Security and Compliance

Featured articles:
Information Security—Motivator of Corporate Compliance Practice
Security Labeling of IT Services Using a Rating Methodology
An Integrated Risk Assessment Program—A Cliché or a Need?
And more...
Reach out and help friends, colleagues and other professionals become ISACA® members. They get the benefits of ISACA Membership. You Get Rewarded.

When ISACA grows, members benefit. More recruits mean more connections, more opportunities to network—and now, better rewards!

Get recruiting today. It’s easy.
Learn more at isaca.org/www.isaca.org/getmembers-Jv6

Member Get a Member 2013
Get Members.
Get Rewarded.

The More Members You Recruit, the Better the Rewards

• Win a mini tablet device from the world’s leading manufacturer—get one entry into a monthly prize drawing for every new member you recruit*
• Get a hand-held digital entertainment device for recruiting 5-9 new members*
• Get a full-size tablet device for recruiting 10+ new members*

*Rules and restrictions apply and can be found at www.isaca.org/getamember-rules. Please be sure to read and understand these rules. If your friends or colleagues do not reference your ISACA member ID at the time they become ISACA members, you will not receive credit for recruiting them. Please remember to have them enter your ISACA member ID on the application form at the time they sign up. Apple® is not a participant in or sponsor of this promotion. © 2013 ISACA. All Rights Reserved.
TeamMate, the proven leader in Audit Management, has recently released TeamMate CM, a breakthrough in Compliance Management Software. Finally, the tool you have been waiting for to address SOX, A-123, and other financial reporting and IT compliance standards, brought to you by a Proven Leader.

Learn More at: TeamMateSolutions.com/CM
Columns

4
Information Security Matters: A Tide in the Affairs
Steven J. Ross, CISA, CISSP, MBCP

6
Information Ethics: Character Traits of an IT Professional
Vasant Raval, DBA, CISA, ACMA

10
Five Questions With... Robby B. Sebopeng, CISA

12
IT Audit Basics: What Every IT Auditor Should Know About Data Analytics
Tommie Singleton, CISA, CGEIT, CPA

Features

15
Reviewed by Upesh Parekh, CISA

16
Information Insecurity—Motivator of Corporate Compliance Practice
Jelmy J. Cano M., Ph.D., CFC, CFE, CMAS
(También disponible en español)

20
Security Labeling of IT Services Using a Rating Methodology
Antonio Ramos, CISA, CISM, CRISC, CCSK

24
An Integrated Risk Assessment Program—a Cliché or a Need?
Syed Fahd Azam, CISA

27
Leading Information Security
Klaus Julisch
(日本語版も入手可能)

31
Doing Business in India Requires Digital Compliance
Anil Vaidya, DBA, CISA, CISM

37
Revisiting the Human Factor in Organizational Information Security Management
Ken H. Guo, CMA

42
A Sustainable and Efficient Way to Meet Client’s Growing Security Expectations
Buck Kulkarni, CISA, CGEIT, PgMP

46
The Criticality of Mobile Device Management
Adesanya Ahmed, CRISC, CEGIT, ACMA, ACPA

Plus

52
Crossword Puzzle
Myles Mellor

53
Quiz #151
Based on Volume 4, 2013
Prepared by Kamal Khan, CISA, CISSP, CITT, MBGC

55
Standards, Guidelines, Tools and Techniques
S1-S8
ISACA Bookstore Supplement

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.

Journal Online

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

Online Features
The following articles will be available to ISACA members online on 2 December 2013.

Buffer Overflows—Seven Points IS Auditors Must Know
Markus Pfister, CISA

Defensive Strategic Posture in the Field of Information Security
David Eduardo Acosta R., CISA, CISM, CRISC, BS 25999 LA, CONA Security, CHFI Trainer, CISSP, PCI QSA, OPST
(También disponible en español)

The Value in Using IT-directed Investor Relationship Management
Frank Bezina, Ph.D., Pascal Lélé, Ph.D., Ronald Zhao, Ph.D., Simon Grima, Ph.D., Robert W. Klein, Ph.D., and Martin Hellmich, Ph.D.

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

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

Join ISACA LinkedIn: ISACA (Official), http://linkedin.isacaofficial

Like ISACA on Facebook: www.facebook.com/ISACAHQ
"Intellectuals solve problems, geniuses prevent them."

Albert Einstein

Applying intelligence to your identity and access equation.

Genius.

call 866.Courion
www.courion.com
I recently encountered two interesting, if
dismaying, articles concerning security protection,
which, until that time, I had considered to be
the keystone of information security.1 The first,
titled “BREACH Compression Attack Steals
HTTPS Secrets in Under 30 Seconds,” states that
researchers Angelo Prado, Neal Harris and Yoel
Gluck were able “to demonstrate a method to
read encrypted messages over the web by injecting
plaintext into an HTTPS request and measuring
compression changes.”2

The second, “Black Hat 2013: Experts Urge
Elliptical Curve Cryptography Adoption,” is even
scarier. It says “Crypto experts speaking at the
Black Hat USA 2013 conference…said there’s
a real—though perhaps not overwhelming—
possibility that much of the Internet’s encryption
will soon become completely unraveled. This
grand unveiling of secrets, they contended, could
arrive within a handful of years.”3 This means
that the public key encryption algorithm first
described by Ronald Rivest, Adi Shamir and
Leonard Adelman in 1977, and known today as
RSA for their initials, may be nearing the end
of its useful life. The same may be said of the
widely used key exchange protocol developed by
Whitfield Diffie and Martin Hellman in 1976.

Until this time, I have advocated that if
an organization is truly intent on securing its
information resources, or at least its most critical
ones, it should encrypt them. This remains true,
but the tools and techniques that have been
employed so successfully for so long may now
require a significant and costly upgrade. It is
important to emphasize that this is a pending
problem not an imminent threat. Now, before
the tide crests, it is timely to consider what the
business impact may be, leaving the impacts on
cryptology to the mathematicians who actually
understand them.

BUSINESS IMPACTS

To a certain extent, very little will change for
many organizations. Most information that is
transmitted or stored in encrypted form can
continue to use existing techniques for some
time to come. The messages and files will still
be unreadable to all except the most determined
attackers. After all, is anyone really likely to use
decryption tools such as Browser Reconnaissance
and Exfiltration via Adaptive Compression of
Hypertext (BREACH)?5 This would require a
major investment in attack capabilities and intent
to penetrate the secrets of targeted organizations.

Oh, but wait…

From what we read in the newspapers,
governments (to say nothing of terrorists and
criminals) around the world are engaged in
preparations for cyberwarfare.6 It might be
easier to consider the governments that are
not doing so; I believe that we can reasonably
exclude Andorra from the list of those doing it.
Unfortunately, there is every reason to believe
that governments are, in fact, attempting to
steal military, governmental and corporate
information.7 Thus, there is a real possibility that
encrypted information may be at risk.

Another concern is the communication
and storage of information in the cloud. It has
long been recognized that “a robust encryption
scheme, supported by an equally robust public
key infrastructure (PKI), is necessary to achieve
confidentiality and integrity for [cloud]-based services.8 In other words, cloud technology, especially for a public cloud in which information from many organizations may be adjoined, if not intermingled, requires encryption in order to provide security not only from outside, but also from within that particular cloud.

If the most widely used encryption algorithm is breakable, or soon will be, organizations must consider the risk of placing sensitive information in the cloud. The nature of that analysis will be governed by the magnitude of the threat of data being stolen, sizable but unknowable, as stated previously. Similarly, the value of the information must be figured into the risk equation. If the information is sensitive, the threat realistic and the available safeguards inadequate, use of the cloud would not be advisable.

ELLiptical Curve Cryptography

Or, organizations could look for a more dependable encryption algorithm, which many cryptanalysts believe is available. Elliptical Curve Cryptography (ECC) was developed by Certicom, a mobile e-business security provider, and many other companies are also working on ECC implementations.9 How does it work? Sorry, but I am not smart enough to explain it. But, those who can think that it may provide a faster, easier-to-use and harder-to-break alternative to RSA.10

The potential obsolescence of RSA is a part of the life cycle of information security. Security techniques have a period of usefulness that at one point comes to an end. By way of illustration, the symmetric-key Data Encryption Standard (DES) was long the prevailing method of protecting information. By 2005, it had been withdrawn as the US national standard,11 and by 2008, it was possible to buy commercial hardware that could break DES keys in less than a day for less than €10,000.12

Is ECC the great next wave in the tide of information security? If it is, it will rise to the top only to sink once again sometime in the future. I am very skeptical of “waves of the future.” In the first article I ever wrote for the Journal, two name changes and 15 years ago, I said: “We have seen a number of such technical ‘advances,’ waves of the future all of them, crash on the beach.”13 The tide in the affairs of information security do flow, but they ebb as well.

ENDNOTES

1 This is being written in August 2013. I am indebted to my colleague, James Anderson, for bringing these articles to my attention.
4 Adapted from Shakespeare, William, Julius Caesar, act 4, scene 3: “There is a tide in the affairs of men. Which, taken at the flood, leads on to fortune; Omitted, all the voyage of their life; Is bound in shallows and in miseries. On such a full sea are we now afloat, And we must take the current when it serves, Or lose our ventures.”
5 Op cit, Mimoso
7 There are far too many accounts of such attacks to give a comprehensive citation. One such, chosen more or less at random, is: Lewis, Leo; “Cyber-attack Cripples South Korean Banks and TV Stations,” The Times (London), 21 March 2013, www.thetimes.co.uk
8 Ross, Steven J.; “Cloudy Daze,” ISACA Journal, vol. 1, 2010
9 Elliptical Curve Cryptography (ECC), http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography
10 Just to confuse matters further, there is RSA, the algorithm, and RSA, a security products company that sells encryption solutions. In this article, the references are to the algorithm.
11 US National Institute of Standards and Technology, “Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation,” 19 May 2005
13 Ross, Steven J.; “If PKI Is the Answer, What is the Question?,” IS Audit & Control Journal, vol. VI, 1998
Character Traits of an IT Professional

In this issue’s column, we focus on the individual professional and strive to describe him/her in terms of virtuous traits that help in his/her professional role. It is beyond debate that a professional is not just an aggregation of cognitive knowledge and skills; a professional is a more holistic person with many more traits. While we have some knowledge of how organizations foster ethical practices (e.g., codes of ethics),¹ we have not yet attempted in this column to take a peek at the individual professional: What would it take for an IT professional to be virtuous in his role? This question is too complex to explore fully in a column, but an attempt can be made to gain a basic understanding of this landscape. Admittedly, we aim to generate more thought; this is not a thorough treatise on virtue ethics of an IT professional at work.

Since we are now talking about individuals, not organizations, we can bring into our discussion not just the externalities of the world of work and its rules of behavior, but rather a broad array of who we are, our inner being, our traits that play a key role in defining our norms of behavior at work.

Virtue ethics focuses on the moral character of the person in contrast to the emphasis on rules (in deontology) or the consequences of action (in utilitarianism). The term “virtue” is derived from the Latin word virtus, which over time took the meaning of a description of Roman virtue. Virtue ethics encompasses three broad spheres: virtue, an expression of a stable disposition or character; practical wisdom or prudence exercised by an individual; and eudaimonia, the sense of well-being or flourishing. Our interest is in examining the second sphere, prudence, the origin of role-based traits.

CHARACTER

A person’s disposition is his/her underlying constitution, which bears upon the individual’s decisions at all levels: physical, mental, moral and spiritual, for example. The disposition cannot be turned on or off; it influences all aspects of life—both private and at work. Disposition is permanent (e.g., glass is fragile), while an occurrence exhibiting the disposition (glass, upon impact of a stone, is shattered) is occasional.² You do not see a habitual smoker smoking all the time. On the other hand, a single observed action is, by itself, insufficient to conclude anything about the character of the person. Finally, disposition is not a habit; it is the source that drives actions from within. Proponents of virtue ethics would argue that the moral education that molds one’s disposition is more important than inculcation of rules, for rules may not have the requisite variety or complete context within which exceptions may be made. This broadening of norms of behavior is often considered as spanning the area of morality from a somewhat bounded definition of ethics.³

A person’s character establishes a reason for action beyond any rules. An honest person is wired to practice nothing but honesty, even in acts where rules are vague or absent; where no one is looking; and where no laws, regulations or policies are violated.

PRUDENCE

A virtue ethics framework for a professional includes meta-virtues (moral or scientific virtues) as well as role-constituted (prudential) traits. Meta-virtues (e.g., integrity) are truly the foundation of one’s character. However, their explication in terms of the practice of a professional produces specific character traits, called role-constituted traits (e.g., integrity expressed in the level of transparency in communication). Thus, meta-virtues not only enhance the good of the professional practice, but also help delineate other practical traits, i.e., traits that are practically visible in action. Such role-constituted or prudential traits emerge from what is called phronesis, or the virtue of practical thought, prudence or wisdom. Any prudent behavior warrants the grasp of particulars (or the context), cleverness in dealing with the situation,
insights beyond the surface and a deeper understanding of the consequences of one’s action. The absence of prudence may not make one unethical, but would in all likelihood make one ineffective. A professional wants to be ethical and effective. Preserving the privacy of information, for example, does not mean blocking private data from all eyes. The latter is a drastic solution void of prudence.

So, the next question is: Where can I find a list of role-based traits pertinent to my professional role? This would help me see what traits are warranted in me as an IT professional. According to Shannon Vallor, “…no account of moral action can be complete without attending to the specific role of virtues in directing and motivating such actions, and…the applied context of IT ethics is a uniquely suitable domain for illustrating that necessity.”4 Vallor sketches several role-based traits relevant in the context of the applications of social networking technology: patience, honesty, empathy, fidelity, reciprocity and tolerance.5 Taking patience, for example, Vallor explains that patience is one of the most important virtues for sustaining close relationships and it develops through communicative activities such as listening. As an enduring element of one’s own character, it allows “a feeling on the part of others that you are willing to connect with them on their terms and not just yours, that your interest in them does not end with their ability to keep you constantly pleased or fascinated.”6 If you were a manager responsible for social networking technologies and their applications, you in all likelihood would be interested in patience as a trait, how it plays out in a social network, how to nurture user patience and what design features would facilitate these aims. Most IT managers at Twitter or LinkedIn, for example, would benefit from a deeper comprehension of patience as a trait.

The best way to comprehend the understanding of the role of virtue ethics, particularly role-based traits, in the information systems domain is to view every system as essentially an allocation of tasks between humans and machines based on their respective comparative advantage.7 Thus, all such systems are sociotechnological systems, in which “the reciprocal relationships of causation between technological structure and human agencies [occur, which] can account for the way the affordances of technological systems and the motivations and capacities of human users come together to determine moral outcomes.”8

TECHNOLOGY AS AN ENabler

As a technology professional, most of the time you are probably looking at technology as an enabler of ideas, visions, hopes and aspirations. These ends goals can be good or bad. For most of us, the overwhelming perception—if not conviction—is that we are working on delivering something good—good for the business and good for the consumer of end products and services that the technology will enable. The third sphere of virtue ethics—eudaimonia, the sense of flourishing—also comes into play here as we think of the well-being of the company, the community and societies in general. You would be close to the thought in practice if, for example, you were working on an innovation in health care.

With specific reference to technology as an enabler, one example is the small telematic device promoted by auto insurance companies.9 If an auto driver opts to install the device in his car, he gets feedback regarding his driving behavior. The insurance company would reward him with a usage-based insurance premium, which may be much less than the traditional ways in which insurance companies determine his risk (their loss potential) for quoting auto insurance premiums.

As an IT manager responsible to drive this technology project, you would work with managers on the business side as well as on the technology side. You would want to capture the most relevant traits of a good driver. For this, you may need to capture the local geography, turns and roundabouts, signal lights, and stop signs along the way. And yet, you are concerned that the telematic does not reveal the exact location of the driver, that it does not capture GPS map locations along the way. Striking a balance between what is relevant for the business decision with what is fair treatment of the driver (e.g., in terms of privacy of location visited) is what you would seek. This product would likely cause considerable panic regarding the driver’s privacy because of the huge amount of shareable data. You would want to minimize these concerns and yet be truthful and transparent in your communication. These are all signs of role-constituted traits that you need to engage to deliver a holistic solution to the telematics project. Such traits may not be apparent from reading the code of ethics; nevertheless, their consideration...
is central to an IT manager acting as a moral agent in the project. If the only forces at work were marketing and revenue forecasts, the manager would likely fall far short on delivering goods that satisfy the sense of well-being (eudaimonia).

**MOTIVATIONS AND CAPACITIES OF HUMAN USERS**

Technology as an enabler is only a beginning. The reality is that the human user, motivated by incentives and fears, could respond differently from what was originally expected. The voluminous amount of data collected by the telematics is a cause for concern; the company might be legally responsible to provide such data to courts of law, for example. Some may reject the idea outright because of “big brother” fears, while others are tempted by the discounts they might earn. Some may feel that the system would help them become a better driver, as they respond to feedback from the system and change their driving habits. Drivers may also ponder the long-term consequences. For example, if a vast majority would become better drivers over time, would this result in lower income to the insurance company, which may prompt increases in premiums? Or if a driver cannot improve on his habits, would it mean that his premium may increase in the long run although there is no penalty imposed at this time?

Putting out a good product that delivers its stated objectives is challenging; the bigger challenge, however, is anticipating and responding to user behaviors. While aiding the company to prosper financially through business growth, the bigger idea is to reward safe drivers and coach, or punish, the bad ones. In the end, the number of lives that can be saved could spell the insurance industry’s moral bottom line. In the tally, hopefully, managers of the project have played a pivotal role—using their role-constituted traits implicit in the company’s generic-looking code of ethics.

**ENDNOTES**

2 Ryle, G.; *The Concept of Mind*, Hutchinson & Company, UK, 1949
3 Some may think of ethics as avoiding the problem, thinking more in terms of complying with the rules of the organization (including the code of ethics) and the laws of the land. The assumption is that behavior that satisfies the rule book is ethical.
5 ibid., p.164
6 ibid., p. 165
8 *Op cit.*, Vallor, p. 158
Regis University 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 18 consecutive years.

Classes can be taken on campus or completely online.
Robby B. Sebopeng, CISA

Robby B. Sebopeng was appointed the auditor general of Botswana in 2010. He had been the acting auditor general since 2008 and the deputy auditor general from 2003-2008. His career began with the Botswana Government in 1983 as an assistant auditor in the Office of the Auditor General.

During his career in the Office of the Auditor General, he introduced the application of monetary unit sampling, general audit objectives, and the concepts of risk and materiality. He pioneered the establishment of email, Internet access and an automatic computer backup system as part of the Office's disaster recovery plan. He introduced COBIT® in Botswana’s public sector to ensure that business objectives are achieved and that undesired events are prevented or detected and corrected.

In his personal time, Sebopeng enjoys spending time with his family, listening to music, reading, gardening and traveling.

Q You have had a long history in the Office of the Auditor General of Botswana, culminating in your appointment as Auditor General in 2010. To what do you attribute your successful growth in the office? What advice would you give to others looking for similar growth within their own career path?

A Within the first six months after joining the office in 1983, I had already completed several complicated audits such as audits of revenue collection and construction projects. My reports were immediately recognized by management. This recognition motivated me to research and keep on producing even better results. The best reports are included in the Auditor General’s Annual Report, which goes to the National Assembly.

I took advantage of on-the-job training, which led me to specialize in value-for-money training and, later, information systems (IS) support and IS audits. I always made sure that I possessed the relevant knowledge and skills needed for my job—these were scarce skills then and still are today.

My advice to my colleagues is that employees who progress to the top are those who derive satisfaction from their work, develop themselves, are willing to take new challenges and are not afraid of change. I strive to excel in my work and I am patient and loyal to the public service. Furthermore, I always take advantage of the opportunities provided to me.

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

A More often than not we have come across many government departments that have questionable governance practices. With the pervasive use of information technology in business processes across government has come the critical need for strategic leadership to ensure that the organization’s IT sustains and extends the organization’s strategies and objectives. The absence of leadership and organizational structures from which to drive IT investments leads to a high risk of failure. Despite the many developments in governance there are still many leaders that fail to see IT governance as an integral part of overall enterprise (corporate) governance. As a result, many IT units within organizations are left to direct their activities leading to poor strategic alignment.

Another prominent risk factor is poor management of IT projects. Many government departments do not have the technical expertise to develop IT solutions for their business needs. This often results in the department outsourcing the system development process and, as a result, introducing such risk factors as vendor failure to deliver, poor quality, lack of documentation and missing functionality. Lack of a system development life cycle (SDLC) has been shown to lead to more errors and cost overruns. Even more worrying is the loss of business knowledge or ability to take over responsibility from the vendor. The outcome of this is that the new system is often abandoned or the organization is tied to a perpetual support contract with the supplier.
These risk factors can be mitigated by adopting best practices in governance. IT governance is the responsibility of executive management, and it should be borne in mind at all times that IT investments are meant to help the organization attain its strategic goals (mandate). It then follows that organizational structures and processes (policies and standards) are introduced to guide operations that will align all efforts toward the ultimate goal. A third party or contractor engaged by the entity is expected to live up to the standards set out by the entity, thus ensuring that there is no deviation from management guidance.

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

A IS audit has not only become an integral part of regulatory audit, in terms of the requirements to gain an understanding of and review internal controls, but has become a key source of audit evidence. Over the years, the involvement of IT auditors on engagements has grown and continues to grow to a point where the IS audit function is no longer an option. In the advent of computerization or automation of accounting systems, complex IT environments have been introduced that require a specialized skill set: IS audit. An effective and efficient audit is dependent on the collection of adequate audit evidence to support assertions. Hence, the collection of such evidence rests on the auditor’s ability to navigate and interrogate the system as one, if not the only, repository of the accounting records/information.

With the reliance that audit engagements or financial auditors place on IS auditors, it is inevitable that the IS auditor’s competence is questioned from time to time (area of concern). There is a need for IS auditors to demonstrate that they have the required skills and knowledge to carry out the task at hand. The Certified Information Systems Auditor® (CISA®) designation is a globally accepted certification that demonstrates these competencies. My advice to IS auditors, thus, is to work toward obtaining and maintaining CISA certification.

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 Having been one of the first CISA professionals in a country with scarce IS auditors, it is obvious to me how marketable CISA holders are, especially when CISA is coupled with accounting and business courses and later strategic management courses.

It is obvious that there can be no audit without information technology diagnostics and performance audit (value-for-money studies) and forensic audit to meet the modern customer’s needs. My office not only looks for professional accountants, but also hires IS auditors and other qualifications. Unfortunately, IT qualifications are very scarce in Botswana and throughout the region.

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

A Having qualified with accounting degrees through the post-graduate level, industry professionals often considered me an academic. To do the accounting and auditing work in practice, the law demanded that I be professionally qualified. This is why professional recognition is critical. CISA and hard work are what helped me to succeed and overcome these roadblocks.
What Every IT Auditor Should Know About Data Analytics

In the last column in this space, the introduction described the current IT environment and reasons why circumstances are driving an increasing demand for subject matter experts (SMEs) in CAATs, data mining and data analytics. Needless to say, there are a variety of needs in business today for effectual data analytics.

For several years, there has been a burgeoning segment of the IT profession known as business intelligence. A range of tools has been developed and used to assist businesses in mining valuable information from its own data to enable it to have more effective strategic and operational insights into executive decision making. Data analytics, as used herein, is similar to business intelligence. Because of the ways data analytics can be used and benefits gained from examining data, there is ample opportunity to apply the same methodology to IT assurance or IT reviews of this growing segment.

This space has also included a series of articles that, when combined, describe the process of using CAATs from data extraction, to data transformation and now to data analytics. The series is modeled after the data warehouse concept of ETL (extract, transform and load) when building the warehouse database. This article will describe factors for the IT auditor to consider in conducting data analytics.

Designing an Analytic Program

There are several key aspects of designing an effective analytic program. Those aspects can be determined through a series of questions:

- Who are the key players?
- What data are needed (tables and fields)?
- What are the purpose and scope of the testing?
- Who will get the report?
- Where are the data residing?
- How will data be requested and/or obtained?
- What tools will be used to perform data analytic tests or procedures and why?
- How will the tools selected be used (processes, tests)?

Answering these questions will enable the IT auditor to design an effective analytic program. Obviously, the IT auditor must have some knowledge of the organization, systems, data files and tools available, as well as the capabilities of those tools.

Analytic Methodology

The IT auditor will need to follow a methodology in getting the data and analyzing the data properly. The approach is similar to that of an IT assurance project or, for internal audit, IT reviews.

Scope

As with all assurance and review projects, the process begins with defining the scope of what needs to be done. This can be done by answering these questions:

- What is the purpose of the audit?
- What is the objective of the audit’s conclusions?
- What parameters need to be applied to the data to accomplish that purpose?
- Where are the data found in the financial or other system?
- What is the risk (e.g., in data reliability)?
- What does the scope of the source data need to be in order to meet the objective and address risk?
- What other information will impact the nature, timing and extent of the procedures to be performed?

After answering these questions, the IT auditor should be able to determine the best approach to take to satisfy the objectives and purpose. Next, a planning meeting, where issues such as the specific procedures and tests can be discussed, should be set. Consideration should be given to relevant data that lie outside the auditee’s systems and data files (e.g., cloud, data center, industry data), and to any issues in getting data, such as usefulness and reliability. Individuals from both IT and the business should be involved, as both perspectives prove...
beneficial. IT understands how the data look, where they reside and how best to obtain them, while the business can answer questions on what information may be required to meet objectives and the flow of data from a business perspective.

Data Acquisition
After the scoping step is complete, the IT auditor is ready to acquire appropriate data to properly perform testing that meets the objectives set forth. Data acquisition can also be referred to as data extraction. Some common elements to consider include:

- Developing a request for data (a standard request form should be developed and used)
- Meeting and reviewing the request form with the appropriate person to obtain the data (maybe with someone in IT, accounting and/or the business)
- Obtaining a sample of the operational transaction processing system (TPS) data (if necessary to ensure proper layout and manageable process)
- Inspecting pro forma data (where feasible), before the final extraction
- Timing (associated with scope and purpose)
- Transferring extracted data from TPS to IT auditor

One key here is about being efficient. Using a standardized request form, for example, should take less time than other alternatives and will reduce time if the auditor chooses to perform this testing again at a future date. The inspect step is critical to efficiency. To ensure that the data being extracted are satisfactory, IT auditors should have some part of the extraction displayed on a screen or partially printed so they can validate the data extraction template and process (which are examples of pro forma data). Going back later—after the discovery that data are incomplete or inaccurate—can be time-consuming.

Data Validation
This step is also critical to a successful data analytics program, just as any other audit evidence. That is, the IT auditor needs sufficient assurance as to the data’s veracity and reliability before performing tests and procedures. That might include understanding, or even testing, controls on the TPS or the IT function (e.g., IT general controls). The goal is to ensure that the data acquired are the precise data on the TPS and they are sufficient for performing the testing required.

That can be done by:
- Validating balances independent of the data set extracted
- Reconciling detailed data to report control totals
- Validating numeric, character and date fields
- Verifying the time period of the data set (meets scope and purpose)
- Verifying that all necessary fields in scoping are actually included in the acquired data set

Validating the data definitions of columns and fields is important because some commands on some CAATs require the target field to be “numeric” or a “date” or “character.” This is also important because the data may appear to be numeric, but be defined, or extracted, as “character.”

Execution of Program
Once data have been imported and validated, the tests can be executed. These tests, generally speaking, enable the IT auditor to:
- Gain an understanding of the data
- Perform ad hoc data analysis
- Run standard scripts
- Run nonstandard scripts
- Sample data
- Run any other analytic program test or procedure

Documentation of Results
Documentation should provide for a clear understanding of the testing purpose, data sources and conclusions reached. The tests should be repeatable. That is, the information contained in the documentation should allow an experienced IT auditor, with no previous experience with the particular testing, the ability to understand and reperform the testing and get the same results.

The good news is that most CAATs provide some automated recording of tests run and their results. It could be a simple matter of copying and pasting to generate much of the documentation.

Review
All work performed should be reviewed to ensure that the testing procedures have been adequately performed and the results analyzed to look for consistency with conclusions documented. The review should be performed by a qualified person (i.e., an SME). Possibilities include:
- Self-review (not recommended)
• Technical review (for scripts and should be performed in conjunction with an independent review)
• Independent review by a team lead (in charge)
• Independent review by someone not on the team

Retention and Archiving
Retention provides several benefits and fulfills multiple purposes, including:
• Regulatory requirements
• Contractual requirements
• Reperformance needs
• Litigation (which often includes reperformance)
   Also the nature of things to be retained should be carefully considered. Items to consider include:
• Program files
• Scripts
• Macros/automated command tests
• Data files

Automated command tests refer to the fact that most CAATs allow the IT auditor to save a complicated command/test as a macro-type object in the CAAT for future usage. It typically is efficient to save certain commands/tests and reuse them on future audits or reviews in which a keystroke or click of the mouse will execute a fairly complex command/test.

In addition to what is retained, the length of retention should also be considered.

APPLICATION FOR IT ASSURANCE
Applying all of these concepts in an IT audit or review is relatively straightforward, but creativity always helps find effective uses for the IT auditor. Data analytics can be effective for IT auditors in both planning (e.g., evaluating risks) and field work, for example, in:

• Combining logical access files with HR employee master files for authorized users
• Combining file library settings with data from the change management systems and dates of file changes that can be matched to dates of authorized events
• Matching ingress with egress records to identify tailgating in physical security logs
• Using data analytics results to produce reports (e.g., group, summarize, exceptions/detail of devices)
• Reviewing table or system configuration settings
• Reviewing system logs for unauthorized access or unusual activities
• Testing system conversion
• Testing logical access segregation of duties (e.g., analyzing Active Directory data combined with job descriptions)

Other fruitful areas include: P-card review, testing of automated controls (by reviewing data associated with the process), Payment Card Industry Data Security Standard (PCI DSS) compliance and testing of general financial reporting.

CONCLUSION
There are a variety of ways data analytics can provide cost-effective benefits to IT audits and reviews. Creativity in spotting opportunities is certainly a plus. This may require an SME to help identify the majority of the opportunities, but any IT auditor who understands CAATs, data and data analytics should be able to find some ways to improve the audit program or review plan by using data analytics.

ENDNOTES
4 Op cit, Singleton vol. 6 2010 and vol. 5 2013. Steps in this process are described in these two articles.

ACKNOWLEDGMENTS
A special thanks to Michele Schaeffer of Carr Riggs & Ingram for sharing her expertise on data analytics and her contributions to this article.
The use of the Internet has evolved a great deal in the last two decades. A few years ago, web sites were mere information repositories with the primary objective of disseminating information. In today’s world, the Internet and World Wide Web have become a hub of online commercial transactions. So much so that global e-commerce revenues are expected to reach US $963 billion by 2013.¹

The importance of web applications cannot be underestimated in this growing e-world. Web applications are the genre of applications that are accessed via a web browser.

Web applications are very popular for many reasons, including the ease of reach and use. Almost all web users have at least one web browser installed on their computer. Users are familiar with navigation using a browser, which means that web application owners are saved from the trouble of distributing and installing the client interface of the software at the user’s end and also training the user. It is easy to develop a web application with the availability of a wide range of easy-to-use development tools.

However, web applications are not without weaknesses. There is a range of security vulnerabilities associated with the use of web applications. If these security vulnerabilities are not handled properly, it exposes the back-end servers and databases, resulting in further losses—financial and nonfinancial. Gartner has noted that almost 75 percent of attacks are tunneling through web applications.² In turn, this means that security of web applications is as important, if not more so, as security of other components of a web solution, such as network security.

To secure web applications, the developers would have to visit the enemy’s camp.

The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, 2nd Edition is a repository of tools and techniques to hack any web application. It allows the reader to step into the shoes of hackers and see the world through their eyes.

The book should be read by anyone with responsibility for ensuring the security of web applications. Because it is technical in nature, the book would be most beneficial to those who have hands-on experience working on security features of any web application. The book is domain-independent, thus the concepts can be extended to any domains that employ web applications for critical and sensitive functions.

This is the second edition of the book and, as such, it covers changes in technology and emerging vulnerabilities since the first edition. The second edition also facilitates trying out certain concepts.³ There are 21 chapters in the book with the bulk of it dedicated to explaining the tools and techniques of breaking any web application.

The security of web applications will remain important as long as e-commerce is around. With the changing times, new technologies introduce new vulnerabilities, but, ironically, existing vulnerabilities will be further exploited by perpetrators to enhance their gains. This book is a handy weapon in the armory of security consultants as they secure web applications.

ENdNOTES
¹ De Lange, Jip; Alessandro Longoni; Adriana Screpnic; “Online Payments 2012—Moving Beyond the Web,” InnoPay, 2012
³ The online labs are subscription-based.

EDITOR’S NOTE
The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, 2nd Edition is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this Journal, visit www.isaca.org/bookstore, email bookstore@isaca.org or telephone +1.847.660.5650.
The word “compliance” is used more and more to refer to the corporate practice of seeking to ensure adherence to and safekeeping of procedures and regulations. Similar to the terms “good habits” and “corporate behavior” (ethical and honest) being used to refer to enhancing clear, effective and efficient management of the business. Along these lines, an enterprise’s compliance function is in charge of safeguarding its operations, since it must always be vigilant in identifying any attempts at altering the “right corporate order” and interfering with and overcoming them as required.

This trend is a warning that world-class corporations are increasingly demanding of themselves high levels of corporate assurance that rely on people and processes to ensure that the execution of their activities does not follow a random path, but instead conforms to open, ethical and transparent corporate practices.

In light of this and the corruption scandals at international and domestic levels globally, it is necessary to insist on a culture that incorporates beliefs and values into its structure. The culture must also include strategies that foster behaviors akin to good corporate reporting and control practices, and can guarantee responsible corporate processes in respect to the enterprise’s global results.

### KEY FEATURES OF THE COMPLIANCE FUNCTION

There are several approaches to defining the compliance or chief compliance officer (CCO) function, which, on first review, show an inquisitive or accusatory role in terms of compliance with regulations:

A **CCO is a corporate official in charge of overseeing and managing compliance issues within an organization, ensuring, for example, that a company is complying with regulatory requirements and that the company and its employees are complying with internal policies and procedures.**

The definition of a CCO presents a corporate executive who considers corporate benchmarks, validates their application and reports on the level of compliance to determine any gaps and risk derived from a limited execution of the benchmarks. That is, 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. This helps strengthen the self-assessment that should be an inherent part of processes and their participants.

Others define compliance as “adherence to and the capacity to show observance of directives, requirements defined by laws and regulations, as well as voluntary requirements, as a result of contractual obligations and internal policies.”

This definition is restricted to a function of law enforcement and ensuring third-party obligations. It does not address the fundamental resources required to consolidate the practices associated with mandates whose fulfillment is compulsory, such as culture and risk anticipation, affecting corporate dynamics. In this sense, in the same way as noted previously, the definition relies on control execution reports defined by the corporation, which indicates a certain level of process assurance and accounts for the evidences revealed by the mitigation status of the identified risk.

The following are five key features for the development of an effective compliance function:

- **Authority**—Authority must be adequately allocated in the organizational structure with a reporting level that ensures independence and the incorporation of practices to help an organization move from one maturity level to the next.
• **Responsibility**—Its duty is fostering the execution of the compliance program and the implementation of the function while working with specialized professionals from other areas of expertise in charge of addressing key identified risk factors and their impact.

• **Competency**—The officer in charge of compliance must have the necessary qualifications, expertise and training to ensure adequate performance in that position.

• **Objectivity**—The compliance officer must be able to withstand organizational pressure regarding specific situations, to keep the focus on the assurance of practices and escalate any findings to the relevant level.

• **Resources**—The resources required for the function, considering the size of the enterprise and the nature of the risk it faces, must be available.

These attributes indicate that the compliance function, notwithstanding the permanent monitoring and control exercise, should implement a concrete and measurable executive reporting style and follow-up. This can serve as a benchmark of maturity so that improvements can be identified through interaction with the business areas.

### COMPLIANCE FUNCTION AND INFORMATION SECURITY

The activities associated with the compliance function stem from searching for limitations or restrictions that do not allow for reinforcing behaviors and practices aimed at increasing the level of assurance of an organizational reality. This means understanding the priorities of the business and its value-generation model in order to free the organization from a minimum requirement culture and drive it toward a maximum requirement practice. In this context, compliance functions are vigilant about the risk of noncompliance, enhanced by corporate scenarios related to penalties, errors or omissions, fines, and other measures, and warn the enterprise of the systematic application of bad practices, which may result in incidents destroying enterprise value and deviating the business from its medium- and long-term strategic path. Considering this argument within the framework of information security, it is clear that the information security officer performs a compliance function that requires the five key features described previously to achieve the transformation of the business and increase the level of failure resistance, with a known response to exceptional circumstances.

Thus, when in the development of the information security program, risk is anticipated, a protection-driven culture is promoted, operation is ensured and the basis of the compliance function is founded at the enterprise level. These features of a compliance function seek to strengthen behaviors, practices and actions aimed to safeguard results, protect corporate image and, above all, forecast the future. (figure 1).

![Figure 1—Key Features of the Compliance Function](image)

The compliance function as a source of good practices and active monitoring systems for businesses finds a natural instance of execution in information security. This is because the compliance function defines recommendations and action plans that fulfill corporate directives and moves the corporation toward a culture of due diligence and responsibility in the processing of information.

### THE NONCOMPLIANCE RISK

The noncompliance risk can be understood as the organization’s inability to prevent, detect, correct and maintain an understanding of the current and/or emerging risk affecting corporate operation and/or its medium- and long-term strategic objectives. Along these lines, it becomes necessary to develop a risk management strategy that not only allows for reversing the imminence of the occurrence of risk, but also promotes repair and transformation of the enterprise to anticipate or visualize the situation.
Regardless of the way in which risk management methods set certain execution conditions, Deloitte\(^4\) proposes a method that seeks to ensure an approach focused on addressing noncompliance risk management, based on international standards, and considering aspects such as context of occurrence, risk requirements or conditions, risk analysis, action prioritization, control effectiveness assessment, monitoring, reporting, and communication. While this approach fosters specific actions, it does not warn of the asymmetry of failure unavoidability and deviates to the cause-effect model that characterizes traditional risk management.

In this context, noncompliance risk, understood as a key factor to information security, requires developing the skill to see, from the perspective of failure opportunities, the structural links among technology, processes and people in order to condense potential threat scenarios. This shows anticipation of exceptional situations and does not merely warn about regulatory noncompliance inherent to certain situations, but also builds on the supporting forecasting capability faced within its business context and considers the responsibility toward all stakeholders (figure 2).

Thus, information insecurity is the foundation from which noncompliance risk is understood; it is a double benchmark that invites the enterprise to find bad-practice emerging patterns in its everyday practice, which, in time, could erode the privileged position of the enterprise in the industry. That is, an event of greater magnitude than a predictable threat may go unnoticed by the risk matrix, since it is not manifested concretely to allow notice of an obvious hazard.

When noncompliance risk is understood as an item beyond compliance with an enterprise’s internal and external regulatory requirements, one makes way for a structural and systemic perspective that allows the enterprise to understand and reveal the hidden laws of economics and psychology and the link to the business sector, enhancing its capabilities to identify disruptors or unidentified agents that change the way of doing business in its own industry.\(^5\)

**CONCLUSION**

Insight over the function of compliance and its link to information security practices means dwelling on the capabilities required by an enterprise to differentiate itself.
from the competition and ensure a privileged position in its business sector. The compliance function requires that its head officer (CCO) breaks the pattern of the surrounding circumstances to find an interconnection of processes, expertise, information technologies and tools, and emerging trends—anticipating its strategies to move forward in valuable areas for its clients and stakeholders.

Although the compliance function is linked to a reduced perspective of reliance on the regulatory context and the promotion of an integral and ethical culture, the function must understand the way in which the enterprise generates, attracts and protects value. By enhancing its capabilities and context sensors, it may continue to fulfill its clients’ needs, even when they vary over time.

Consequently, once the function of information security is understood as a natural enforcement of corporate compliance, it becomes necessary to walk along the information insecurity path to establish the potentiality of noncompliance risk. This helps the enterprise detect future patterns of environmental threats to prepare and respond to these threats and to develop new practices that create opportunities and unbalancing factors, which change the strategic reality of the company and its context. Developing the enterprise’s anticipation capability in terms of information insecurity allows it to identify risk synergies, increase monitoring capability, and optimize resources and operational management, so that the enterprise is prepared to act in response to unexpected situations and move confidently, while having the necessary skills to recover from total or partial failures.

Consequently, information security as a compliance function should be synchronized with the enterprise’s normal dynamics and its information flows to ensure security and control practices inherent to current business risk. Also, it is important to keep a constant understanding of inner relationships among operations, clients, processes, and big and ambitious corporate goals.

Finally, the compliance function—as management’s guarantor in assuring the operation, the development of an assurance culture and the forecasting of new risk scenarios—finds a natural ally in information security, which seeks a natural sphere to promote structural change and reach new maturity levels in the relationship among people, processes and technologies that goes beyond adherence to a regulatory benchmark or noncompliance deviation report.

ENDNOTES
1 TechTarget, “Chief Compliance Officer,” http://searchcio.techtarget.com/definition/CCO
Subcontracting certain IT functions has been common over the last few decades (e.g., in development, housing, hosting and outsourcing), but the irruption of cloud computing has taken it to a new level. And, although some argue that cloud computing is only an evolution of outsourcing, it is, in fact, a new paradigm that is changing the approach to IT. Instead of something that organizations make themselves, IT is becoming a service they consume (similar to what happened with energy in the industrial revolution).

Security professionals have long been aware that subcontracting does not eliminate the IT risk that organizations face; in fact, with subcontracting, organizations lose control over the security measures implemented by service providers. Thus, security professionals have applied a recipe based on audits and certifications to build trust relationships with these service providers. However, this approach must change in order to fit the new paradigm. Despite audits and certifications, users continue thinking that more transparency is needed:

Among the limiting factors [of cloud computing adoption], security and data ownership (both related to the ability to protect information assets) and factors related to legal issues, contracts and regulatory compliance topped the list. The fifth factor, information assurance, is significant because it is related to the transparency of cloud offerings and management’s ability to gain comfort that information is protected to the required degree.¹

That is to say, although security professionals have been applying best practices and asking for security audits and certifications, these mechanisms have not been able to transmit the level of trust required by customers of cloud computing services.

DO AUDITS AND CERTIFICATION REALLY FAIL IN PROVIDING TRANSPARENCY?

Security audits and certifications are the foundations of trust-building between customers and providers, but they have some characteristics that oblige the development of further mechanisms:

- Typical audit reports cannot be freely distributed; they are only for the parties involved (typically, the customer and the provider), which requires the provider to be audited by every (potential) customer.
- Service Organization Control (SOC) reports can be made public, but then other issues appear: The criteria used by the auditor may or may not be relevant to the customers because they have been fixed by a third party. If the criteria are not relevant for the customer, the first point is applicable again.
- Finally, regarding certifications, there is no certification for the security of services. What providers are certifying is their information security management system against the ISO/IEC 27001 standard. This certification has two issues:
  1. It does not say anything about the security measures implemented by the provider; it indicates only if the provider has an IS management system.
  2. It obliges the customer to understand the scope of the certification because it could be relevant for the service to which it wants to subscribe.

Of course, 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. The certification provides only simple information: that the provider implements an ISMS following ISO/IEC 27001.
The tools that security professionals have for the moment require customers to be security specialists in order to understand the outcomes and do not provide comparable results.

Catherine Ashton, High Representative of the European Union for Foreign Affairs and Security Policy, has highlighted the same issue and invites the industry to “develop industry-led standards for companies’ performance on cybersecurity and improve the information available to the public by developing security labels or kite marks helping the consumer navigate the market.”

A NEW TOOL: RATING
Exploring the economic theory that explains the relationship between customers and providers may be useful while looking for new ways of building trust in the cloud services market. In fact, the security of cloud services (i.e., cybersecurity) faces a well-known problem: information asymmetry.

This concept was explained by George Akerlof in 1970 and refers to “decisions in transactions where one party has more or better information than the other,” which is exactly what happens in the cloud service market regarding security: The provider has better information about the security measures implemented than the customer.

Information asymmetry creates an imbalance of power that can sometimes cause the transactions to go awry. The most common problems that arise are adverse selection and moral hazard. The worst consequence that information asymmetry could have is the disappearance of the market.

Economists Michael Spence and Joseph E. Stiglitz analyze two primary solutions to this problem:

1. **Signaling**—Signaling means that one party (in this case, the cloud provider) credibly conveys some information about itself to another party (the customer). This could sound a bit strange, but security professionals are very familiar with this kind of mechanism, called a security certification, which provides a seal that organizations can use to signal that they are compliant with some set of requirements.

2. **Screening**—The screener (the one with less information; in this case, the customer) attempts to rectify the asymmetry by learning as much as it can about the provider. Again, it may sound strange, but security professionals use screening continuously; it is called an audit.

Once the underlying economic theory is understood, is there any other option to build up trusted relationships?

There are alternatives in the economic world. The same problem about information asymmetry that the cloud service market faces today was faced at the beginning of the debt markets, for example. In those days, investors were in a weak position in relation to companies asking for financing: They did not know how likely the debtors were to reimburse the credit. Thus, credit agencies began to rate debtors as a signaling mechanism.

SECURITY LABELS USING A RATING METHODOLOGY
Using these concepts from the economic world in the security field, a security labeling system for IT services can be implemented. This system could help (potential) customers to understand easily the security characteristics of the services in the market and analyze whether they fit their needs according to their risk profile (see figure 1)—in the same way that household appliances are rated by their energy consumption or cars are rated for their safety. The labeling system is also more efficient, because all the customers willing to subscribe to a service do not need to audit the security controls due to the approach “audit once, use many times” (in the way that FedRamp does).

Rating security measures according to, for example, five levels (from A to E, A being the best) in the different dimensions of cybersecurity (confidentiality, integrity and availability [CIA]) could provide 125 different possible ratings (5 levels, 3 dimensions) to help customers choose those services that best fit their needs. This is unlike certification, which divides all the providers into two groups: those that are certified and those that are not.

The rating methodology outcome should be a set of three letters indicating the soundness of the security measures implemented by the service provider in each specific service in the mentioned security dimensions. For example, a rating of BDC means (figure 2):
• A rating of B in the confidentiality dimension
• A rating of D in the integrity dimension
• A rating of C in the availability dimension

In the example, the service pays more attention to confidentiality aspects, but it is not suitable for those with high availability requirements (who should look for A or B ratings in the third dimension).

BUILDING THE RATING SYSTEM
The first step to building the rating system is to create a system to assign a level (from A to E) to the security measures implemented by the provider. To do so, two tasks should be carried out:

1. **Elaborate an inventory of security measures to be evaluated.**
   This task should be supported by generally accepted standards, controls and frameworks (e.g., National Institute of Standards and Technology [NIST] standards, ISO 27002, the Payment Card Industry Data Security Standard [PCI DSS], ITIL, the European Union Data Privacy Directive).

2. **Define the five levels for each security measure.** This definition has two components: (i) Security measures that are processes are rated according to their maturity level (similar to the COBIT Process Assessment Model); and (ii) Security measures that depend on technology (e.g., security configurations, tools) are rated according to their robustness (e.g., a password of 12 characters is stronger than a password of six characters, and a password of 12 characters is stronger if it requires a combination of letters, numbers and special characters).

Besides security controls maturity (analyzed previously), there are other elements that should be considered in the rating methodology to build up the security label because they contribute to trust relationships (figure 3):

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.
• **Vendor reliability**—Information related to the strategy of the service provider including business plans, financial stability, management bodies, service road map and qualification of employees

• **Resilience**—The ability of the provider to recover in the case of incidents

---

**CONCLUSIONS**

Security audits and certifications are necessary, but not sufficient, conditions to build up trust relationships in cyberspace. Security professionals must be a step ahead and propose new ways to evaluate the security and resilience of IT services and be prepared for new scenarios such as those caused by cloud computing and cybersecurity. In this situation, security labeling based on a rating methodology could, for example, help users understand the risk they face when using IT services, compare different options and be more efficient in the procurement processes.

---

**ENDNOTES**

4 Adverse selection “refers to a market process in which undesired results occur when buyers and sellers have asymmetric information (access to different information); the ‘bad’ products or services are more likely to be selected.” Chandler, Seth J.; “Adverse Selection,” The Wolfram Demonstrations Project
5 A moral hazard is a “situation where a party will have a tendency to take risks because the costs that could incur will not be felt by the party taking the risk. In other words, it is a tendency to be more willing to take a risk knowing that the potential costs or burdens of taking such risk will be borne, in whole or in part, by others.” Dembe, Allard E.; Leslie I. Boden; “Moral Hazard: A Question of Morality?,” *New Solutions*, 10(3), 2000, p. 257-279
7 In screening, “[t]he underinformed party can induce the other party to reveal their information. They can provide a menu of choices in such a way that the choice depends on the private information of the other party.” Stiglitz, Joseph E.; “There Is No Invisible Hand,” *The Guardian Comment*, UK, 20 December 2002
8 In 2001, the Nobel Prize in Economics was awarded to George Akerlof, Michael Spence and Joseph E. Stiglitz for their “analyses of markets with asymmetric information.”
Risk assessment has become an integral part of today’s organization as business operations are expanding and being diversified, resulting in increased risk exposure. In addition, the tightening of regulatory bodies across the globe has resulted in the emergence of assurance functions such as operational risk management, information security, internal audit, internal control and compliance. Each of these functions stresses the importance of risk assessment within the organization and performs independent comprehensive exercises within the specific domain.1

Generally, there is room for debate about integration among all assurance functions and the use of an integrated risk assessment program (IRAP). Most standards have mapping documents available that show control overlaps among various standards and best practices, but they are rarely followed and adopted by the assurance functions of organizations.2, 3, 4

The question arises: Is the integration of assurance functions really a need?

Generally, professionals working in compliance, audit, risk management or information security departments face the following issues that give rise to the need for an integrated risk management program:

• Risk assessments performed by assurance professionals are specific to their respective domain and do not give a holistic risk profile of the organization, which results in the presence of unmitigated and undetected threats.
• Often, assurance functions need different departments to nominate representatives for their correspondence and coordination. Typically, a department can assign the responsibility to a single resource. The efforts of the nominee multiply as each assurance function forms its respective teams within the organization. The individual often ends up performing similar tasks, such as self-assessments, statistics reporting and call-tree updating, for different groups, resulting in duplication of effort and repetitive and redundant activities.
• 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.
• The different audits and review exercises of the assurance functions often frustrate the auditee because of the constant information gathering and response requirements associated with these activities and performed in short intervals of time.
• The auditee sometimes provides different resolution and target dates for observations that are similar to those reported by different assurance functions in their audit or review reports.

Keeping these issues in mind, organizations could start considering integration of assurance functions by identifying the overlapping and redundant activities. Examples of areas of common interest include:

• Obtaining nomination for departmentwide coordinators
• Conducting awareness sessions
• Obtaining departmentwide asset inventory
• Identifying business processes
• Identifying internal and regulatory requirements
• Performing business impact analysis
• Assessing risk
• Investigating incidents
• Reporting to management

The assurance functions should synchronize and align with common activities with respect to their scope, objective and methodology. This would allow for the development of an IRAP. For risk assessment, international standards are used to ensure that best practices and controls are used to mitigate risk associated with systems, services and processes. An illustration of integrating two departments is depicted in the following figures, where one department uses ISO 27001:2005 and the other Basel II.5
Figure 1 identifies the steps to carry out risk assessment of different departments through integrated self-assessment.

Figure 1—Methodology

<table>
<thead>
<tr>
<th>Basel II and ISO Control Mapping</th>
<th>Assign weight age to department.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify Business Criticality</td>
<td>ISO 27001 Controls</td>
</tr>
<tr>
<td>Identify Likelihood</td>
<td>Determine number of preventive and detective controls against threats.</td>
</tr>
<tr>
<td>Identify Impact</td>
<td>Determine number of corrective controls against threats.</td>
</tr>
<tr>
<td>Calculate Risk</td>
<td>Risk = Criticality * Likelihood * Impact</td>
</tr>
</tbody>
</table>

Figure 2 specifies the factors for assigning the values for criticality, likelihood and impact.

Figure 3 is a demonstration of an IRAP.

The risk assessment integration could benefit the organization in the following ways:

- **A holistic risk management approach**—Effective coordination among assurance functions enables each function to understand the key risk areas of the organization. This, in turn, results in mitigation of risk based on consensus. Each assurance function evaluates risk with respect to its domain and views risk collectively to give an aggregated mitigation.

- **Synchronized risk assessment efforts**—The departments can strengthen each other by providing assistance through knowledge and resource sharing. This could include performing joint risk assessment exercises for areas of common interest or sharing materials such as risk assessment reports and audit programs. This can reduce redundant engagement of resources and improve synergy across assurance functions.

- **Maximum risk treatment**—When risk is analyzed from various perspectives, the likelihood of gaps within the mitigated control is greatly reduced. Maximum risk treatment results in minimal residual value, which can be accepted easily by the organization.

- **Standardized control across the enterprise**—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.
Low-cost and enterprisewide coverage—The cost of carrying out continuous risk can be lowered if self-assessment is performed against the joint control baseline. This reduces the number of redundant activities and man-hours of different assurance functions.

Comprehensive and consistent risk reporting—The coordination among assurance functions results in identification of risk factors that might have gone unnoticed. Also, evaluation of risk from different perspectives helps in assigning appropriate priority with respect to impact on business area or service.

Follow-up and control resolution convenience—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. It becomes easier even for the compliance department, as it will not have to follow up on controls separately.6, 7

CONCLUSION
The assurance functions in organizations should be closely associated with each function’s activities and risk findings, and mechanisms should be in place to keep abreast of these activities and risk findings. Based on overlapping activities, the functions should devise assessment strategies to work on potentially high-risk areas. Upon mutual consensus, it is critical to synchronize and align areas of engagement with the intent to strengthen the organization’s controls and improve risk posture.

ENDNOTES

Table 3—Sample Self-assessment

<table>
<thead>
<tr>
<th>Department Name</th>
<th>Finance</th>
<th>Category</th>
<th>Core Business Function</th>
<th>Risk %</th>
<th>28.54</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filled by:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basel II</td>
<td>ISO 27001 Controls</td>
<td>Control Status</td>
<td>Risk</td>
<td>Recommended Control</td>
<td>Target Date</td>
</tr>
<tr>
<td>External Fraud</td>
<td>Information security coordination</td>
<td>Does your department have an updated asset inventory in place?</td>
<td>NO</td>
<td>Coordinate with information security for formalization of asset inventory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality agreements</td>
<td>Does your department have a formal confidentiality/nondisclosure agreement with vendors, consultants associated with your business functions?</td>
<td>NO</td>
<td>Ensure that formal confidentiality/nondisclosure agreements with vendors are in place in case bank’s information is being shared.</td>
<td></td>
</tr>
</tbody>
</table>
Since Operation Aurora was publicly disclosed in early 2010, information security and, more specifically, cybersecurity (i.e., the protection of information assets against threats from cyberspace) have become top priorities in many organizations. Executive management generally understands the importance of the topic and follows accepted good practice by setting “the tone at the top.” A common problem is that in large organizations with multiple divisions, global operations and layers of management, tone frequently disperses and fails to move the organization toward a stronger cybersecurity stance. What is needed is information security leadership.

This article presents a framework that can help information security leaders build a sustainable information security program that avoids security gaps and blind spots. Specifically, the framework:

• Identifies the security dimensions that information security leaders must understand
• Presents five key decisions on which information security leaders should focus
• Explains three mistakes of which information security leaders should be aware
• Clarifies the concepts behind some terminology that is not always used consistently

The objective is not to define a detailed framework—volumes have been written on that—but rather to offer a pragmatic and actionable map that executive managers can use to shape their organizations’ information security in a more direct and tangible manner.

DIMENSIONS OF INFORMATION SECURITY

Information security is difficult to attain because it is a systemic property that requires vigilance along three dimensions (figure 1):

1. **Security controls are the mechanisms**—including procedures, structures, culture and policies—that organizations deploy to obtain reasonable assurance that threats are mitigated and regulatory requirements are addressed.

2. **Organizational structures** are the divisions, regions, management layers and processes that determine how organizations accomplish work.

3. **Technology** comes in different types (e.g., wireless, bring your own device [BYOD], cloud) from different vendors and different generations or versions.

Failure to properly manage any of these dimensions increases the risk of security incidents. If key security controls are missing, risk increases substantially. If security controls are not deployed systematically across the organization, critical information assets are left unprotected. If security controls fail to cover all critical technologies (e.g., wireless, BYOD, cloud, Wintel, mainframe), the information assets processed by these technologies are exposed and vulnerable. It is the job of information security leaders to prevent such gaps and to oversee the deployment of security controls across all technologies, divisions, regions, management layers and processes.

Figure 1 also shows that security controls follow from policies and standards. A policy is a...
high-level and generic statement regarding security principles and requirements. A standard refines and operationalizes policies by providing detailed performance and compliance criteria, possibly including specific activities and processes. Security controls implement standards by defining specific activities, defining individuals to perform the activities, and delineating when and how the activities should be performed.

Figure 1 further shows threats. Risk and threat are sometimes used interchangeably, but they are different concepts. A risk is an adverse event that is characterized by its probability and its impact. A threat is the potential for harm that can be inflicted either intentionally (e.g., by an adversary) or accidentally (e.g., random failures or acts of God). A threat is not much of a risk if the target system has appropriate controls and is not vulnerable to that threat. Similarly, threats that are unlikely or have a small impact give rise to minor risk. Laws and regulations are also included in Figure 1 as they can also be drivers for security controls (e.g., Payment Card Industry Data Security Standard [PCI DSS]).

SECURITY DECISIONS
As explained in the last section, the information security leader’s challenge is to make sure that the information security threats are understood, adequate mitigating controls are identified, and these controls are deployed consistently across the entire organization and all its technologies. Any gaps in this chain increase the likelihood of security incidents. To offer a more structured framework, the information security leader’s task can be described in terms of five security decisions:

1. **Identify and prioritize the relevant environmental factors.**
   This includes laws, regulations and threats. Many of these factors are generic (e.g., Sarbanes-Oxley Act compliance, activist hackers), but certain industries face unique laws, regulations and threats that must be understood because one cannot select security controls without first understanding what to defend against.

2. **Determine the key security controls.**
   Assess the threats in relation to the organization’s risk appetite; for high-risk threats, identify key security controls (i.e., controls that mitigate the largest possible number of threats and are enforceable and difficult to circumvent). To contain cost, it is important to keep the number of controls as small as possible. Controls that mitigate many threats are, therefore, preferable. Moreover, security controls must thwart intelligent adversaries and, consequently, must be enforceable and difficult to circumvent. Advice not to open attachments from untrusted sources is a weak security control by itself as people can be tricked and attackers can evade the control by luring users to web pages rather than offering email attachments.

3. **Decide on the amount of regional and divisional autonomy.**
   Most organizations use a combination of global
and regional/divisional policies, standards and security controls. The decisions about what to enforce globally and what autonomy to give to the regions and divisions are key governance decisions that information security leaders must make. As a general rule, the more essential a security control is, the more likely it is enforced organizationwide along with any associated standards and policies. Further considerations are the security and scale advantages that can be realized by centrally providing controls to an entire organization. For example, identity and access management as well as security operation centers benefit from such economies of scale.

4. Define the organization. Information security leaders must make sure that all security policies, standards and controls have owners. An owner is an individual who is accountable for the definition, implementation and continuous management of the policy, standard or control. Owners also have certain authorizations that must be defined. In particular, decision rights must be defined along with the limits of decision-making authority (e.g., when reviews or approvals are required). Assigning ownership is a delicate task as existing organizational structures, politics and power relationships must be considered. Further factors to consider include:
  – Whether to assign ownership to the business divisions or to IT
  – Within IT, whether to assign ownership to a support/staff function (e.g., IT risk) or to an operational function (e.g., security engineering or security operations)
  – Seniority of owners and their ability to “own” and advance a topic effectively
  – Organizational affinity; for example, assigning a security role to the chief financial officer (CFO) that may be at odds with his/her interests, skills and time availability
  – Separation of duty constraints
  – Completeness of coverage, i.e., when owners accept accountability for the entirety of their assigned scopes (e.g., enterprise-wide, a region, a division, a process, a technology or a combination thereof). Organizations are vulnerable to attacks when they have areas for which policies, standards or controls are not owned by anyone.

5. Set the budget. As a final decision, information security leaders must allocate budgets to maintain or improve information security.

While information security leaders will delegate much of the detailed work of these decisions to their teams, they must understand the bigger picture so that proper priorities are set, key tasks are not overlooked and details are not addressed precipitously.

MISTAKES TO AVOID
This section reviews three common mistakes about which information security leaders should be aware:

1. Overshooting—After larger incidents, some organizations overshoot and start working on best-in-class security controls that are designed to “make it go away once and for all.” While laudable, such an approach runs a high risk of introducing too much complexity and cost into the organization, which can ultimately lead to failure. Moreover, by shining the spotlight on best-in-class controls, such initiatives have a tendency to overlook foundational controls with better cost-benefit trade-offs. Organizations should, therefore, consider staged approaches in which security controls are rolled out incrementally and over time, based on actual risk, the costs and benefits of controls, and the organization’s ability to absorb change.

2. Fixing symptoms—Symptoms of weak security controls include, for example, unpatched applications, use of unauthorized software and outdated access rights. It is a good first step to remediate these deficiencies by applying patches, uninstalling unauthorized software and disabling unnecessary access rights. By itself, however, this step is insufficient, as it fails to prevent the same problems from reoccurring. To obtain a sustainable solution, security controls must be put in place to address the root causes. To continue these examples, a vulnerability management process, a software asset inventory and a systematic access right recertification process are needed to mitigate the root causes and improve security in a sustainable manner.
5. Spreading security too thinly—Auditors know that manual controls are error-prone. People are fallible, and when faced with intelligent adversaries, the likelihood of failure increases. Bruce Schneier reaches the same conclusion when he argues that security awareness training has a poor cost-benefit trade-off.11 Organizations that have many part-time security staff members or distribute security responsibilities too widely consequently run the risk of undermining their information security. Put differently, security controls generally work best when they are implemented by dedicated and skilled full-time staff or are automated using tools.

CONCLUSION

While information security leaders do not implement or run security programs, they do have to set the priorities and direction of these programs. To support information security leaders in this task, this article presents the key security dimensions and decisions that information security leaders should focus on and it describes common pitfalls to be avoided. Thus, the article supports the achievement of three important outcomes:

1. Security gaps are eliminated by driving the systematic deployment of key security controls across all divisions, regions, processes and technologies.

2. Information security is embedded into the organization, where it is engrained and made sustainable.

3. Return on security investment increases and costs are reduced by focusing security efforts on the key issues and priorities.

DISCLAIMER

The views and conclusions presented herein are those of the author and do not necessarily represent the views of any particular organization and/or company.

ENDNOTES


11. Schneier, Bruce; On Security Awareness Training, Crypto-Gramm, 19 March 2013
Doing Business in India Requires Digital Compliance

The Information Technology Act in India is an ever-evolving document, progressing on all fronts. Business must be in sync with it.

The proliferation of digital media in every aspect of business has been changing the way businesses run. The spread of networks and easy access to the Internet has brought a common denominator to the world. Companies have gone global with business partners and customers spread around the globe. This has resulted in newer compliance requirements and, consequently, legal implications in the case of shortcomings. Over the last decade, Asian countries have emerged as major contributors to globalized businesses. With one-third of the world’s population living in Asia, it also offers an opportunity to tap a bigger customer market.

Much has been said about the growth of India’s IT service sector—from 1.2 percent in 1998 to 8 percent of its gross domestic product (GDP) in 2012-13.\(^1\) Outsourcing to Indian companies has been popular for several years. In addition to outsourcing, many firms have set up their own shops in India for back-office services, development, health care and engineering, among others. Furthermore, many enterprises have joint ventures and subsidiaries doing business in India.

It is important to know that India has been progressing on the cyberfront in many ways. E-commerce has been provided legal recognition. The governments—central and state—have offered e-filing facilities for businesses and individuals. Copyrights, patents and trademarks have been officially supported through international cooperation. All of this has become possible because of the legal framework of India’s Information Technology Act 2000 and other allied Acts.

This article addresses the vital components of this structure and brings forth the compliance requirements.

**THE LEGAL FRAMEWORK AND ITS AIM**

ITA-2000 seeks to:

- Provide legal recognition for electronic records and digital/electronic signatures, thus facilitating e-commerce
- Facilitate e-governance and encourage the use and acceptance of filing of electronic records with government agencies
- Identify cybercrime and provide penalties

ITA-2000 covers e-commerce, e-governance, e-records, digital signatures and electronic signatures. In keeping with this, the following Acts were amended:

- Indian Evidence Act
- Bankers Books Evidence Act
- India Contract Act

With electronic records granted legal recognition, the Indian Government has also amended the Indian Penal Code, thus bringing the offences against electronic records within the purview of ITA-2000. Further, considering the significance of digital assets, those are now covered under the following acts (amended):

- The Copyright Act 1957
- The Patents Act 1970
- The Design Act 2000
- The Trade and Merchandise Marks Act 1958

**SCOPE OF ITA-2000—ITS JURISDICTION**
ITA-2000 is applicable to the whole of India, i.e., all states and union territories. All acts committed using computer resources in India are covered by this Act. The term “computer resource” includes, for example, all computers,
cell phones, mobile devices, databases and networks. Any action committed by a person located outside the geographical boundaries of India also falls under the jurisdiction of this Act if the action involves a computer resource located in India, per section 75 of the Act. However, one may argue that extension of jurisdiction beyond Indian geographical boundaries poses additional challenges.

THE LEGAL FRAMEWORK—SALIENT FEATURES
In India, three sections of society are involved in the enactment of cyberlaws: the legislators, the judiciary and the government. The primary cyberlaw in India is the legal framework provided by ITA-2000 and allied amended laws. The legislations award necessary powers to the judiciary to rule on various matters as required. The Indian legal system also follows precedents established by prior decisions—the principle of stare decisis. The decisions of higher courts are binding on the lower courts. Rulings of peer courts and lower courts also carry persuasive value though they are not binding. This implies that any precedent may be cited while arguing the case.

Following the legislature and the judiciary, the central and the state governments are required to ensure that the laws are enforced as required. Four major steps are required for a statute to come into force in India. First, the government has to prepare a draft bill and present it to Parliament. The bill is discussed and, if accepted, is passed in both houses of Parliament. The passed bill is sent to the president of India for approval. On receiving the assent, the government provides notification in the official gazette of India. The Act comes into force on the date of notification. As an example, a cyberoffense committed prior to 17 October 2000 (the date on which ITA-2000 was notified) cannot be tried in the court of law under ITA-2000.

E-COMMERCE
ITA-2000 provides protection to electronic transactions by legalizing the digital and electronic signatures. IT introduced digital signatures and the necessary provisions for certifying authorities. While digital signatures were the first step toward promoting e-commerce, it was not enough to get the common consumer on the Internet. The electronic signature recognized in the amended Act in 2008 was instrumental in allowing customers to perform electronic transactions on the Internet. The e-payment facility is the central aspect of e-commerce. Entities intending to provide a payment system in India need to obtain authorization from the Reserve Bank of India (the central bank) under the Payment and Settlement Systems Act 2007. The Reserve Bank publishes a list of authorized prepaid payment instruments on its website. In the same vein, the Reserve Bank has also approved four card payment networks as of April 2013.

INTELLECTUAL PROPERTY
The Copyright Act 1957 has been amended from time to time—the latest being the International Copyright Order 1999 and the Copyright (Amendment) Act 2012, effective 21 June 2012. The Copyright Act 1957, section 40, protects the rights of member countries of the Berne Convention, Universal Copyright Convention, World Trade Organization and Phonograms Convention. In effect, a program developed in any of the treaty countries becomes copyrighted material in India. Computer software registered as a “literary work” under section 2 enjoys protection under the Copyright Act in India. Similar to the Copyright Act, the Trade and Merchandise Marks Act, the Patents Act, the Geographical Indications of Goods Act, the Designs Act and the Semiconductor Integrated Circuits Layout-Design Act are in force to protect intellectual property rights.

LEGAL REMEDY
The complainant may seek remedy through civil or criminal courts. The secretary of information technology of the state is the adjudicating officer to hear cases relating to chapter 9 (ITA-2000) contraventions. The secretary carries powers equal to those vested in a civil court. In the event of an unsatisfactory outcome, the complainant or defendant may appeal to the Cyber Appellate Tribunal. Further recourse is available to both parties: to approach the High Court. For more serious offenses under chapter 11 of ITA-2000, the complainant may approach the cybercrime cell of the local police. The cybercrime cell carries out necessary investigations and then the trial is held in the relevant criminal court. The parties may appeal to a higher court in case of an unacceptable outcome.

HIERARCHY OF COURTS IN INDIA
The Supreme Court is the highest court of law in India. The courts have varying powers to grant sentences. The Judicial Second Class Magistrate can sentence up to one-year jail terms for criminal offenses. Going up the hierarchy are the
Metropolitan Magistrate/Judicial First Class Magistrate, Chief Judicial Magistrate/Chief Metropolitan Magistrate, Assistant Sessions Court and Sessions Court/District Court/Additional Sessions. The next two levels are High Court and then Supreme Court. For civil cases falling under chapter 9 (ITA-2000), the adjudicating officer is the first level. The Cyber Appellate Tribunal is the next level, followed by High Court and then Supreme Court. Depending on the size of the claim and the offense committed, one has to approach the appropriate court.

In 2012, Google and Facebook faced criminal trial in Patiala House Court (District Court in Delhi) for allegedly hosting objectionable material on their sites. While the case was still in progress, both respondents petitioned the High Court to terminate the criminal proceedings against them. The Delhi High Court exempted heads of both companies from appearing at the trial; however, it did not stay the trial in the lower court.

COMPLIANCE REQUIREMENTS
It is imperative that companies doing business in India, by themselves or through their partners, meet certain compliance requirements. Closer attention is required if the business involves collecting customer information. Such information may be personal and sensitive in nature, which if disclosed, misused, modified or lost, may carry severe legal repercussions—even for the parent company located outside India. Data protection is clearly described in sections 43, 43A, 66 and 72 of ITA-2000. Furthermore, the government of India may ask for cooperation of a company or individual in accessing information when required. The company and its officials are obliged to provide all possible cooperation if asked. The government and its agencies have powers to block/intercept data or order the company to remove contents from hosted sites. The company must make necessary provisions to meet all such demands.

The employees and the directors of the company are liable for punishment in case of wrongdoing. The complaints, notices and other communication received from customers, employees, partners or the general public offer clues of such wrongdoing; they need to be addressed. Section 85 of ITA-2000 states that in case of failure to protect sensitive information, all persons responsible to the company for conduct of its business shall be held guilty, barring certain exceptions. Section 43A in the amended ITA-2000 spells out the responsibility of corporate bodies handling sensitive personal information in a computer resource. The corporate bodies have an obligation to ensure adoption of reasonable security practices.

A process for prompt investigation and resolution is required. Furthermore, there should be a well-maintained record of such issues and their resolution. It is vital to put in place a robust security policy, safety practices and precautions. The privacy code needs to be published and made known to all concerned. A regular audit and review can help to bring out issues to be addressed and corrective measures to be put in place.

REASONABLE SECURITY PRACTICES
Section 43A of ITA-2000 brings in corporate responsibility of data protection. Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules 2011 specifies the compliance expected of a corporate body.

A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.

The Rules 2011 also makes a mention of ISO/IEC 27001 as one such standard. In case of breach, the body corporate and all personnel concerned with data protection are considered liable under ITA-2000. For banks, the Reserve Bank of India has published its guidelines for reasonable security practices. The banks are required to adopt practices matching these guidelines and submit regular compliance reports to the Reserve Bank of India.

ITA-2000 does not specifically mention the hardware/software required. Exception has been given for the certifying authorities for whom certain standards have been prescribed. Similarly, the banks may get certain guidelines from the...
Reserve Bank of India, specifying certain standards. It is quite clear that no mandate is issued in terms of hardware or software. Electronic transactions are expected to be confidential. ITA-2000 does not specify any reporting on transactions. It only expects that the corporate body maintains adequate security and confidentiality.

All entities that handle personal/sensitive information and/or collect and/or process such information need to comply with the requirements of ITA-2000. Examples of businesses with entities that may engage encompass e-commerce, business process outsourcing (BPO), banking and financial services, and social media. Under section 79, the intermediaries, such as network service providers, are not liable for the third-party information if they provide only access to such information. However, the intermediaries are held liable under ITA-2000 in the case of having received notice of unlawful content and having failed to remove or disable access of such content. Examples of such businesses include network providers, hosting services, marketplace providers and social media. It is imperative that all of these businesses set up appropriate processes to meet the legal requirements. Besides, it is essential to have the governance structure in place to ensure that intended practices are followed in reality. Figure 1 shows three aspects of compliance: processes, documentation and governance. Adequate documentation provides evidence that underlying processes are followed, while governance provides for monitoring, controlling and updating features of compliance.

To summarize, digital compliance in an organization can be deployed through:

1. **Processes**—These are used to:
   - Understand the compliance requirements and to gather information from sources such as cyberlaw consultants, legal databases, published reports and newspaper clippings
   - Document and publish expected actions and processes
   - Execute the setup processes

2. **Documentation**—The actions and their outcomes need to be documented (digital documentation is acceptable).

3. **Governance**—It is vital that the organization has a formal structure to monitor the process execution and regular update. As part of such a structure, one would expect to have a cell to coordinate activities and report noncompliance, if any, to the governing body.

**EXAMPLES OF VIOLATIONS AND CONTRAVENTIONS**

The legal framework and expected compliance discussed in the previous sections can be seen in light of the cases filed in the courts of law. Depending on the severity of crime, the trials are held in different courts. Examples of such court cases presented here underscore the digital compliance requirements.

**Penalties**

ITA-2000 stipulates varying penalties or punishments, depending on the offense committed. For criminal offenses (chapter 11), such as publishing/transmitting offensive material, cyberterrorism, violating directions of Indian Computer Emergency Response Team (ICERT) or accessing a protected system, the punishment may range from two years imprisonment to life imprisonment in addition to fines. For access-related crimes involving, for example, unauthorized access, copying, damage to computers or fraud (chapter 9), compensation is awarded to the aggrieved party.

Chapter 9 (ITA-2000) contraventions mainly cover crimes related to unauthorized access, pornography, damage and fraud. Chapter 11 offenses deal with, for example, hacking, privacy or cyberterrorism. Even the rights of a nonresident are protected under Indian Law. This can be exemplified by the case of Shri Umashankar Sivasubramaniam vs. ICICI Bank.3 The case shows responsibility of the corporate body toward expected due diligence for the safety of data and customer

---

**Figure 1—Compliance Requirements**

Because ITA-2000 is a living act, compliance needs to be perpetually attended. Processes need to be updated and followed.
Role of Intermediaries
The role of intermediaries is examined by the court in the complaint filed by Vinay Raj against 21 companies in Delhi in 2011. The arguments were about the contents on the web sites and whether the intermediaries were responsible for defamatory contents. Facebook and Google were among the defending companies.

In the case of Google India Pvt. Ltd. vs. M/S Visaka Industries Limited in Andhra, Pradesh High Court issued its ruling on 19 April 2011. Google petitioned that, being a platform provider, it was not responsible for any content hosted on its servers. The court observed that Google failed to remove the defamatory contents when the respondent brought those to the notice of Google. The court dismissed Google’s petition saying that Google cannot claim any exemption under section 79 of ITA-2000.

Personal Liability—Employees, Directors, Partners
In the Bazee.com case, the organization’s Indian-born, American-citizen chief executive officer was arrested by authorities for objectionable material on the site. Bazee.com was acquired by eBay. The arrest was carried out under section 67 of ITA-2000 for transmission of obscene material. Although he was later released on bail, the case demonstrates the expected responsibility of persons running the company.

Intellectual Property
As an example of legal protection in India, one may cite the cases that Microsoft has won in Indian courts for infringement of copyright. In these cases, the courts granted relief to complainant Microsoft Corp. and ordered injunction restraining further infringement.

Recently Telefonaktiebolaget Lm Ericsson filed a case in the Delhi High Court against Micromax Informatics Ltd. for patent infringement, claiming damages of Rs 100 crore (INR 1 billion or US $18.52 million). Micromax is an Indian manufacturer of mobile handsets and tablets. The court passed an interim order in favor of Ericsson. Micromax was ordered to deposit with the court 1.25 to 2.5 percent of the sale value. In addition, Ericsson officials were authorized to inspect Micromax consignments at customs. If Ericsson gets its way, it may take legal action against more companies.

ROLE OF IT AUDITOR
In the changing environment of businesses in the cyberworld, IT auditors must widen their perspective and get to know the legal provisions of ITA-2000. It is not the aim of this article to consider whether the auditor should play the consultant role or conventional audit role. However, it is clear that auditors must be much more vigilant about the legal aspects of cyberspace in India. They must understand and describe the strengths and weaknesses of the organization with respect to ITA-2000.

Cybercrimes have evolved rapidly, but the legislations also try to curb such acts through newer enactments of rules, guidelines and notifications. In this environment, it is insufficient to provide a traditional checklist for the audit function. The following is suggested:

1. Know the business; get to understand the business involvement in the cyberworld, including:
   • Products/services sold on the Internet
   • Sensitive/personal data collected or processed through computers
   • Remote services provided over the Internet
   • Connections offered as intermediaries
2. Find the relevant processes practiced in the organization.
3. Get to know the current status of ITA-2000 and the guidelines/mandates from any related agency such as the Reserve Bank of India.
4. Check the documentary evidence on processes and governance.
5. Report shortcomings and strengths to the relevant authority in the organization.

Figure 2 provides examples of businesses and related information that an IT auditor must possess.

<table>
<thead>
<tr>
<th>Business Examples</th>
<th>Relevant Notifications/Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet banking</td>
<td>The Reserve Bank of India guidelines issued in 2011 on IT governance, information security, IS audit, IT operations, IT services outsourcing, cyberfraud, business continuity planning and customer awareness programs</td>
</tr>
<tr>
<td>Cybercafé</td>
<td>Information Technology (Guidelines for Cybercafé) Rules 2011</td>
</tr>
<tr>
<td>Hosting services</td>
<td>Intermediary rules</td>
</tr>
<tr>
<td>Distribution/sale of software</td>
<td>The Copyright Act</td>
</tr>
</tbody>
</table>
CONCLUSION
It is of utmost importance that IT auditors keep their eyes and ears open to happenings around the world. The Reserve Bank of India regularly issues guidelines to banks, e.g., for Payment Card Industry Data Security Standard (PCI DSS) compliance to protect cardholder data. These may be important to get a feel of expectations, even if the company does not deal in the financial sector. The government of India and the state governments also issue orders and notifications from time to time. An internal cell may be organized to gather and understand the requirements that may originate from such communiqué. The IT auditor and the company doing business in India need to be abreast of the legal aspects and the adequacy of internal processes.

ENDNOTES
2 Reserve Bank of India, circulars, www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx
3 Shri Umashankar Sivasubramaniam vs. ICICI Bank petition no. 2462, judgment delivered on 12 April 2010
4 Vinay Raj vs. accused, complaint no. 156 of 2011 in the court of Sudesh Kumar, Metropolitan Magistrate Patiala House Courts, New Delhi, 2011
5 Google India Pvt. Ltd., vs. M/S.Visaka Industries Limited, on 19 April, 2011, Crl.P.No. 7207 of 2009
6 Microsoft Corporation vs. Mr. Yogesh Papat and Anr, 22 February 2005
7 Delhi High Court, Microsoft Corporation vs. Mr. Kiran and Anr, 7 September 2007
Revisiting the Human Factor in Organizational Information Security Management

The human factor is a well-recognized issue in organizational information security management; however, there is a tendency to equate the human factor with insider threat of end users. It is critical to take a holistic view, examining the roles of three groups of people: end users, information security professionals and top executives. Each group plays an important role in organizational information security management. Top executives should take the leadership role in envisioning an optimal security strategy, security professionals should be able to execute the security strategy and end users must participate in security management processes. All three groups are accountable for information security.

Employees play an important role in organizational information security management. How they use IT to perform daily business activities has an impact—negative or positive—on the overall security of the organization’s information systems. The role of employees is often referred to as the human factor in information security management; however, the definition of human factor in academia and practice is “end users.” End users are often referred to as insider threats to organizational information security. To address this type of insider threat, organizations are urged by scholars and practitioners to implement and enforce security policies that aim to deter end users’ undesirable behaviors. The deterrent effect of security policies has recently been examined in many studies that generally focus on those factors that may lead to end users’ violation of or compliance with security policies. An underlying assumption is that violation of organizational policies causes damage to security and must be prevented.

There has been less discussion, however, on the behavior of information security professionals—probably because they are the ones who manage security in organizations. They are supposed to be aware of the importance of security and the importance of proper use of IT. Thus, the role of information security professionals appears to be implied by their job descriptions: They are security protectors and should behave better than end users in terms of using IT. The role of top executives is often narrowly referred to as “top management support” in information security literature.

There appears to be an assumption that:
- Information security professionals are security guards—the good people
- End users are security violators—the bad people
- Top executives support information security professionals to implement and enforce security policies to prevent undesirable behaviors by end users

Based on such a narrow assumption, security problems are largely, and maybe unfairly, attributed to end users rather than information security professionals and top executives. Perhaps more important, the unbalanced focus on one group of people, i.e., end users, may hinder the theoretical and practical advancement of the information security field. To some extent, the end-user-focused assumption gives organizations the wrong impression that security problems will not exist if end users are contained. The tendency to treat end users as the enemy leads to a lack of user-centered design in security mechanisms that may look secure on paper but will fail in practice. The police-violator focus may also widen the so-called digital divide between information security professionals and end users and result in questionable management strategies. These issues call for a balanced examination of the human factor in information security management.

**THE ROLES OF EMPLOYEES**

The human factor is not limited to end users. Information security professionals who implement and manage security measures, end users who use IT solutions to carry out their...
business tasks, and top executives who make decisions about security strategy play an important role (figure 1). Top executives must take a leadership role in defining an optimal security strategy for the organization, information security professionals are in charge of the execution of the strategy and end users should participate in security management processes. Each of the three groups also requires different skills and knowledge.

**Information Security Professionals**

Information security professionals initiate, implement and monitor security measures. Undoubtedly, they are the foundation of any organization’s information security strategy. As such, their role is focused on security execution. To execute the organization’s security strategy, information security professionals must have the necessary skills and knowledge in technical and business areas. Thus, the most important trait that information security professionals should have is security competence.

One of the key factors in information security is technology; information security professionals must have sufficient technical skills. They need to know specific technologies and, more important, how to put different technologies together to make information secure. It is equally important, however, that information security professionals have solid business skills and knowledge. Such business skills and knowledge are vital for them to effectively manage information security. To convince top executives to invest in security, security professionals need to use a language that top executives understand. In this regard, information security professionals should have sufficient communication skills. Another aspect of business skills is the understanding of business. Information security professionals should understand business problems and needs and must be able to link security and IT with business objectives.

In terms of the relationship between IT and business, IT should play a supporting role in organizational business activities, i.e., help achieve business objectives. This suggests that information security professionals should be business-oriented rather than close-mindedly security-oriented. More specifically, this supporting role can be reflected in the following two aspects: IT as business facilitator and IT projects as business projects.

From a means-end perspective, business is the end, while information systems are just one of the means. Security should protect business from risk. The hindrance caused by security measures should be kept at a minimal level. This principle should guide what and how security measures should be implemented. Unless end users and top executives see the value of IT measures for achieving their business goals, they are less likely to wholeheartedly embrace the measures.

Given the supporting role in organizations, IT projects do not stand alone. Instead, they should be an integral part of business projects and should be led by business managers rather than IT managers. The job of security managers is to make business managers understand risk and how risk can be mitigated.

**End Users**

End users rely on information systems to carry out their business tasks. An important factor that may influence the effectiveness of security measures is end-user awareness. Due to their limited security knowledge and skills, end users may have a false sense of security and, thus, may engage in some security-threatening behaviors, such as downloading and installing unknown software from the Internet. End users may not know how to use certain technology, the value of the data they handle and/or the possible consequences of their use of IT, for example. End users may also ignore security measures because those
measures often require various degrees of changes to their
day-to-day business tasks. As a result, their interactions
with systems may inadvertently cause damage to
information security.

To deal with problems caused by end users, organizations
often take an authoritative approach by implementing and
enforcing security policies. The logic behind security policies
is that sanctions can help prevent end users from engaging
in those undesirable behaviors that may damage security.
However, many studies in information security literature have
found that sanctions may not work as expected.5,6 End users’
focus on business tasks is one of the key reasons why they fail
to follow security policies.7,8 Most do not have any malicious
intent to cause damage; thus, treating end users as the enemy
of information security may not be an effective strategy.9

What role should end users play?

Instead of the passive role of security rule followers,
end users can play a more active role in participating in
organizational information security management. End users
are not the enemy within, but are the partner of information
security professionals in protecting an organization’s information.10 End users can be
an important resource
that contributes to effective
security measures.11,12
End-user participation in the
design and implementation
of security measures can
ensure that measures are situated in the business processes
for which the end users are responsible. As a result, the best
fit between security measures and business processes can be
accomplished. Any measures that can secure organizational
information without interfering with end users’ business tasks
can better win their acceptance.

To participate in security management, end users must
understand the security implications of their actions in
dealing with organizational information and, perhaps more
important, the impact of security problems on their business
tasks. Thus, awareness is an important factor that influences
how end users participate and whether they fully embrace
those security measures implemented by information security
personnel. It is generally accepted that end users must receive
sufficient training and education in information security. It
remains a challenge, however, as to what exactly end users
should know in terms of security.

**Top Executives**

Top executives of an organization make decisions on the
overall IT strategy and the amount of resources that the
organization invests in IT. Their decisions ultimately influence
how secure the organization’s information systems are. What
priority executives give IT in general and security in particular
likely determine the resources allocated to this area.

One problematic trend is that the role of top executives
is often reduced to a supporting part, sometimes termed
“top management support.” By playing a supporting role,
top executives turn security management into an IT problem
rather than a business problem. The drawback of this
approach is that top executives are taking a passive, reactive
approach to security issues—trying to do something only after
security breaches occur. Another problem is that information
security professionals often lack the ultimate authority to push
security measures across functional boundaries.

Thus, instead of merely supporting, top executives must
lead security management. Strong leadership helps foster a
proactive approach to information security that emphasizes
proactive prevention rather than reactive correction after
security problems occur. It also helps facilitate dialog among
information security professionals and end users and, as
a result, ensures that security measures are effective and
supportive of business needs. As discussed earlier, higher
levels of acceptance by end users can be expected if security
measures fit end-user needs for carrying out business tasks.

To truly lead security management, top executives must
understand the impact of security issues on business. Top
executive awareness is an important factor in security
management. As mentioned earlier, end users’ awareness is also
an important factor that influences how they deal with security
measures. Due to the differences of their job scopes, there is an
important difference between the awareness of these two groups
of people. For top executives, the focus is business risk—how
security issues impact overall business strategy. For end users,
on the other hand, the focus is on the risk related to processes
and tasks—how security issues impact their daily work and how
their behavior impacts security.

**INTERGROUP RELATIONSHIPS**

While each group of employees (information security
professionals, end users and top executives) plays an
important role, how they interact with each other also has an
impact on organizational information security management.
They should not act in an isolated manner.

---

**End users are not the enemy within, but are the partner of information security professionals.**
Information Security Professionals and End Users

To ensure that end users take a participative role in managing information security, information security professionals must engage and encourage them to do so. This requires information security professionals to treat end users as partners— not as the enemy within—in the endeavor to secure an organization’s systems. Such partnerships have two important implications.

First, information security professionals need to make a shift from passive responses to proactive engagement. Traditionally, the IT department (including information security professionals) of an enterprise is organized as a silo. Physically, IT staffs are located in a self-enclosed environment that makes interaction with end users difficult; functionally, the IT department often acts as an external vendor charging out services provided to end users and a help desk is often the only interaction point between IT professionals and end users. The key problem with the help-desk approach is that it is passive; information security professionals are waiting for end users to ask for help. This is particularly problematic in terms of security. End users may not be able to identify security issues due to their non-IT background and low awareness.

Second, information security professionals need to make an effort to understand the end users’ point of view and get feedback from them. This includes an understanding of how security measures impact their business tasks and what measures can best meet the requirements of business and security objectives. From a value-focused thinking perspective, this requires information security professionals to examine the values of end users—the fundamental objectives for information security and business performance and the means to achieve them. It is important to identify and reconcile areas of conflict between security procedures and legitimate professional work values.

Information Security Professionals and Top Executives

While top executives must truly lead any security endeavor, information security professionals are not merely followers. Information security professionals, who are in charge of the implementation of security strategy, must be able to give top executives proper advice on security matters, and they must be able to convince top executives to pay more attention to and make sufficient investment in security. To do that, information security professionals must see a big picture beyond security by situating security in the bigger context of the business strategy and building the link between security and business.

As discussed earlier, information security professionals need to have technical skills as well as business skills and orientation to foster the advisor-leader relationship with top executives. Perhaps more important, information security professionals need to have good communication skills to discuss security issues in a nontechnical manner. They must be able to answer the “so what?” questions in terms of the impact of security issues on business. In addition, information security professionals must proactively engage in dialog with top executives rather than passively wait for questions to come.

End Users and Top Executives

In addition to providing leadership in terms of overall security management, top executives play an important role in influencing end users’ dealings with security. First, top executives must lead by example in terms of complying with security policies and rules; their actions and attitudes have an impact on the end users’ attitudes toward security and ultimately how end users use technology and deal with security issues.

Second, top executives are in a better position to motivate end users to follow security policies and rules and participate in security management. When faced with a conflict between business tasks and information security, end users are likely to sacrifice security for their tasks on hand. It would be up to top executives to balance business performance requirements and security mandates. A balanced performance evaluation on business tasks and security matters helps motivate end users to be mindful of security issues when they use technology.

Conclusion

Human factors are well-recognized issues in organizational security management; however, there is a tendency to equate the human factor with end users who are typically referred to as insider threats. The risk of such a narrow definition is that the roles of information security professionals and top executives, which are no less critical than end users, may be inadvertently neglected.

Each of the three groups plays an important role in information security management. Top executives should take the leadership role, information security professionals should
be able to execute security strategies and end users must participate in security management processes. An organization can be resilient in preventing, detecting and recovering from security problems only if all three groups take their share of responsibility. Each group is accountable for security in different capacities.

ENDNOTES
1 Adams, A.; M. A. Sasse; “Users Are Not the Enemy,” *Communications of the ACM*, vol. 42, 1999, p. 41-46
3 *Op cit*, Adams
9 *Op cit*, Adams
13 *Op cit*, Adams
A Sustainable and Efficient Way to Meet Clients’ Growing Security Expectations

Achieving Holistic Security Compliance With NIST SP 800-53

Regulatory compliance continues to grow and is here to stay. As big corporations come to terms with the new realities of compliance, their response to noncompliant vendors will be ruthless. Enterprises that want or have big corporations as clients must include compliance as an integral part of their business model. The challenge is to integrate it without losing their agile service and cost-effective structure.

NIST SP 800-53,¹ an information security model developed by the US National Institute of Standards and Technology (NIST), can be a useful guide for service providers to build their security posture.

Security breaches, and the fundamental flaws they bring to light, are becoming more numerous and more complicated with each passing year. Each technological advancement brings new security vulnerabilities in its wake, and many, after following a tortuous path, end with a regulatory requirement in one form or another. While interpreting, assessing and complying with these regulatory requirements are huge hurdles for big organizations, they present an especially daunting challenge for the small and medium-sized firms that find themselves increasingly in the path of regulatory maelstroms with the potential to bring their business to a halt.

The Internet empowered entrepreneurs in ways unthinkable a mere decade ago. An innovator could, while sitting in Utah with three part-time employees (if that many), create a unique service that big corporations would beat a path to his/her (virtual) door to use. The giant companies see opportunities to leverage the tools created by these tech entrepreneurs to enrich their offerings to their customers. Today, the big banks (or manufacturers, retailers and others) use hundreds, if not thousands, of such small companies to keep their supply chain lubricated. Often, these services are white-labeled, meaning they are offered in the big corporation's name. A logistics company uses a web service that automatically overlays delivery addresses on a map for each of its 11,000 drivers, for example. Or, a bank uses a web service that connects securely and confidentially to millions of businesses with which the bank's customers want to transact. Or, a doctor's office uses a web service that tracks all of its insurance payments in process and sends an alert when there is a problem.

Different innovators and different solutions that have two common threads:
1. These disruptive technology solutions are light on footprint and heavy on innovation and value-addition.
2. They are very inexpensive. For example, the logistics company may pay pennies per truck per day, saving more than 60 minutes of the driver's time each day.

THE PROBLEM

Everything seems to be working well and everybody seems to be happy. The problem, however, is that third-party vendors receive, transmit, store and/or process—on the big corporation's (i.e., client's) behalf—information that is subject to many different regulatory controls, and the corporation is required to prove that such data are secure across the entire supply chain and not just inside its corporate walls. Based on the vendor's role in the corporation's supply chain, the vendor may be low, medium or high on the risk scale of the organization, and its compliance machinery starts cranking accordingly. A questionnaire with 200 to 400 questions or controls is sent to the vendor every one or two years, and the questions/controls are at a level of detail that the vendor has never thought of, let alone designed to, while developing the product or service.

The firm's owners instinctively know that to support these requirements, they will have to build a large organization (that they do not need otherwise) and the key value proposition, “pennies per day per truck,” will evaporate.
As the cost of compliance and noncompliance (i.e., penalties) mounts—from millions to hundreds of millions to even billions—big corporations are turning to their vendors to wring out that extra penny in savings. The message is: “We want more for less.”

These two factors, growing compliance mandates and growing cost of compliance, are the new normal for business, and demonstrated compliance is an integral feature of the business model for every organization—big or small—that wishes to conduct business in this environment.

THE CHALLENGE WITH COMPLIANCE

Most auditors understand the complexities of IT security and are able to appreciate how good the organization is and how secure the service is. But the vendor also needs to realize that the auditor has a different frame of reference. The auditor needs the vendor to demonstrate that it is compliant. This is often a tricky concept: How does an organization demonstrate its compliance? The following are examples of how to achieve this:

1. Demonstrate an understanding of the data the organization handles and the legal implications of their misuse.
2. Demonstrate a security culture with a high degree of consciousness among employees.
3. Demonstrate a set of policies and procedures aimed at ensuring security.
4. Demonstrate the compensating controls that mitigate gaps in controls.
5. Demonstrate a security vision and a road map to achieve continuous improvement.
6. Demonstrate adoption of security best practices in the organization.
7. Demonstrate how the organization identifies, tracks and acts upon risk incidents.
8. Demonstrate how the organization is engaged in the broader security community and dialog.

Large organizations build risk and compliance groups (sometimes thousands of people strong) to address these. Small and medium-sized organizations cannot afford this. Fortunately, there are many best practices and standards available worldwide that an organization can adopt to improve its security posture. An organization can achieve a quantum improvement in its security and demonstrate the same while keeping the cost within an appropriate range for small firms.

One such standard comes from NIST, a body under the US Department of Commerce. NIST is tasked with creating a technology security controls framework that all US government organizations can use to meet their security obligations. NIST has done pioneering work in this field and provides a conceptual framework that any organization can study, adopt and practice to achieve significant improvements in its security posture. NIST SP 800-53 provides a set of security controls for federal systems and NIST encourages private commercial enterprises to use it as well.

THE NIST SP 800-53 SECURITY CONTROLS FRAMEWORK

This framework defines more than 200 individual controls spread over 18 control families (figure 1) that take care of the baseline information security requirements of an organization—large or small, private or public. It acknowledges that not every organization is large and complex enough to warrant all 200-plus controls, and that it may be beyond the technological and financial means of a small organization to simultaneously implement all of the controls.

Hence, it classifies controls into three security baselines: low, moderate and high. This allows an organization to determine what security classification best fits it based on its size, complexity, supply chain, sensitivity of information handled, third-party obligations and regulatory expectations.
For example, the Access Control, one of the NIST SP 800-53 families, statement is:

The organization develops, disseminates and reviews/updates on a quarterly basis:

1. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and regulatory compliance; and
2. Formal, documented access control procedures to facilitate the implementation of the access control policy and associated access controls.

![Table](image)

These few lines, when implemented properly, can change the way an organization faces various examinations and what its clients and auditors understand about the organization. To a security professional evaluating the organization, this means that:

- The organization has thought about its access-control-related goals, challenges and risk, and has proactively articulated a policy in formal terms (not implicit in or implied by actions)
- The organization has a policy statement that defines:
  - The purpose behind developing such a policy
  - The scope, such as units, locations, levels of people and third parties
- Every actor involved in the life cycle of the policy and their responsibilities
- Management’s commitment to putting its authority behind the policy, empowering people to monitor compliance and authorizing punitive actions
- Procedures are in place to explain how to comply with this policy under different operational scenarios in the organization, e.g., how access control is enforced under the UNIX environment, under the Windows environment, and under web and cloud environments.
- Depending on the layers and complexity of the environment, it may create or refer to other documents such as runbooks, workflows or guidelines, in addition to the procedures documents, to make sure that the entire process is captured, documented and published for all stakeholders to understand and satisfy

An access control policy, developed as part of a comprehensive framework, puts the policy in organizational context and helps the organization be compliant and demonstrate compliance to auditors and examiners or other interested parties.

### IMPLEMENTATION ROAD MAP

While a framework such as NIST SP 800-53 empowers an organization to look at the total security picture, it does not warrant that the whole framework is implemented in a big bang, single-shot fashion. The organization marks the controls that seem most urgent, relevant and directly connected to what the auditors want to see. This affords the organization the ability to flexibly draw up an implementation road map for 18 to 36 months, for example, and embark on a preplanned journey. This is invaluable for knowing the total scope, stakeholders and approximate investments up front, so management knows what the organization is embarking upon without having to deal with surprises at every turn. Figure 2 illustrates an example of a NIST SP 800-53 high-level implementation road map.

### CONCLUSION

The primary targets of NIST SP 800-53—the federal departments required to comply with the Federal Information Security Management Act (FISMA) information security regulations—have realized enormous gains. Furthermore, NIST SP 800-53 has been taken deeper and wider over the years to help higher-risk organizations such as utilities and defense.
Adopting such a standard not only gives a ready-made frame of reference for the organization to plan its security journey, but provides a proven, recognized prism through which the external world (comprising the organization’s clients, examiners, auditors, suppliers and other supply chain partners) can look at the organization. Small and medium-sized firms can, thus, find a balance between raising their security profile to meet client expectations and not lose their fundamental value proposition.

Organizations can get a grip on information security using NIST SP 800-53 and then leverage other specialist frameworks to improve the quality of the software development process, service delivery and other areas of work. COBIT® may be used to provide the overarching guidance necessary to bring all initiatives together in a holistic and synchronized manner.

### Figure 2—High-level NIST SP 800-53 Implementation Road Map

<table>
<thead>
<tr>
<th>ID</th>
<th>Family</th>
<th>Priority</th>
<th>Start</th>
<th>Complete</th>
<th>Owner</th>
<th>Budget*</th>
<th>Tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Control</td>
<td>1</td>
<td>Feb-13</td>
<td>Jul-13</td>
<td>CTO</td>
<td>400</td>
<td>AD, MAC</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training</td>
<td>1</td>
<td>Apr-13</td>
<td>Jun-13</td>
<td>HR</td>
<td>40</td>
<td>LMS</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability</td>
<td>3</td>
<td>Oct-14</td>
<td>Feb-15</td>
<td>External</td>
<td>TBD</td>
<td>N/A</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
<td>2</td>
<td>Aug-13</td>
<td>Dec-13</td>
<td>CTO</td>
<td>TBD</td>
<td>HPCM</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
<td>1</td>
<td>Mar-13</td>
<td>Dec-13</td>
<td>Ops Lead</td>
<td>250</td>
<td>TBD</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication</td>
<td>2</td>
<td>Oct-13</td>
<td>Dec-13</td>
<td>CTO</td>
<td>TBD</td>
<td>Bio Met</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
<td>3</td>
<td>Jun-14</td>
<td>Dec-14</td>
<td>Ops Lead</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
<td>2</td>
<td>Jan-14</td>
<td>Mar-14</td>
<td>Ops Lead</td>
<td>80</td>
<td>HPALM</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection</td>
<td>1</td>
<td>Feb-13</td>
<td>May-13</td>
<td>CTO</td>
<td>22</td>
<td>Enc, Shr</td>
</tr>
<tr>
<td>PE</td>
<td>Physical and Environmental Protection</td>
<td>3</td>
<td>Feb-14</td>
<td>Jun-14</td>
<td>Ops Lead</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>PL</td>
<td>Planning</td>
<td>1</td>
<td>Feb-13</td>
<td>Apr-13</td>
<td>COO</td>
<td>80</td>
<td>N/A</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Security</td>
<td>2</td>
<td>Aug-13</td>
<td>Jan-14</td>
<td>HR</td>
<td>45</td>
<td>UtiliPr</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
<td>1</td>
<td>Feb-13</td>
<td>Apr-13</td>
<td>External</td>
<td>20</td>
<td>N/A</td>
</tr>
<tr>
<td>SA</td>
<td>Systems and Services Acquisition</td>
<td>3</td>
<td>Jun-14</td>
<td>Dec-14</td>
<td>CTO</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>SC</td>
<td>Systems and Communication Protection</td>
<td>2</td>
<td>Sep-13</td>
<td>Feb-14</td>
<td>Ops Lead</td>
<td>225</td>
<td>IBM Tiv</td>
</tr>
<tr>
<td>SI</td>
<td>System and Information Integrity</td>
<td>2</td>
<td>Sep-13</td>
<td>Feb-14</td>
<td>Dev Lead</td>
<td>110</td>
<td>IBM Tiv</td>
</tr>
<tr>
<td>PM</td>
<td>Program Management</td>
<td>3</td>
<td>Jun-14</td>
<td>Dec-14</td>
<td>Dev Lead</td>
<td>TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>

* = Thousands

### ENDNOTE

1. NIST SP 800-53 provides the “Recommended Security Controls for Federal Information Systems and Organizations.” It is published by the National Institute of Standards and Technology, a nonregulatory body of the US Department of Commerce. NIST’s mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.
Mobile devices are changing the way people work and many businesses are starting to extend their business applications and business intelligence (BI) capabilities to these devices. Smartphones, tablets and other mobile devices are playing an increasingly central role in how people communicate, network, work, shop and receive information. Mobile computing has been in the news frequently over the last two years. So much so, that the average consumer would think that it is a new innovation; however, this is not the case. Mobile computing has been around for over a decade. Lack of wireless connectivity, poor interface design and inefficient power management restricted early mobile equipment to limited markets, and there was no broad commercial success.

The use of smart devices is exploding. Gartner predicts sales of 1.2 billion smart devices in 2013, with much of this sales growth in the consumer market as a media-consumption platform. However, more and more enterprises are evaluating and using tablets for their mobile workforces. Gartner also predicted that in 2013, 80 percent of businesses will support tablets for their employees.

There is also a diverse initiative facing network administrators planning for mobility where IT may consider using consumer-grade devices, such as tablets, to lower hardware costs and increase productivity for dedicated applications such as retail kiosks or electronic medical records (EMR).

The consumerization of IT is being driven by the use of consumer-oriented devices and applications crossing over into the small and medium-sized enterprise (SME) markets. IT must figure out how to accommodate this because if the business does not simulate the kind of experience users have on the consumer side, they will figure out a way to go around IT to get their job done. Thus, it is important for network intelligence to embrace the inherent cost savings and flexibility built into such devices while controlling exactly what and how the devices are used on the network. A truly comprehensive mobile device solution will need to address both consumerization of IT and bring your own device (BYOD) in order to support, contain and embrace both types of devices. Currently, more than half of companies support BYOD environments in some shape or form. However, workers’ preferences for Apple’s iOS and Google’s Android mobile operating systems are driving out enterprise-friendly platforms, such as BlackBerry’s longtime operating system (OS) (now called BlackBerry 10) and Microsoft’s Windows Mobile OS.

As mobile device management (MDM) solutions continue to evolve, next generation technologies are geared to help security professionals move beyond consumer-oriented end points and their inherent security trade-offs. Moreover MDM adoption is being driven primarily by companies’ needs to properly manage an increasingly diverse population of devices. Nearly half of all organizations—46 percent—reportedly use MDM today, and 84 percent expect to deploy MDM by the end of 2014.

The Criticality of Mobile Device Management

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: www.isaca.org/currentissue
Enterprises are excited about the smaller form factor and increased mobility, but they have concerns about privacy, security and device management.

As organizations move to embrace the trend, it is important to consider how traditional security controls intersect with BYOD. It is understood that security policies need to be revisited in light of usability considerations during an enterprise’s BYOD deployment, but one area that is often overlooked is user density, which is critical in today’s BYOD planning.

For example, the recent US approval on TV white space (available frequency within UHF and VHS) will have a great impact on mobile technology, regulation and a new standard of 802.11ac and 802.11af for Wi-Fi. This development will facilitate very high-speed, efficient Internet connectivity in rural areas and developing countries. It may come in the form of machine-to-machine (M2M) communication by use of a cognitive radio.

With pressure on radio spectrum increasing all the time, it is necessary to utilize the available spectrum as efficiently as possible; one method of helping to achieve this is to utilize radio technology that is able to sense the available frequencies and configure itself accordingly. Using this technology, it will be possible for 802.11af systems to detect transmissions and move to alternative channels. TV white space will work efficiently when integrated with 4GLTE Advanced and connected to Wi-Fi 802.11ac radio. It can also establish connectivity to M2M integrated 802.11af in automobile, medical equipment and surveillance cameras regardless of their location (see Figure 1).

This will enable a very high bandwidth for triple-play video-streaming without buffering, allow for a longer-distance Internet connection with no line-of-sight challenges and enhance mobile hospitals regardless of the patients’ locations. Further, TV white space will also enhance automobile advancement for mobile Wi-Fi and maintenance, it will improve the scope of surveillance.

---

**Figure 1—Architectural Design for Last-mile Connectivity (Super Wi-Fi) With MDM Solution**

![Diagram showing the architectural design for last-mile connectivity using Super Wi-Fi with MDM solution.](image-url)
by security personnel regardless of the distance, and it will resolve intermittent Internet service, which has been the major obstacle to mobile-computing penetration and cloud computing for rural areas and developing countries with last-mile challenges.

BENEFITS OF MOBILE DEVICES

Early MDM solutions were designed to restrain the functionality of iOS and Android devices using secure container technology. These technologies provided a secure, managed workspace for employees to log in to access company data and core business tools such as email, calendars and contacts. Unfortunately, these solutions proved to be too security-focused; the secure container technologies got in the way, made apps inconvenient to use and interfered with the integrated user experience that made these devices so attractive. Most solutions, at the time, did not support single sign-on (SSO), thus forcing workers to reenter their authentication credentials every time their device woke from sleep mode in order to get back to work. Today’s secure container solutions have evolved to better meet both usability and security requirements, in addition to offering functionality that reflects the growing importance of apps in the workplace.

The benefits of mobile devices include:

• Improved business and employee collaboration—Employees use a variety of devices and tools to collaborate with their colleagues. While email is the universal application, the long tail of mobile applications includes browsers, content sharing, collaboration, unified communications and access to systems of record, such as the company intranet, sales force automation tools and line-of-business applications. With collaboration tools that can allow employees to use a single interface for multiple instant messaging (IM) accounts, access voice messages and enable others to see them when they are online, the risk of using mobile devices is eliminated, leaving only the benefits.

• Decreased worker latency—A tablet computer allows the mobile worker to be more responsive to important communications (i.e., text, voice, video) and better able to contribute to enterprise workflow and social networking. The decreased latency and improved mobile worker reach should improve customer satisfaction. Tablet computers can also be deployed at the executive level to replace notepads and binders.

• Increased productivity—Mobile devices enable employees to work anywhere their work takes them. Applications available for mobile workers form the core of collaboration solutions. Smartphones and tablets make it easier to read and respond to emails, review and edit important documents, and participate in strategic enterprise workflow.

MITIGATING RISK

While complying with security standards goes a long way toward mitigating risk, good policy planning and enforcement can do even more. The following needs to be considered for BYOD:

• Robust control and security—The enterprise’s smartphones and tablets must be managed by the corporate MDM system. Enforced MDM can improve security of the mobile device by forcing encryption, strong authentication and virtual private network (VPN) usage for communications with the corporate network. Sensitive data should always reside on a different network from that which is open to guests, contractors or other nonemployees, with a segmented network. The BYOD policy should also include specific applications that are acceptable, as well as those that are not. With application controls in place, the network becomes agnostic to the device and, instead, can enforce policies based on specific, acceptable applications.

• Securing and delivering corporate network access and services—BYOD requires IT departments to deliver the right level of access to the corporate network, based on the user’s profile and device. Users must also be able to access the appropriate applications, data and services. In accordance with standard security practices, companies should always enforce minimal access controls. In other words, even with BYOD, a strong security policy would be to deny all except for approved devices, applications and users.

• Corporate counsel involvement in recruitment processes—Organizational leaders must think through how their employees will handle information on a personally owned device. For example, depending on the jurisdiction, a merchant who experiences a breach may have to pay for a
legal settlement and Payment Card Industry Data Security Standard (PCI DSS) information control audits for up to five years. Specifically, it is important to remember that if an employee undertakes business activities using his/her own device, that device—and the data on it—could be discoverable during a legal proceeding. That situation would require the employee to surrender the device for examination.

• **Secure data transmission**—Security and encryption directly from the device to the network infrastructure, whether wired or wireless, allow a company to provide even its most sensitive data to mobile users regardless of device or location. The following are a few basic security points to keep the enterprise’s data safe on the respective mobile devices:
  – Update the smartphone OS, irrespective of it being an Android or an iOS, for example, whenever any application patches or OS upgrades are released.
  – Require the use of a pass code to lock the device in order to avoid data leakage if the device were to be used by a stranger.
  – Do not “jailbreak,” root or modify the OS files.
  – Install antivirus and firewall software to detect and stop any infection and intrusion.
  – Install device-tracking applications to find the phone if it is lost or stolen.
  – Regularly back up or synchronize the settings and other personal information in order to avoid the loss of data due to theft.

• **Unified policy, awareness, regulation and compliance**—This can help companies quickly and efficiently close the “mobile policy gap” and make BYOD more secure. Unified policy management is essential to enable, identify and manage all mobile devices that access the network. Damage controls should be in place, so that if an employee loses a smartphone or tablet, it can be wiped to avoid loss of data. Regulatory laws and compliance rules can further impact an organization’s bottom line in the event of data loss. For example, depending on the jurisdiction, a merchant who experiences a breach may have to pay for credit monitoring services for affected customers, payment of legal settlements and PCI DSS information control audits for up to five years.

• **Device protection and future consideration**—An additional layer of security at the device level, for both corporate and employee-owned devices, is essential for protecting sensitive company data. MDM allows network administrators to deny access and remotely wipe data from lost or stolen devices. IT must also prepare for the future wave of employees who expect to collaborate via the web, automotive Wi-Fi and Super Wi-Fi (using remote access solutions), and have the freedom to use their personal mobile devices in the workplace environment. Knowing that work is a thing employees do, no longer necessarily a place that they go, IT must afford secure access solutions, such as VPNs in order to empower employees to work anywhere.

• **Training and policy management**—Users need to appreciate that losing a mobile device is not just an inconvenience but might also be the cause of a data breach. Therefore, there has to be a strong emphasis on avoiding loss or theft. To reduce theft or misuse, the organization should conduct risk training for end users that emphasizes information asset ownership and physical security awareness. It should also consider stronger disciplinary measures, including suspension or even termination in the event of a serious breach and the implementation of a policy to focus employees’ attention on safeguarding their smartphone and tablet.

**CONCLUSION**

MDM is a major technology trend that is dramatically changing the IT paradigm. Knowing this and having a BYOD strategy in place is critical for success and data security. IT leaders will need to implement MDM solutions that address the variety of devices, apps and OSs that make up today’s increasingly diverse corporate computing environment. 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.

**REFERENCES**


Wi-Fi Alliance, www.wi-fi.org


Carlson Wireless, www.carlsonwireless.com
XIRRUS Wi-Fi Inc., www.xirrus.com
Nomadix Inc., www.nomadix.com


ENDNOTES
ISACA Training Week event in Las Vegas, NV, 9-12 December 2013 provides a unique opportunity for professionals with up to 5 years’ experience to:

- Earn up to 32 CPEs
- Learn from ISACA-accredited subject matter experts
- Choose from 5 courses designed to grow your expertise and your value to enterprises worldwide

Select the topic most relevant to your role and your goals:
- COBIT 5: Strategies for Implementing IT Governance
- Fundamentals of IT Audit & Assurance
- Governance of Enterprise IT
- Information Security Management
- IT Risk Management

To register or to learn more visit
www.isaca.org/trainingVegas/journal6
By Myles Mellor

www.themecrosswords.com

ACROSS

1. Public key encryption algorithm first outlined in 1977
3. Corporate official in charge of overseeing and managing compliance issues, abbr.
6. One of the developers of the key exchange protocol in 1976, Martin _____
10. Google ___s
11. Universally accepted designation for an IS auditor, abbr.
15. He explained the concept of information asymmetry in 1970, ___ Akerlof
15. Determine the sum of
16. German article
17. US DOD agency that develops new technologies, abbr.
18. Noncompliance can result in ___ of productivity and profit
21. Clever tactic
22. ___ Palmas
23. URL ending for MIT
25. Indicator
26. Warns
27. Voice publicly
28. Symbol for iron
29. Lively intelligence
31. Teach

36. Less disciplined
38. Acronym for a powerful but very expensive decryption tool
39. Financial and IT security inspectors
43. ____ answer (superficially plausible)
44. Superlative ending
45. Theft
46. Binary system basic

DOWN

1. Take a flawed product back
2. Weigh
5. Data storer
4. Piece in a machine
5. Global nonprofit think tank and community
6. Obstacles to be overcome
7. Distrustful
8. The foundation of one’s character: integrity would be one of these (2 words)
9. Evidence is growing that many of these bodies are engaged in clandestine cyberwarfare
12. Association promoting excellence in information systems, abbr.
14. US federal budget group, for short
19. Havens
20. Short poem
23. The E in ECC, an encryption algorithm
24. www address
25. Complete metric system of units of measurement for scientists
27. One of the five key features for the development of an effective compliance function
28. Workable
30. Marked by sound judgment, character trait important in IT professionals
32. Disapproval
33. Seeks help from (2 words)
34. Opposite of post-
37. Remedy
40. Make a selection
41. Data description
42. Reputation

(Answers on page 54)
TRUE OR FALSE

SULE ARTICLE

1. In 2005, Bob Sullivan quoted research figures that showed that 63 million US citizens were banking online in 2004.

2. An MITB attack is essentially a man-in-the-middle (MITM) attack, but unlike typical MITM attacks, which usually occur at the protocol layer, MITB attacks are introduced between the user and browser.

3. MITB attacks are cheap to carry out; therefore, they are usually performed by teenagers in their spare time.

4. A preventive measure for online banking interfaces is the bank sending a confirmation message (e.g., an SMS, email, call) to the customer describing the transaction.

PIRONTE ARTICLE

5. An information risk profile only documents the priority of information risk that an organization finds acceptable.

6. Enterprise risk management (ERM) is an evolving and important concept within many organizations and includes information risk management as one of its functions.

7. An organization's information risk profile should include guiding principles, including providing accurate identification and evaluation of threats, vulnerabilities and their associated risk.

8. Transparency is not at all critical to the success and adoption of an information risk profile.

GELBSTEIN ARTICLE

9. ISACA's Risk IT framework defines IT risk as “The business risk associated with the use, ownership, involvement, influence and adoption of IT within an enterprise.”

10. A well-developed business impact assessment (BIA) should reflect how business information is impacted and how time affects such impact.

11. Information risk management (IRM) came to the attention of business managers through factors including the convergence of increasing dependency on information technology in enterprise operations.

12. When IBM introduced System 360 in 1967, it became the largest software project at the time, totaling an estimated 50 million lines of code.

KUMAR ARTICLE

13. Hackers have managed to weaponize the encryption layer, using it to launch application-level and SSL attacks that can escape detection and remain hidden until it is too late.

14. According to a report released by a DDoS mitigation service provider security firm, a 188 percent increase in the total number of DDoS attacks was seen in the third quarter of 2012.

15. DDoS attacks are evolving in a number of ways, including an increase in frequency and impact.

16. To address issues appropriately in real time, a solid and tested incident response plan and procedures need to be in place.
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.

COBIT® Focus

is where global professionals share their practical tips for using and implementing ISACA’s frameworks.

For more information contact Jennifer Hajigeorgiou at publication@isaca.org.

The next issue accepting articles is January, volume 1, 2014.
Submission deadline is 4 December 2013.

Free subscriptions. Subscribe Now!

Answers—Crossword by Myles Mellor
See page 52 for the puzzle.

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

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

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should follow 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 (effective 1 November)

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 (in exposure)

Please note that the following list captures the structure and naming convention of the guidelines as they are being updated for integration into ITAF™. An exposure draft of the revised guidelines is posted for comment on the ISACA web site (www.isaca.org).

- **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 60008-3105, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at www.isaca.org/standards.
RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

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

**FEATURED...**

www.isaca.org/featuredbooks

**Reverse Deception: Organized Cyber Threat Counter-Exploitation**
464 pages — 31-MRDO

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$40.00</td>
<td>$50.00</td>
</tr>
<tr>
<td>Nonmember</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Transforming Cybersecurity: Using COBIT® 5**
Print Format — 190 Pages, 2013 — CBSTC

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$35.00</td>
<td>$60.00</td>
</tr>
<tr>
<td>Ebook</td>
<td>WC85TC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>Free</td>
<td>$60.00</td>
</tr>
<tr>
<td>Nonmember</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Responding to Targeted Cyberattacks**
Print Format — 90 pages, 2013 — RTC

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$35.00</td>
<td>$59.00</td>
</tr>
<tr>
<td>Ebook</td>
<td>WRTC</td>
<td></td>
</tr>
</tbody>
</table>

**Cloud Computing: Assessing the Risks**
306 pages — 17-ITCC

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$40.00</td>
<td>$50.00</td>
</tr>
</tbody>
</table>

**Pragmatic Security Metrics**
(Applying Metametrics to Information Security)
512 pages — 55-CRC

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$70.00</td>
<td>$80.00</td>
</tr>
</tbody>
</table>

* Published by ISACA and ITGI

ISACA member complimentary download www.isaca.org/downloads

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

---

**New Books...**

www.isaca.org/newbooks

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

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$35.00</td>
<td>$75.00</td>
</tr>
<tr>
<td>Ebook</td>
<td>WC85RK</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Management: Using COBIT® 5**
60 pages — CB85CM

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$30.00</td>
<td>$55.00</td>
</tr>
<tr>
<td>Ebook</td>
<td>WC85CM</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$35.00</td>
<td>$60.00</td>
</tr>
<tr>
<td>Ebook</td>
<td>WAPT</td>
<td></td>
</tr>
</tbody>
</table>

**Cyber Forensics**
342 pages — 100-WCF

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$80.00</td>
<td>$80.00</td>
</tr>
</tbody>
</table>

**Securing Cloud Services**
338 pages — 16-ITSCS

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$40.00</td>
<td>$50.00</td>
</tr>
</tbody>
</table>

**Computer Forensics InfoSec Pro Guide**
318 pages — 34-MCF

<table>
<thead>
<tr>
<th></th>
<th>Member</th>
<th>Nonmember</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>$40.00</td>
<td>$50.00</td>
</tr>
</tbody>
</table>

We are constantly expanding. Check out our new books and Ebooks!

https://www.isaca.org/bookstore/Pages/New-Arrivals.aspx
COBIT® 5 for Risk
By ISACA

COBIT 5 for Risk builds upon the COBIT 5 framework, in that it focuses on risk, and provides more detailed and more practical guidance for the risk professionals and other interested parties at all levels of the enterprise.

Using COBIT 5 for Risk brings a number of risk-related capabilities to the enterprise, which provides benefits such as:

- A more accurate view of risk throughout the enterprise, and the success with which the enterprise is addressing them
- End-to-end guidance on how to manage risk
- A common and sustainable framework/language for assessing and responding to risk
- Improved risk awareness throughout the enterprise

Print Format—213 pages, 2013—CB5RK
Member $35.00 | Nonmember $175.00
Ebook—WC5RK
Member $35.00 | Nonmember $175.00

Configuration Management: Using COBIT® 5
By ISACA

Change is imminent, as enterprises and technology become larger and more complex. Change without proper communication and coordination leads to business disruptions, inefficiencies and potential financial loss. Configuration management is a key component to help enterprise leaders manage change and minimize unforeseen impacts.

Practice shows that enterprise stakeholders have varied ideas about the meaning of the term “configuration management” and what it entails, causing misalignment in the implementation of CM and the possibility of unmanaged expectations.

Configuration management is a strategic capability that supports many other activities within an enterprise, not a standalone process with simple objectives.

This publication details the necessary elements required to develop, implement and manage a homogenous and sustainable configuration management (CM) process including the most important challenges and mitigating strategies.

Print Format—60 pages—CB5CM
Member $30.00 | Nonmember $55.00
Ebook—WC5CM
Member FREE | Nonmember $55.00

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.

This book is designed primarily for security managers, IT managers, IT auditors and students studying for computer science or information security qualifications. It is written in clear, nontechnical language so it will also be of value to business managers and government officials responsible for valuable intellectual assets or critical services that might be the target of an APT attack.

Print Format—132 pages—APT
Member $35.00 | Nonmember $60.00
Ebook—WAPT
Member FREE | Nonmember $60.00

* 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
Transforming Cybersecurity: Using COBIT® 5

By ISACA

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability. This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.

Print Format—190 pages, 2013—CB5TC

Ebook—WCB5TC

Cloud Computing: Assessing the Risks

By Jared Carstensen, Bernard Golden and J. P. Morgenthal

‘Cloud Computing’ are the words on everyone’s lips – it’s the latest technology, the way forward. But how safe is it? Is it reliable? How secure will your information be?

Cloud Computing: Assessing the Risks answers these questions and many more. Using jargon-free language and relevant examples, analogies and diagrams, it is an up-to-date, clear and comprehensive guide the security, governance, risk, and compliance elements of Cloud Computing.

Written by three internationally renowned experts, this book discusses the primary concerns of most businesses leaders—the security and risk elements of the Cloud. But ‘security and risk’ are just two elements of Cloud Computing, and this book focuses on all the critical components of a successful cloud programme including — compliance, risk, reliability, availability, areas of responsibility, Cloud Computing borders, legalities, digital forensics and business continuity. This book covers them all.

Print Format—306 pages—17-ITCC

Pragmatic Security Metrics (Applying Metametrics to Information Security)

By W. Krag Brotby and Gary Hinson

Other books on information security metrics discuss number theory and statistics in academic terms. Light on mathematics and heavy on utility, PRAGMATIC Security Metrics: Applying Metametrics to Information Security breaks the mold. This is the ultimate how-to-do-it guide for security metrics.

Packed with time-saving tips, the book offers easy-to-follow guidance for those struggling with security metrics. Step by step, it clearly explains how to specify, develop, use, and maintain an information security measurement system (a comprehensive suite of metrics) to help:

• Security professionals systematically improve information security, demonstrate the value they are adding, and gain management support for the things that need to be done
• Management address previously unsolvable problems rationally, making critical decisions such as resource allocation and prioritization of security relative to other business activities
• Stakeholders, both within and outside the organization, be assured that information security is being competently managed

Print Format—512 pages—55-CRC

* 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
EXAM REFERENCE MATERIALS

2014 CISA® EXAM REFERENCE MATERIALS

To prepare for the June 2014 CISA exam, order
www.isaca.org/cisabooks

CISA Review Manual 2014*
CISA Review Questions, Answers & Explanations Manual 2013 Supplement*
CISA Review Questions, Answers & Explanations Manual 2014 Supplement*
CISA Practice Question Database v14*

2014 CISM® EXAM REFERENCE MATERIALS

To prepare for the June 2014 CISM exam, order
www.isaca.org/cismbooks

CISM Review Manual 2014*
CISM Practice Question Database v14*

2014 CGEIT EXAM REFERENCE MATERIALS

To prepare for the June 2014 CGEIT exam, order
www.isaca.org/cgeitbooks

CGEIT Review Manual 2014*
CGEIT Review Questions, Answers & Explanations Manual 2013 Supplement*
CGEIT Review Questions, Answers & Explanations Manual 2014 Supplement*

2014 CRISC EXAM REFERENCE MATERIALS

To prepare for the June 2014 CRISC exam, order
www.isaca.org/criscbooks

CRISC Review Manual 2014*
CRISC Review Questions, Answers & Explanations Manual 2013
CRISC Review Questions, Answers & Explanations Manual 2014 Supplement*

COBIT 5 PUBLICATIONS

www.isaca.org/featuredbooks

COBIT 5 CB5
Member $35.00
Nonmember $50.00
WCB5—EBOOK PDF FORMAT
Member FREE
Nonmember $40.00

COBIT 5: Enabling Processes CB5SEP
Member $35.00
Nonmember $135.00
WCB5SEP—EBOOK PDF FORMAT
Member FREE
Nonmember $135.00

COBIT 5 for Information Security CB5IS
Member $35.00
Nonmember $175.00
WCB5IS—EBOOK PDF FORMAT
Member $35.00
Nonmember $175.00

COBIT Process Assessment Model (PAM): Using COBIT 5 CPAMS
Member $30.00
Nonmember $50.00
WCPAMS—EBOOK PDF FORMAT
Member FREE
Nonmember $40.00

COBIT for Assurance CB5A
Member $35.00
Nonmember $175.00
WCB5A—EBOOK PDF FORMAT
Member $35.00
Nonmember $175.00

COBIT 5 Implementation CB5IG
Member $35.00
Nonmember $150.00
WCB5IG—EBOOK PDF FORMAT
Member FREE
Nonmember $150.00

COBIT Self-assessment Guide: Using COBIT 5 CSG5
Member $30.00
Nonmember $50.00
WCSAG5—EBOOK PDF FORMAT
Member $30.00
Nonmember $80.00

COBIT Assessor Guide: Using COBIT 5 CAG5
Member $30.00
Nonmember $80.00
WCAG5—EBOOK PDF FORMAT
Member $30.00
Nonmember $80.00

COBIT 5 for Risk CB5RK
Member $35.00
Nonmember $175.00
WCB5RK—EBOOK PDF FORMAT
Member $35.00
Nonmember $175.00
### 2014 CISA® EXAM REFERENCE MATERIALS

#### To prepare for the June 2014 CISA exam, order

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-14</td>
<td>English Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CM-14C</td>
<td>Chinese Simplified Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CM-14F</td>
<td>French Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CM-14I</td>
<td>Italian Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CM-14J</td>
<td>Japanese Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CM-14S</td>
<td>Spanish Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
</tbody>
</table>

#### CISA Review Questions, Answers & Explanations Manual 2013*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>QA-13E</td>
<td>Chinese Simplified Edition (950 Questions)</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>QA-13I</td>
<td>Italian Edition (950 Questions)</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>QA-13J</td>
<td>Japanese Edition (950 Questions)</td>
<td>130.00</td>
<td>100.00</td>
</tr>
<tr>
<td>QA-13S</td>
<td>Spanish Edition (950 Questions)</td>
<td>130.00</td>
<td>100.00</td>
</tr>
</tbody>
</table>

#### CISA Review Questions, Answers & Explanations Manual 2014 Supplement*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>QA-14ES</td>
<td>English Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14CS</td>
<td>Chinese Simplified Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14FS</td>
<td>French Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14IS</td>
<td>Italian Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14JS</td>
<td>Japanese Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14S</td>
<td>Spanish Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

#### CISA Practice Questions Database v14 (1,150 Questions)*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD-B-14</td>
<td>CD-ROM—English Edition</td>
<td>225.00</td>
<td>185.00</td>
</tr>
<tr>
<td>CD-B-14W</td>
<td>Download—English Edition (no shipping charges apply to download)</td>
<td>225.00</td>
<td>185.00</td>
</tr>
<tr>
<td>CD-B-14S</td>
<td>CD-ROM—Spanish Edition</td>
<td>225.00</td>
<td>185.00</td>
</tr>
</tbody>
</table>

#### 2014 CISM® EXAM REFERENCE MATERIALS

#### To prepare for the June 2014 CISM exam, order

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-123</td>
<td>Japanese Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
</tbody>
</table>

#### CISM Review Manual 2014*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-14M</td>
<td>English Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CM-14S</td>
<td>Spanish Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
</tbody>
</table>

#### CISM Review Questions, Answers & Explanations Manual 2014*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>QA-14</td>
<td>English Edition (615 Questions)</td>
<td>90.00</td>
<td>70.00</td>
</tr>
<tr>
<td>QA-14J</td>
<td>Japanese Edition (615 Questions)</td>
<td>90.00</td>
<td>70.00</td>
</tr>
<tr>
<td>QA-14S</td>
<td>Spanish Edition (615 Questions)</td>
<td>90.00</td>
<td>70.00</td>
</tr>
</tbody>
</table>

#### CISM Review Questions, Answers & Explanations Manual 2014 Supplement*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>QA-14E5</td>
<td>English Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14S</td>
<td>Spanish Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14S</td>
<td>Spanish Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QA-14S</td>
<td>Spanish Edition (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

#### CISM Practice Questions Database v14 (915 Questions)*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>MB-D-14</td>
<td>CD-ROM—English Edition</td>
<td>160.00</td>
<td>120.00</td>
</tr>
<tr>
<td>MB-D-14W</td>
<td>Download—English Edition (no shipping charges apply to download)</td>
<td>160.00</td>
<td>120.00</td>
</tr>
</tbody>
</table>

#### 2014 CGEIT EXAM REFERENCE MATERIALS

#### To prepare for the June 2014 CGEIT exam, order

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGCM-14*</td>
<td>CGEIT Review Manual 2014</td>
<td>115.00</td>
<td>85.00</td>
</tr>
</tbody>
</table>

#### CGEIT Review Manual 2014*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CG-01*</td>
<td>CGEIT Review Questions, Answers &amp; Explanations Manual 2013 (60 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CG-03E5*</td>
<td>CGEIT Review Questions, Answers &amp; Explanations Manual 2013 Supplement (60 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

#### CGEIT Review Questions, Answers & Explanations Manual 2014 Supplement*

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CG-01E5*</td>
<td>CGEIT Review Questions, Answers &amp; Explanations Manual 2014 Supplement (60 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

#### 2014 CRISC EXAM REFERENCE MATERIALS

#### To prepare for the June 2014 CRISC exam, order

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR-14</td>
<td>CRISC Review Manual 2014</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CR-123</td>
<td>CRISC Review Questions, Answers &amp; Explanations Manual 2013 (200 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CR-13E5*</td>
<td>CRISC Review Questions, Answers &amp; Explanations Manual 2013 Supplement (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CR-14E5*</td>
<td>CRISC Review Questions, Answers &amp; Explanations Manual 2014 Supplement (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CRX</td>
<td>CRICRISCExamSelf-StudySubscription–6Months</td>
<td>225.00</td>
<td>185.00</td>
</tr>
</tbody>
</table>

#### COBIT® 5

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CB5-5</td>
<td>Arabic</td>
<td>50.00</td>
<td>35.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>English</td>
<td>50.00</td>
<td>35.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Chinese Simplified</td>
<td>50.00</td>
<td>35.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>German</td>
<td>50.00</td>
<td>35.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Japanese</td>
<td>50.00</td>
<td>35.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Spanish</td>
<td>50.00</td>
<td>35.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Russian</td>
<td>50.00</td>
<td>35.00</td>
</tr>
</tbody>
</table>

#### COBIT® 4.1

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WC5-5</td>
<td>English, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>WC5-5</td>
<td>Chinese Simplified, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
</tbody>
</table>

### SUPPLEMENT

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CB5-5</td>
<td>English, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Chinese Simplified, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>German, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Japanese, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Spanish, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Romanian, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>French, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Spanish, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
<tr>
<td>CB5-5</td>
<td>Romanian, Print Format</td>
<td>135.00</td>
<td>95.00</td>
</tr>
</tbody>
</table>

---

*Published by ISACA and ITGI

**ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE**

Shaded — New Books

S-5
**Customer Order Form**

Order Online at www.isaca.org/bookstore

---

Please return to: ISACA, 1055 Paysphere Circle, Chicago, IL 60674, USA  
Phone: +1.847.660.5650  
Fax: +1.847.253.1443  
E-mail: bookstore@isaca.org

**PLEASE NOTE:** READ PAYMENT TERMS AND SHIPPING INFORMATION BELOW. ALL ORDERS MUST BE PREPAID.

Your contact information will be used to fulfill your request, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. To learn more, please visit www.isaca.org and read our Privacy Policy.

---

### Customer Information

<table>
<thead>
<tr>
<th>Name</th>
<th>FIRST</th>
<th>MIDDLE</th>
<th>LAST/FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA Member:</td>
<td>No</td>
<td>Yes</td>
<td>Member Number</td>
</tr>
</tbody>
</table>

**Company Name**

**Address:**  
Home  
Company

<table>
<thead>
<tr>
<th>City</th>
<th>State/Province</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zip/Postal Code</td>
<td></td>
</tr>
</tbody>
</table>

**Country**

**Phone Number**  
( )

**Fax Number**  
( )

**E-mail Address**

---

### Code

<table>
<thead>
<tr>
<th>Title/Item</th>
<th>Quantity</th>
<th>Unit Price</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Subtotal**

**Sales Tax:** Add sales tax if shipping to:  
- Louisiana (LA)—4%  
- Oklahoma (OK)—4%  
- Wisconsin (WI)—5%  
- Florida (FL), Minnesota (MN), Pennsylvania (PA), South Carolina (SC), Texas (TX), Washington (WA)—6%  
- California (CA), New Jersey (NJ), Puerto Rico (PR), Tennessee (TN)—7%  
- Illinois (IL)—9%

**For all orders please include shipping and handling charge—see chart below.**

**Shipping & Handling Rates for Orders**

All orders outside the US are shipped Federal Express Priority.

<table>
<thead>
<tr>
<th>For Orders Totaling</th>
<th>Outside US</th>
<th>Within US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to US $30.00</td>
<td>US $10.00</td>
<td>US $5.00</td>
</tr>
<tr>
<td>US $30.01 to US $50.00</td>
<td>US $15.00</td>
<td>US $7.00</td>
</tr>
<tr>
<td>US $50.01 to US $80.00</td>
<td>US $20.00</td>
<td>US $8.00</td>
</tr>
<tr>
<td>US $80.01 to US $150.00</td>
<td>US $26.00</td>
<td>US $10.00</td>
</tr>
<tr>
<td>Over US $150.00</td>
<td>17% of Total</td>
<td>10% of Total</td>
</tr>
</tbody>
</table>

No shipping charges apply to Meycor CobiT.

No shipping charges apply to CISA Practice Question Database v13—download.

No shipping charges apply to CISM Practice Question Database v13—download.

---

**Shipping Information** (If different from customer information)

If shipping to a PO Box, please include street address to ensure proper delivery.

<table>
<thead>
<tr>
<th>Name</th>
<th>FIRST</th>
<th>MIDDLE</th>
<th>LAST/FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Address:**  
(IF PART OF SHIPPING ADDRESS)

<table>
<thead>
<tr>
<th>City</th>
<th>State/Province</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zip/Postal Code</td>
<td></td>
</tr>
</tbody>
</table>

**Country**

**Phone Number**  
( )

**Fax Number**  
( )

**E-mail Address**

---

**Thank you for ordering from ISACA. All purchases are final.**

---

**Payment Information—Prepayment Required**

- Payment enclosed. Check payable to “ISACA” in US dollars, drawn on US bank.  
- Bank wire transfer in US dollars. Date of transfer:  
- Charge to  
  - Visa  
  - American Express  
  - MasterCard  
  - Discover

**Credit Card #**

**Exp. Date**

**Print Cardholder Name**

**Signature of Cardholder**

---

**Shipping & Handling Rates for Orders**

All orders outside the US are shipped Federal Express Priority.

<table>
<thead>
<tr>
<th>For Orders Totaling</th>
<th>Outside US</th>
<th>Within US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to US $30.00</td>
<td>US $10.00</td>
<td>US $5.00</td>
</tr>
<tr>
<td>US $30.01 to US $50.00</td>
<td>US $15.00</td>
<td>US $7.00</td>
</tr>
<tr>
<td>US $50.01 to US $80.00</td>
<td>US $20.00</td>
<td>US $8.00</td>
</tr>
<tr>
<td>US $80.01 to US $150.00</td>
<td>US $26.00</td>
<td>US $10.00</td>
</tr>
<tr>
<td>Over US $150.00</td>
<td>17% of Total</td>
<td>10% of Total</td>
</tr>
</tbody>
</table>

No shipping charges apply to Meycor CobiT.

No shipping charges apply to CISA Practice Question Database v13—download.

No shipping charges apply to CISM Practice Question Database v13—download.

---

**Shipping details www.isaca.org/shipping**

International customers are solely responsible for paying all custom duties, service charges, and taxes levied by their country.

**All purchases are final. Pricing, shipping and handling, and tax are subject to change without notice.**
Clarity. Unity. Trust.

COBIT 5 for Risk

Linking IT Risk to Business Risk to Achieve Enterprise Objectives

AVAILABLE NOW AT
WWW.ISACA.ORG/COBIT-RISK
The Security Intelligence Report (SIR) is an analysis of the current threat landscape based on data from over a billion systems worldwide and some of the Internet’s busiest online services to help you protect your organization, software, and people.

View the Security Intelligence Report at www.microsoft.com/SIR