusive behavior, thus a reduction in the new type of risk (or threats to abuse the development and use of information). The participants were part-time, final-year students for an undergraduate award in computing at The Hong Kong Polytechnic University, aged from early 20s to early 40s in regular full-time employment in the computer industry, with two to 15 years of experience ranging from technical to managerial positions. The survey was carried out at the beginning and at the end of a compulsory course that
included the topics of ethics and professionalism, using the same questionnaire. Three questions to which a yes/no indication was sought were set for the beginning of the course, and five for the end of the course. The annual number of participants over the entire period of the survey averaged 95 students. The responses to each question (summarized in figure 1) have been consistent over the seven consecutive years (p > .05) and indicate that less than 10 percent of students are aware of computer ethics. Further, more than 60 percent claimed that they were not sure if they carried out their work ethically and, conversely, about 30 percent claimed that they thought they carried out their work ethically.

Computer ethics aims to cultivate good behavior in cyberspace and image and reputation depend on proven fairness (in conducting business and personal affairs) or confidence (in us by others). There will be no fairness or confidence unless people consistently demonstrate honoring promises and stand by the consequences of their words and deeds by closely adhering to ethical principles, and so on.

It is a common interest and a set of different objectives that connects computer ethics and computer auditing. As a soft, humanistic methodology based on ethical principles, computer ethics aims to supplement computer auditing.11

ETHICAL ANALYSES AND DECISION
An ethical decision is simply a binary choice of right or wrong, or good or bad. It can, however, be complex because of the inevitable bias, prejudice and subjectivity of the decision make, as he/she is never free from interfering and competing factors, nor is any decision maker free of value judgment. To guide decision makers through the labyrinth of often conflicting ethical views, a unified model was contemplated and developed. Most notable are the menu-like checklists including the four-step approach,12 the Five-step Principled Reasoning,13 the Seven-step Path for Making Ethical Decisions14 and the Ethical Matrix.15

Briefly, the checklists cover more or less the same ground and guide users through the predetermined steps, with the major steps being:
• Analyze the situation.
• Make a defensible ethical decision.
• Describe steps to resolve the situation.
• Prepare policies and strategies to prevent recurrence.

The ethical matrix was originally designed for making ethical decisions in the field of food and agriculture and, since its release, has been adapted for other fields, for example, business16 and information engineering.17 The matrix is made up of three columns and as many rows as the particular case needs. A row is allocated to a stakeholder; the three columns correspond to three common ethical principles—well-being, autonomy and fairness—and the cells contain the concerns of the stakeholders (the main criterion that should be met with respect to a particular principle).

The following case illustrates the matrix method in action: A high-tech facilities distributor replaced its existing offline help-desk platform with an online monitoring facility, and the new system enables help-desk staff to see exactly what is on the users’ screens and respond to users’ requests for help quickly. The fast response time and elimination of the help-desk staff’s traveling time (to reach the users) has increased user satisfaction and operational efficiency. The executive vice president (EVP) is impressed, particularly with the surveillance function, and asked the chief information

<table>
<thead>
<tr>
<th>Figure 1—Questions and the Average Response Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Questions Before Attending the Course</strong></td>
</tr>
<tr>
<td>(Yes/No Response) Rate</td>
</tr>
<tr>
<td>i) I heard or was aware of computer ethics, but I did not know if I used my computer ethically.</td>
</tr>
<tr>
<td>ii) I never heard of, nor was I aware of, computer ethics and I was not sure if I used my computer ethically.</td>
</tr>
<tr>
<td>iii) I never heard of, nor was I aware of, computer ethics and I thought I used my computer ethically.</td>
</tr>
<tr>
<td><strong>Questions After Attending the Course</strong></td>
</tr>
<tr>
<td>(Yes/No Response) Rate</td>
</tr>
<tr>
<td>iv) I understand computer ethics and I will use my computer according to ethical principles.</td>
</tr>
<tr>
<td>v) I understand computer ethics and I will not use my computer according to ethical principles.</td>
</tr>
<tr>
<td>vi) I will not change my view because I do not fully understand the subject of computer ethics.</td>
</tr>
<tr>
<td>vii) I will not change my view because I do not subscribe to the subject of computer ethics.</td>
</tr>
<tr>
<td>viii) I am indifferent because I do not care much about computer ethics.</td>
</tr>
</tbody>
</table>

officer (CIO) to have a copy of the system installed in her office as she has been searching for a tool to deal with drug dealing allegedly occurring on company premises. The first-cut analysis identified four interest groups: The firm, staff, the EVP and the CIO, and reveals two major sets of concerns of each interest group with respect to the ethical principles (summarized in figure 2):

1. Watching (by the help-desk staff) over the users’ screens without the users knowing it has the potential to violate personal privacy in the workplace. This certainly alarms the staff (for fear of privacy invasion) and the firm (for concern over corporate image and personnel welfare).

2. Entertaining the EVP’s request implies using the surveillance function for spying on the staff and deviates from the original, approved purpose for acquiring the new system. This disturbs the CIO (with respect to professionalism and deontological issues), the EVP (on her duty to protect the corporate image from possible damage), the staff (about being exploited by one or a few rotten apples) and the firm (about staff morale and company policy).

CONCLUSION

Some unethical actions, whether unintentional or otherwise, can get one into trouble with the law, while other unethical actions, though legal, can ruin reputations, even careers. Furthermore, some unethical actions can be carried out faster with the computer while other unethical actions may have been difficult or infeasible without the computer, but are now possible. As the usage of computers proliferates, individuals and organizations are becoming increasingly vulnerable.

The more professionals, including IS auditors, appreciate ethical principles, the more they are capable of discerning the good from the bad. As a result, they will be able to improve their chances of arriving at a desirable and defendable case, for example, against allegations of being unprofessional. This will help them do the right thing in cyberspace, build up their professional reputation, win the trust of their clients.

Reflecting on the ethical analysis and decision-making models, the menu-like checklists provide a well-structured, user-friendly list to guide users through a series of structured steps in analyzing the dilemmas with respect to the explicitly specified theories/principles and, in the end, taking certain actions or answering certain questions. The ethical matrix, though designed for making ethical decisions in the field of food and agriculture, can be adopted for other fields with appropriate adjustment.

Risk is not only a tangible, but also a sociotechnical issue—not only a technical task, but also a managerial concern. Hence, cost-benefit analysis (which is based on bottom-line, economic reasoning) and risk analysis (which relies on probabilistic, computational arguments) are inadequate. IS auditors are alerted to a tripartite analysis model, a new decision analysis paradigm that comprises cost-benefit, risk and ethical analyses.

ENDNOTES

1 “Computer” is used in this article to encompass the computer-based information system and its associated hardware, software, networking, enabling facilities and people.
2 Neumann, P. G.; Computer Related Risk, ACM Press/Addison-Wesley, USA, 1995
6 The Computer Ethics Society, iEthics, www.iEthicsSoc.org
7 Op cit, Johnson
18. *Op cit*, Johnson
In November 2013, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) formally released the long-anticipated updates to ISO/IEC 27001 and 27002. The last time these standards were updated was in 2005.

The revised version of ISO/IEC 27001:2013 has set the stage for significant structural changes in the standard’s individual sections with the introduction of changes as well a number of new information security controls. Much of the text and requirements from the previous version of the standard is still there, but has been adapted to fit new and expanding topics.

**KEY CHANGES TO THE REVISED STANDARD**

The following are the key changes in the newly revised standard:

- **Changes introduced in risk assessment (clause 6.1.2)**—Assets, vulnerabilities and threats are not the basis of risk assessment anymore. The new requirements identify risk associated with confidentiality, integrity and availability (CIA) factors (organizational-context-based). Organizations will now have the option of deciding whether to outline the risk they face and how risk should be controlled without first needing to break down asset threats, vulnerabilities and impact by individual assets. While an asset-based approach is still permitted and can achieve more rigorous protection, organizations that may have been deterred by this workload can relax with the option provided by the revised standard. This will provide greater flexibility for organizations in choosing the way they want to assess their information security risk. It will also provide opportunities for identifying strategic risk related to information security apart from the technical risk found around IT assets.

- **Introduction of risk ownership (clauses 6.1.2 and 6.2)**—The concept of asset owner is replaced with a new term, “risk owners,” which makes management at a higher level responsible and accountable for various identified risk. By focusing on the risk-owners approach, organizations will no longer be bound by the old asset ownership, allowing them the flexibility to choose and implement any risk management method that better suits the organization. Also, this will help better align information security risk management activities with the enterprise risk management activities of an organization.

- **More importance given to interested parties (clause 4.2)**—The importance of interested parties, which can include shareholders, authorities (including legal and regulatory requirements), clients and partners, is recognized in ISO/IEC 27001:2013. In the revised standard, a separate clause has been added that specifies that all interested parties must be listed together with all their requirements. This is helpful in getting key inputs into the information security management system (ISMS) from various interested parties who will have a stake in an organization’s ISMS implementation.

- **Addressing strategic risk**—ISO/IEC 27001:2013 also includes upside risk (strategic risk) instead of focusing only on downside risk (technical risk). As part of the risk management process, organizations are now required to

---

**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.

---

**Enjoying this article?**

- **Read COBIT 5 for Risk.**
  
  [www.isaca.org/cobit](http://www.isaca.org/cobit)

- **Learn more about, discuss and collaborate on information security management and risk management in the Knowledge Center.**
  
  [www.isaca.org/knowledgecenter](http://www.isaca.org/knowledgecenter)
identify opportunities and make sure these are realized. These are improved opportunities of the ISMS that will support the business, which will enable business to do things in a better way than previously.

- **Changes in the number of control sections and controls**—This change has resulted in the removal of some controls, the addition of other controls, the requirement of some new documents and the omission of some unnecessary documents. The number of controls has decreased from 133 to 114, while the number of sections has increased from 11 to 14 (figure 1 and figure 2). The structure of some of the sections has been changed to allow for better arrangement of controls for implementation.

- **Improved communication on information security (clause 7.4)**—In the previous version of the standard, not much emphasis was given to communication of information security implementation in an organization. There is a new clause added in the revised standard where all the communication requirements (e.g., what needs to be communicated, when, by whom, through which means) are summarized. This is meant to help overcome the problem of information security being viewed as only an “IT thing” or a “security thing.”

- **Improved management oversight through monitoring of controls (clause 5.1)**—ISO/IEC 27001:2005 broadly talked about monitoring the ISMS implementation and the effectiveness of information security controls through management oversight. The revised standard takes a much more focused approach and calls out the importance of having a documented plan or rationale for monitoring specific processes and controls through exclusive clauses introduced with very concrete rules. These rules explain how to set clear objectives, who will measure them and when, and who should analyze and evaluate those results. This is intended to bring ISMS closer to other management processes in an organization.

**VALUE ADDITION ALIGNED WITH OTHER MANAGEMENT SYSTEM STANDARDS**
The revised standard is aligned with most of the management system standards practiced in the industry globally (figure 3). It is also important to note that the revised standard has a strong focus on aligning information security management with enterprise risk management (ERM) practices.

**BUSINESS CASE FOR ISO/IEC 27001:2013 IMPLEMENTATION**
The updated standard can be implemented for the following purposes:

- **Fighting cybercrime**—Introducing the ISO/IEC 27001 ISMS will help protect businesses from the threat of organized crime.
• **Recovering from accidents**—Organizations can minimize the risk that information will be lost or corrupted as a result of human error.

• **Improving corporate governance**—Reducing the organization’s financial exposure to the risk of losses resulting from IT system failure is now a corporate governance requirement. ISO/IEC 27001 can help companies comply.

• **Aligning with ERM**—The newer version aligns information security risk management (ISRM) with ERM activities.

---

**CONCLUSION**

The improved management oversight and flexible context-based risk assessment practices of ISO/IEC 27001:2013 will help organizations in aligning ISRM practices completely with the ERM practices of organizations. It is advisable that organizations plan to implement, as well as transition into, the newer version of ISO/IEC 27001:2013 from the current version (ISO/IEC 27001:2005).

**ENDNOTE**

ACROSS

1. Term used in data security, meaning “considered vital to operations”
5. Auxiliary memory
10. Word at the start of a business letter
12. Did not put as much time and money into a project as its importance warranted
13. Where backups of data should be stored
15. Large scale
16. Restoring data after a disaster
20. Acquire, as in a contract
21. Be indebted to
22. Some companies approach security on the basis of the ____ minimum
27. Exchange regularly
28. Piece of advice
30. City transport
31. Have a consensus on
32. Judge who ruled NSA’s bulk collection of metadata was unconstitutional
35. Retailer that recently suffered a huge data breach
36. Classification given to data of lesser importance (i.e., nonvital) (2 words)
38. Term for information needed to access a system
39. System, for short
40. Surfaces
41. Operative

DOWN

1. Valuable certificate for those dealing with IT and risk management
2. Mirror
3. Not capable of being affected by some event or circumstance
4. Supplies assistance to
6. Simple storages devices
7. His work led to The Uncertainty Principle
8. Erode, with into
9. Programmer’s creation
11. Depend (on)
14. Diagram showing sequences of movements of people and materials (2 words)
17. Roman 7
18. Assumes as an axiom
19. What a hacker might do (3 words)
23. Right, for short
24. Time for completion of a project
25. Identifying and removing errors from
26. Situation requiring immediate attention and action
29. Kaizen is a philosophy that strives to always improve this
34. Concepts of self-importance that can get in the way of logical decision making
35. Six on a big clock
37. Connect
38. Word before Amigos and Angeles

(Answers on page 58)
QUOTATION # 153

Based on Volume 6, 2013—Security and Compliance
Value—1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

CANO ARTICLE

1. The CCO develops a proactive and preventive monitoring function that detects inadequate execution of practices, reports them, and performs a follow-up on the assessed areas in order to overcome the identified condition.

2. Once the function of information security is understood as a natural enforcement of corporate compliance, it becomes necessary to walk along the information security path to establish the potentiality of noncompliance risk.

RAMOS ARTICLE

3. As security professionals have been applying best practices and asking for security audits and certifications, mechanisms have been able to transmit the level of trust required by customers of cloud computing services.

4. A provider that implements a certified information security management system (ISMS) follows best practices and adopts security measures following a risk management process, but the customer cannot derive the robustness of security measures that the provider has in place only from the certification.

5. Rating (for services, not for providers) gives a relative value that can be understood as a forecast about technical solvency of the vendor in relation to its security and resiliency. In this way, services with a better rating would have a lower probability of suffering an incident that affects service level agreements in a significant way.

AZAM ARTICLE

6. Risk assessments performed by assurance professionals are not specific to their respective domain and give a holistic risk profile of the organization, which results in the presence of well-mitigated and detected threats.

7. Management often misinterprets observations that are common across different reviews and audit reports because of the difference in severity level and recommendation. As a result, these observations are inappropriately treated and reappear.

8. The mapping of international standards and best practices to identify controls enables the assurance functions to develop a control baseline that could be implemented across the organization.

9. The cost of carrying out continuous risk can be lowered if self-assessment is performed against the control baseline for different assurance functions.

10. If similar or repetitive controls from various assurance functions are grouped together, their resolution by the auditee becomes simpler since he/she will have fewer observations and target dates to meet.

GUO ARTICLE

11. By playing a supporting role, top executives turn security management into a business problem rather than an IT problem.

12. From a value-focused thinking perspective, information security professionals are required to examine the values of end users, the fundamental objectives for information security and business performance, and the means to achieve them.

13. Information security professionals need to have technical skills as well as business skills and orientation to foster the follower-advisor relationship with top executives.

AHMED ARTICLE

14. Gartner predicted that in 2013, 60 percent of businesses will support smart devices for their employees.

15. Even with BYOD, a strong security policy would be to deny all except for approved devices, applications and users.

16. To reduce theft or misuse, the organization should conduct risk training for end users that emphasizes information asset ownership and logical security awareness.

17. As part of a strong BYOD strategy, having well-designed policies to accommodate the future trend is key to combating new sets of security challenges and opportunities for business as well as the IT department.
ISACA Journal
CPE Quiz
Based on Volume 6—Security and Compliance
Quiz #153 Answer Form

(Please print or type)
Name ________________________________________________
__________________________________________________
Address _____________________________________________
__________________________________________________
__________________________________________________
CISA, CISM, CGEIT or CRISC # __________________________

Quiz #153

True or False

CANO ARTICLE
1. __________
2. __________
3. __________
4. __________
5. __________

RAMOS ARTICLE
6. __________
7. __________
8. __________
9. __________
10. __________

GUO ARTICLE
11. __________
12. __________
13. __________

AHMED ARTICLE
14. __________
15. __________
16. __________

AZAM ARTICLE
17. __________

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

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

Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address. You will be responsible for submitting your credit hours at year-end for CPE credits.

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

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

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

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

ITAF™, 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**

The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorisation as the standards (also divided into three categories):
- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

**IS Audit and Assurance Tools and Techniques**

- These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance program 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 be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IS environment.

### IS Audit and Assurance Standards

The titles of issued standards documents are listed as follows:

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

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

**Reporting**
- 1401 Reporting
- 1402 Follow-up Activities

**IS Audit and Assurance Guidelines**

Please note that the 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.

**General**
- 2001 Audit Charter (G5)
- 2002 Organisational Independence (G12)
- 2003 Professional Independence (G17 and G34)
- 2004 Reasonable Expectation
- 2005 Due Professional Care (G7)
- 2006 Proficiency (G30)
- 2007 Assertions
- 2008 Criteria

**Performance**
- 2201 Engagement Planning (G15)
- 2202 Risk Assessment in Planning (G13)
- 2203 Performance and Supervision (G8)
- 2204 Materiality (G6)
- 2205 Evidence (G2)
- 2206 Using the Work of Other Experts (G1)
- 2207 Irregularity and Illegal Acts (G9)
- 2208 Sampling (G10)

**Reporting**
- 2401 Reporting (G20)
- 2402 Follow-up Activities (G35)

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 60008-5105, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at www.isaca.org/standards.
**ISACA Journal**, formerly Information Systems Control Journal, is published by ISACA, a nonprofit organization created for the public in 1969. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors, employers or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

© 2014 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC) (www.copyright.com), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1944-1967), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

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

**ISSN 1944-1967**

---

### Advertisers/Web Sites

<table>
<thead>
<tr>
<th>Advertiser</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capella University</td>
<td><a href="http://www.capella.edu/ISACA">www.capella.edu/ISACA</a></td>
<td>3</td>
</tr>
<tr>
<td>Client and Friends</td>
<td><a href="http://www.adaptivegrc.com">www.adaptivegrc.com</a></td>
<td>Back Cover</td>
</tr>
<tr>
<td>Regis University</td>
<td><a href="http://www.informationassurance.regis.edu/ISACA">www.informationassurance.regis.edu/ISACA</a></td>
<td>10</td>
</tr>
<tr>
<td>TeamMate</td>
<td><a href="http://www.TeamMateassurance.com/CM">www.TeamMateassurance.com/CM</a></td>
<td>1</td>
</tr>
</tbody>
</table>

---

### Leaders and Supporters

**Editor**  
Deborah Oetjen

**Senior Editorial Manager**  
Jennifer Hajigeorgiou  
[publication@isaca.org](mailto:publication@isaca.org)

**Contributing Editors**  
Sally Chan, CEGT, CMA, ACIS  
Kamal Khan, CISA, CISSP, CIP, IBMS  
Vasant Raval, DBA, CISA  
Steven J. Ross, CISA, CBIP, CISSP  
Tommie Singleton, Ph.D., CISA, CEGT, CPA  
B. Ganapatl Subramaniam, CISA, CIA, CISSP, SP, CIE, CISA, CISM, CEGT, CRISC, ISMS, LA  
Smita Totade, Ph.D., CISA, CISM, CEGT, CRISC

**Advertising**  
[media@isaca.org](mailto:media@isaca.org)

**Media Relations**  
[news@isaca.org](mailto:news@isaca.org)

**Editorial Reviewers**  
- Matt Allman, CISA, CISM, CEGT, CRISC  
- Geetantra Bachhri, BCIP, BCP, HPCP  
- Brian Bannier, CEGT, CRISC  
- Linda Betz, CISA  
- Pascal A. Bizaro, CISA  
- Jerome Caprirossi, CISA  
- Cassandra Chasnys, CISA  
- Ashwin K. Chaudhary, CISA, CISM, CEGT, CRISC  
- Reynaldo J. de la Fuente, CISA, CISM, CEGT  
- Christos Dimitriadis, Ph.D., CISA, CISM  
- Ken Doughty, CISA, CRISC, CBP  
- Nikesh L. Dubey, CISA, CISM, CRISC, CSPP  
- Ross Dworman, CISM, GSLC  
- Robert Findlay  
- Jack Freund, CISA, CISM, CRISC, CIPP, CSPP, PMP  
- Sailsh Gadia, CISA  
- Anq Goel, Ph.D., CISA, CEGT, CRISC, CSPP  
- Manish Gupta, CISA, CISM, CRISC, CSPP  
- Jeffrey Hare, CISA, CPA, CIA  
- Jocelyn Howard, CISA, CISSP, CSPP  
- Francisco Igual, CISA, CEGT, CSPP  
- Jennifer Inserso, CISA, CSPP  
- Timothy James, CISA, CRISC  
- Khawaja Faisal Javed, CISA, CRISC, CBP, ISMS, LA  
- Keni Lemme-Moretti, CRISC  
- Romulo Lompante, CISA, CEGT, CRISC  
- Juan Macias, CISA, CRISC  
- Larry Marks, CISA, CEGT, CRISC  
- Norman Marks  
- David Earl Mills, CISA, CEGT, CRISC, MCSE  
- Robert Moeller, CISA, CSPP, CPA, CSQE  
- Auneo Monteiro Tavares Da Silva, CISM, CEGT  
- Ramu Mutthiah, CISM, ITL, PMP  
- Gretchen Myers, CSPP  
- Mathew Nicho, CSH, RWSP, SAP  
- Daniel Paula, CISA, CRISC, CSPP, PMP  
- Pak-Lok Poon, Ph.D., CISA, CSQA, MIEE  
- John Pouey, CISA, CISM, CRISC, CIA  
- Steve Primost, CISM  
- Hari Ramachandra, CEGT, TOGA  
- Panvathi Ramesh, CISA, CA  
- David Ramirez, CISA, CISM  
- Antonio Ramos Garcia, CISA, CISM, CRISC, CDPP, ITL  
- Ron Roy, CISA, CRP  
- Louisa Saunier, CISSP, PMP, Six Sigma  
- Green Belt

**ISACA Board of Directors**  
(2013–2014)  
- **International President**  
  Tony Hayes, CEGT, AFCHSE, CHE, FACS, FCPA, FIA  
- **Vice President**  
  Allan Boardman, CISA, CISM, CEGT, CRISC, ACA, CA (SA), CSPP  
- **Vice President**  
  Juan Luis Canselle, CISA, CEGT, CRISC  
- **Vice President**  
  Ramzes Gallego, CISM, CEGT, CCSS, CSPP, SCPM, Six Sigma Black Belt  
- **Vice President**  
  Theresa Grafenstine, CISA, CEGT, CRISC, CGAP, CGMA, CIA, CPA  
- **Vice President**  
  Vittal Raj, CISA, CISM, CEGT, CFE, CIA, CSPP, FIA  
- **Vice President**  
  Jeff Spivey, CRISC, CPP  
- **Vice President**  
  Marc Vael, CISA, CISM, CEGT, CSPP, ITIL  
- **Past International President, 2012-2013**  
  Greg Grocholski, CISA  
- **Past International President, 2011-2012**  
  Kenneth L. Vander Wal, CISA, CPA  
- **Director**  
  Christos Dimitriadis, Ph.D., CISA, CISM, CRISC  
- **Director**  
  Krysten McCabe, CISA  
- **Director**  
  Jo Stewart-Rattray, CISA, CISM, CEGT, CRISC  
- **Acting Chief Executive Officer**  
  Ron Hale, CISM
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**

**COBIT® 5 for Risk** *
213 pages—CB5RK

- **Member** $35.00  
  - **NonMember** $175.00

**Big Data Governance**
368 pages—IMCBD

- **Member** $41.00  
  - **NonMember** $51.00

**COBIT 5 for Risk** *
213 pages—CB5RK

- **Member** $35.00  
  - **NonMember** $175.00

**eBook—WC5BK**

- **Member** $35.00  
  - **NonMember** $175.00

**Advanced Persistent Threats: How to Manage the Risk to Your Business** *
132 pages—APT

- **Member** $35.00  
  - **NonMember** $60.00

**eBook—WAPT**

- **Member** FREE  
  - **NonMember** $60.00

**Crime On-Line: Correlates, Causes, and Context: Second Edition**
268 pages—2CAP

- **Member** $35.00  
  - **NonMember** $45.00

**There’s a New Sheriff In Town**
111 pages—2EA

- **Member** $20.00  
  - **NonMember** $30.00

**Hiles on Business Continuity: Global Best Practices, 3rd Edition**
252 pages—7RO

- **Member** $99.00  
  - **NonMember** $109.00

**Responding to Targeted Cyberattacks** *
90 pages—RTC

- **Member** $35.00  
  - **NonMember** $59.00

**eBook Format—WRTC**

- **Member** Free  
  - **NonMember** $59.00

**Information Security Management Handbook**
CD-ROM 2012—56CRC

- **Member** $200.00  
  - **NonMember** $210.00

**Mobile Hacking Exposed: Security Secrets & Solutions**
320 pages—35MHEM

- **Member** $40.00  
  - **NonMember** $50.00

**ITIL Foundation Essentials: The Exam Facts You Need**
148 pages—19TIF

- **Member** $15.00  
  - **NonMember** $25.00

**Controles Estrategicos y Operacionales de la Ti (Spanish Edition)**
711 pages—20ITCE (Spanish Language Version)
6ITSOC (English Language Version)

- **Member** $60.00  
  - **NonMember** $70.00

**Engineering Safe and Secure Software Systems**
304 pages—11ART

- **Member** $109.00  
  - **NonMember** $119.00

* 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](https://www.isaca.org/bookstore/Pages/New-Arrivals.aspx)
Big Data Governance: An Emerging Imperative
by Sunil Soares

Written by a leading expert in the field, this guide focuses on the convergence of two major trends in information management—big data and information governance—by taking a strategic approach oriented around business cases and industry imperatives. With the advent of new technologies, enterprises are expanding and handling very large volumes of data; this book, nontechnical in nature and geared toward business audiences, encourages the practice of establishing appropriate governance over big data initiatives and addresses how to manage and govern big data, highlighting the relevant processes, procedures, and policies. It teaches readers to understand how big data fits within an overall information governance program; quantify the business value of big data; apply information governance concepts such as stewardship, metadata, and organization structures to big data; appreciate the wide-ranging business benefits for various industries and job functions; sell the value of big data governance to businesses; and establish step-by-step processes to implement big data governance. 2013, 368 pages

Print Format—1MCBD
Member $41.00  Nonmember $51.00

Advanced Persistent Threats: How to Manage the Risk to Your Business *
by ISACA

This book explains the nature of the security phenomenon known as the advanced persistent threat (APT). It also provides helpful advice on how to assess the risk of an APT to the organization and recommends practical measures that can be taken to prevent, detect and respond to such an attack. In addition, it highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk. 132 pages, 2013

Print Format—APT
Member $35.00  Nonmember $60.00

eBook—WAPT
Member FREE  Nonmember $60.00

There’s a New Sheriff In Town
by Mary Lou Heastings

Today’s information security leaders are faced with unprecedented challenges: complexities of the broadening scope of regulations, the accelerated pace of new technologies introduced to the market, and rising levels of risks to their organizations. These are only a few of the challenges that are placing increased pressure on leaders to consistently deliver 24x7 on their promise to protect their organization and its customers. Where the lawmen of the mid-1800’s, with badges pinned to their vests, were symbols of protection, so today are the executives that contributed to this book. 2010, 111 pages

Print Format—2EA
Member $20.00  Nonmember $30.00

Edited by Harold F. Tipton, CISSP and Miki Krause Natale, CISSP

Information Security Management Handbook is the most comprehensive and up-to-date reference available on information security and risk management. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations.

Reporting on the latest developments in information security, this volume features 31 new entries on Social Networking, Secure Software Lifecycle, Insider Threat, Application Whitelisting, Server Virtualization, Security Requirements Analysis, CERT Resilience Management Model, Continuous Monitoring, Service-Oriented Architecture, Cloud Security, Managing Advanced Persistent Threats, Virtualization Forensics, Protected Health Information under HIPAA and HITECH, and more. This edition updates its popular predecessors with the information you need to address the vulnerabilities created by recent innovations such as cloud computing, mobile banking, digital wallets, and near-field communications.

This 2012 CD-ROM Edition contains the complete contents of every annual edition of the handbook since 1997, including 2012. It is an authoritative resource that is linked, searchable by keyword, and organized under the CISSP® CBK® domains. In addition to the complete contents of the set, the CD-ROM includes an extra volume’s worth of information—including chapters from other security and networking books that have never appeared in the print edition of the Information Security Management Handbook. 2012

CD-ROM—56CRC
Member $200.00  Nonmember $210.00

* 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
by Thomas J. Holt

The ubiquity of computers and the Internet have drastically changed the landscape of crime and deviance. Computer technology enables offenders to anonymously target victims around the world, connect with others who share their interests, and participate in various crimes. The Internet and cellular telephony are increasingly incorporated into real world offenses like prostitution in order to connect sex workers and clients with minimal risk of detection. At the same time, new forms of offending have emerged as a direct consequence of technology, such as computer hacking, which can be used for both beneficial and illegal purposes. The Internet has also become an important environment for extremists and terror groups to communicate their beliefs globally in order to recruit others and generate funds. 2013, 268 pages

Print Format—2CAP
Member $35.00  |  Nonmember $45.00

COBIT 5 for Risk*
by ISACA

Effectively managing IT risk helps drive better business performance by linking information and technology risk to the achievement of strategic enterprise objectives. Risk is generally defined as the combination of the probability of an event and its consequence. COBIT 5 for Risk defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. 213 pages, 2013

Print Format—CB5RK
Member $35.00  |  Nonmember $175.00

eBook—WCB5RK
Member $35.00  |  Nonmember $175.00

Mobile Hacking Exposed: Security Secrets & Solutions
by Neil Bergman, Mike Stanfield, Jason House, Joel Scambray, Sarah Geethakumar, Swagat Deshmukh, Scott Matsumoto, John Steven, Mike Price

Identify and evade key threats across the expanding mobile risk landscape. Hacking Exposed Mobile: Security Secrets & Solutions covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems. 2013, 320 pages

Print Format—35MHEM
Member $40.00  |  Nonmember $50.00

ITIL® Foundation Essentials: The Exam Facts You Need
by Claire Agutter

ITIL® Foundation Essentials is a distillation of critical information - no waffle or padding - just exactly what you need to understand the key points required for a successful exam. Aimed at self-study candidates, ITIL community training delegates, ISMF/BCS members and V2 Foundation Certificate holders, who have yet to take an upgraded exam, this pocket guide is fully aligned with the ITIL 2011 core volumes. Project managers, who are looking to expand their qualifications, and IT contractors or consultants, who don’t want to take time out from their day jobs to attend a course, will also find this pocket guide an essential companion to their studies and education. THE essential companion for those studying the ITIL Foundation syllabus, the pocket guide covers key areas including: A basic introduction to ITIL and a description of service classifications (core, enabling, enhancing) and an outline of internal and external services. A point-by-point summary of the purpose, objectives, scope and value of the five stages of the service lifecycle that form the ITIL core; from strategy and design, through to transition, operation and continual service improvement (CSI). Separate sections in the guide are dedicated to describing key concepts and terminology (including “stakeholders” and “processes, functions and roles”); and throughout the pocket guide the wide range of 3, 4 and 5 letter ITIL acronyms (including PBA, FMITS, BRM, SLM, OLA, SLR, V8F, ITSOM, SACM, RADM) are expanded and explained. A brief summary of the ITIL qualification scheme and the Foundation exam. Preparation for the ITIL Foundation Certificate in IT Service Management - Use it to get the results you need! 2012, 148 pages

Print Format—19ITIF
Member $15.00  |  Nonmember $25.00

* 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
Responding to Targeted Cyberattacks *

By ISACA

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

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

This publication covers a few of the basic concepts that will help answer the key questions posed by a new outlook that a breach WILL eventually occur. Responding to Targeted Cyberattacks is available for purchase in ebook and as print format. ISACA members have complimentary download access to the ebook. Nonmembers of ISACA may choose to purchase the ebook. 90 pages, 2013

Print Format—RTC         Member $35.00  Nonmember $59.00
Ebook—WRTC               Member FREE   Nonmember $59.00


by Andrew Hiles, FBCI

For 35 years, Andrew Hiles has traveled to 60+ countries, consulting to major private and government organizations, training the next generation of Business Continuity practitioners. With this new third edition of his classic text on global best practices, you’re inviting one of the world’s most highly regarded practitioners to “learn teach” with you. Hiles has updated and enhanced his widely used best practices book, first published in 1999, to provide step-by-step guidance in building and maintaining a world-class BC management system and plan. He includes details on plan content, structure and format for businesses with a single location; headquarters and regional offices; manufacturing and retail operations. His instructions incorporate the 10 disciplines of the Disaster Recovery Institute International (DRII) and the 6-phase BCM Lifecycle Model of the Business Continuity Institute (BCI).

2012, 252 pages

Print Format—7RO       Member $99.00  Nonmember $109.00

Engineering Safe and Secure Software Systems

by Warren Axelrod

This first-of-its-kind resource offers a broad and detailed understanding of software systems engineering from both security and safety perspectives. Addressing the overarching issues related to safeguarding public data and intellectual property, the book defines such terms as systems engineering, software engineering, security, and safety as precisely as possible, making clear the many distinctions, commonalities, and interdependencies among various disciplines. You explore the various approaches to risk and the generation and analysis of appropriate metrics.

This unique book explains how processes relevant to the creation and operation of software systems should be determined and improved, how projects should be managed, and how products can be assured. You learn the importance of integrating safety and security into the development life cycle. Additionally, this practical volume helps identify what motivators and deterrents can be put in place in order to implement the methods that have been recommended. 2012, 304 pages

Print Format—11ART     Member $109.00  Nonmember $119.00

Controles Estrategicos y Operacionales de la Ti (Spanish Edition)

by John Kyriazoglou

Tome el control de sus sistemas informaticos y obtenga las recompensas que le ofrece el negocio. Todos estamos familiarizados con los beneficios que la informatica proporciona a los negocios. Sin embargo, los sistemas informaticos desestructurados o mal controlados pueden sembrar el caos, ocasionar resultados inesperados e incluso amenazar su negocio a través de crímenes informaticos y de violaciones de seguridad. Para llevar estos riesgos al minimo, cualquier sistema informatico necesita una serie de controles que aseguran el máximo beneficio de la tecnología al mismo tiempo que una reducción de las amenazas potencial para la empresa. Desarrolle controles para sacar el máximo partido a su sistema mientras reduce las amenazas.

Controles estratégicos y operacionales de la TI es una guía exhaustiva para poner en marcha una serie de controles informaticos integrados, de manera metodica. Esto ayuda a las compañias a desarrollar los controles oportunos donde sea necesario y les permite reducir riesgos operacionales mientras respaldan los objetivos estratégicos de la empresa. Entender e implementar los conceptos y los problemas de los controles informaticos.

2013, 711 pages. (Also available in English—IT Strategic and Operational Controls, 2010, 686 pages)

Print Format—20ITCE (Spanish Language Version)     Member $60.00  Nonmember $70.00
Print Format—6ITSOC (English Language Version)     Member $60.00  Nonmember $70.00

* 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
Over 325 international exhibitors under one roof
Collect CPD and CPE credits by attending Europe’s biggest free information security education programme

Europe’s biggest Information Security Event
29 April to 01 May 2014
Earl’s Court, London UK

- Over 325 international exhibitors under one roof
- Collect CPD and CPE credits by attending Europe’s biggest free information security education programme

Register free now at: infosec.co.uk

Contact our team: (0)20 8271 2130
Looking for an integrated GRC solution?

AdaptiveGRC - one system, one database, be one

Get all of the functionality for just $9,995 / €7,500 / £6,500*

* The AdaptiveGRC starter pack:
  - Vendor Compliance Management
  - Compliance Assessments (internal and external)
  - Checklist Management
  - Enterprise Risk Management
  & state of compliance reporting

Sign your license before the end of April 2014 and get a hosted 2 user system up and running in up to 3 working days!

Looking for a unique GRC solution for your customers? Contact us and become the AdaptiveGRC consultancy channel in your region

www.adaptivegrc.com
info@adaptivegrc.com
US: +1 678 591 6965
UK: +44 207 022 4884
PL: +48 22 323 73 60

AdaptiveGRC is a Trade Mark of Customer Friendly Sp. z o.o. S.K.A.