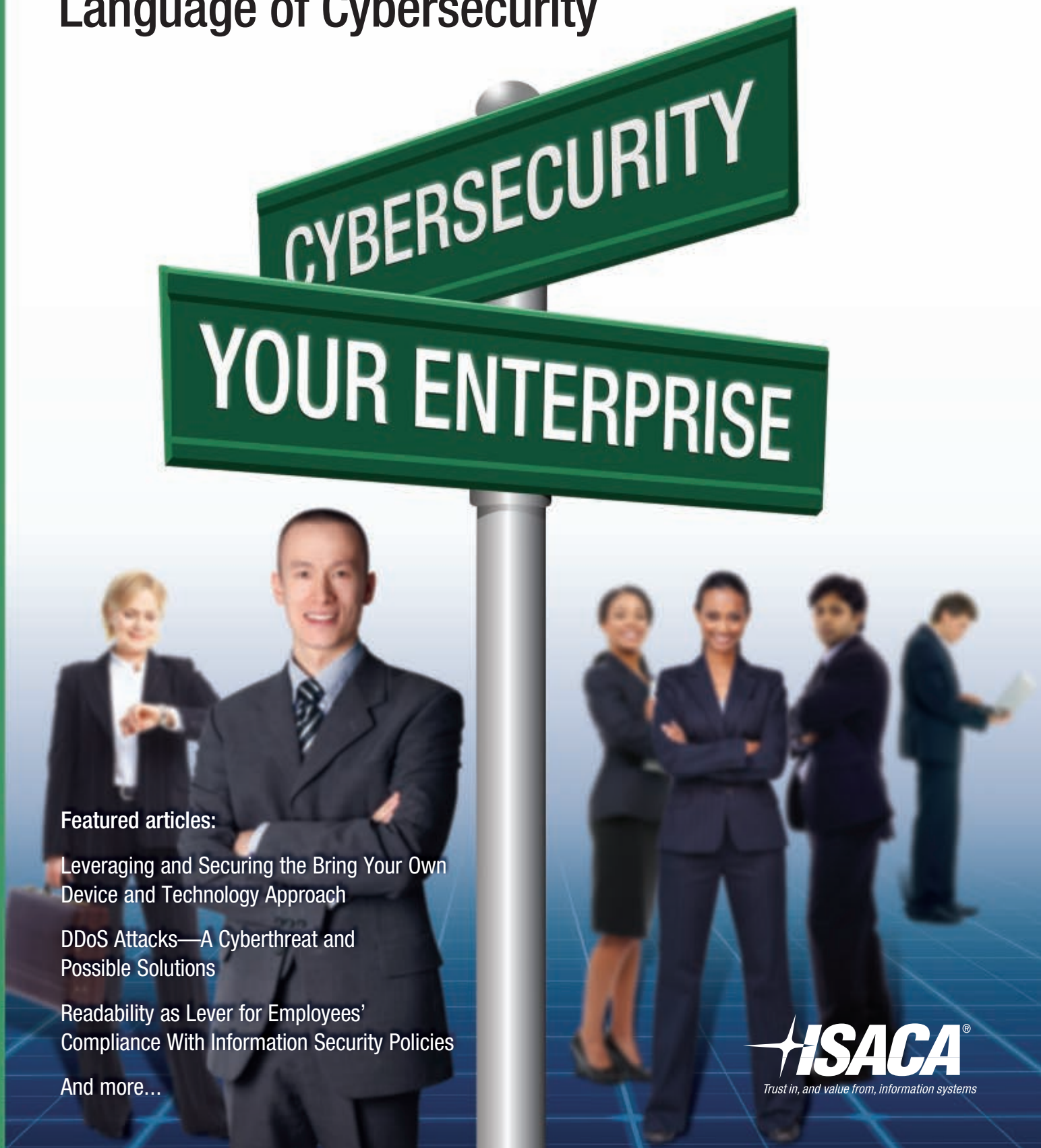
VOLUME 4, 2013

ISACA® Journal

Language of Cybersecurity



Featured articles:

Leveraging and Securing the Bring Your Own Device and Technology Approach

DDoS Attacks—A Cyberthreat and Possible Solutions

Readability as Lever for Employees' Compliance With Information Security Policies

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification

UPCOMING EXAM DATE—All four certification exams

14 DECEMBER 2013

Early registration deadline: 21 August 2013
Final registration deadline: 25 October 2013

For more information and to register for an ISACA exam, visit ***isaca.org/myfuture-Jv4***.

TeamMate®

World Leading Audit & Controls Management Tools

TeamMate AM is the solution of choice for 90,000 auditors in more than 2,200 organizations world-wide. AM addresses key audit management functions such as risk assessment, scheduling, documentation, issue tracking, and time reporting, enabling you to standardize and streamline your entire audit process.

TeamMate CM is focused on the management and testing of SOX, COBIT®, IT Governance or any other set of internal controls. CM allows you to view and interact with controls through an innovative user-defined structure based on Dimensions and Perspectives of data that leads to greater efficiency and deeper insight when managing your compliance needs.

The integration of TeamMate AM and TeamMate CM promotes leveraging and sharing of data and workflows across the Internal Audit and Compliance disciplines.

Learn more at **TeamMateSolutions.com**

Join the Conversation

Wolters Kluwer
Audit, Risk & Compliance

VOLUME 4, 2013

ISACA® Journal

Columns

Features

Plus

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

Journal Online

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

Online Features
The following articles will be available to ISACA members online on 1 August 2013.

Evolving Perimeter Information Security Models in Smart Grids and Utilities
Naresh Kurada, CISA, MSEE, P.Eng., A. Alex Dhanjal, P.Eng. and Bala Venkatesh, Ph.D., P.Eng.

Mitigating Software Supply Chain Risk
C. Warren Axelrod, Ph.D., CISM, CISSP

What's in a Word? Measuring the Language of Information Security
Lance Hayden, Ph.D., CISM, CRISC, CISSP

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

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

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

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

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

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

KEEP YOUR **CAREER** ON TRACK

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.

REGIS UNIVERSITY
School of Computer & Information Sciences

LEARN MORE

www.regisdegrees.com/ISACA | 855.508.8454

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1999. He can be reached at *stross@riskmastersinc.com.*

Just Privacy

I recently attended a conference on the subject of the privacy of electronic medical records. Speaker after speaker arose and reassured the attendees that privacy was "not an IT problem." The more I listened, the more perturbed I became, so at the coffee break, I took a marker and a piece of paper and wrote, in capital letters, one word. I stood outside the auditorium with my sign that said: JUST. I expected to attract attention to what I considered to be a serious error in the speeches, and I did get some conversation started. There are many nontechnical ramifications to data privacy, so it is not JUST an IT problem, but at bottom, there is much electronic information that is at risk of misuse and the solutions stem from the implementation of technical solutions.

RULES AND RAMIFICATIONS

I recognize that data privacy has many aspects—cultural, societal, legal, regulatory and managerial—in addition to the technical ones. Nations differ as to what privacy means and how it is to be accomplished. Western European countries, through the European Union, consider privacy to cut across all uses of personal information, while the US applies vertical sectors, for example, in government, finance and health care. Societies show their support for privacy by passing and enforcing laws and regulations. But, unless there is a general, societal commitment to enabling the subjects of data records to retain an interest in and a degree of control over how those records are used, privacy laws are of little avail.

Rules do have their place; so does a broad-based culture of security[1] within businesses and government agencies. But, without the application of the necessary technical tools, all the laws, policies and directives in the world are fond wishes, not reality.

While information security encompasses more than just privacy, it is the *sine qua non*. An organization must control who has access to which information and how it will be used if it is to ensure that the data it collects about individuals are used only for their intended purpose, that they are stored in such a way that they cannot be used in unintended ways and that they are disposed of when they are no longer needed. Unfortunately, access control as it has historically been implemented is too blunt an instrument for the purpose.

In general, access control tools limit the ability to read from or write to certain files; they may also control who may use transactions that have the same effect. In my experience, greater emphasis is placed on the integrity of data and the ability to change data, than on data's confidentiality, which is necessary for privacy, but not sufficient. Thus, in the organizations I have seen, many people can view information, but the ability to write or manipulate it is more restricted. Moreover, it is not good enough for privacy purposes to say that a person may see all related records of a type of data subject, e.g., hospital patients.[2] For privacy purposes, access must be limited more rigorously—and with greater difficulty. But, tools to facilitate efficient delegation of access, for example, are not always sufficient to address legitimate access control needs.

ROLES AND FIELDS

Privacy often requires a complex set of rules and data relationships that may be summarized as *role-based* and *field-level* access control. So, for example, nurses may see information about patients; as stated before, this is a necessary rule but not granular enough for privacy's sake. Individual nurses may see information only about the patients assigned to them. Although they have access to the patient database, they do not have license to roam at will through the records of all patients at all times. Thus the field <nurse-name> must be associated with that of <patient-name>. It may also be connected to a field indicating working hours, <shift>, so that nurses can see the data only during their time on duty. While it is intended that nurses see all sorts of medical and diagnostic information in the course of their routine responsibilities, they have no need or

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:

permission to access financial information, e.g., whether a patient has paid his/her bills.

While nurses should see only their own patients' information, medical researchers should be restricted to diagnostics. If they are studying, for example, lung cancer, then they may see information only about those with that disease, but they may not see that which would identify the person with it. Thus, the fields <researcher-name> and <diagnosis> must be associated, while access to fields such as <patient-name> and <patient-address> (and even <nurse-name>) must be blocked.

The hospital's payroll department needs to have access to data about both nurses and researchers, but only in their roles as employees, not in terms of their professions. The field <employee-name> should equate to that of <nurse-name> and <researcher-name>,[3] but payroll clerks should not be able to traverse databases unrelated to their job functions. In the context described here, a single institution must establish the privacy of health care, financial and employment data.

It is not my purpose here to address the specific technical tools that are needed for achieving data privacy. A combination of database designers, information security professionals and application developers must select, implement and manage the mechanisms by which privacy is effected. These people do not make the rules, they do not populate the fields, but they do make privacy possible. To a great extent, privacy *is* IT.

> "To a great extent, privacy is IT."

FAIR AND EQUITABLE

There is another connotation to privacy being JUST IT, in the sense that retaining a data subject's rights and control is fair and equitable to the people involved. I believe that organizations should institute privacy in policy and in deed for its own value, not simply to comply with society's laws. This is simply good business practice that needs neither rules nor laws. To continue the health care example, patients should be able to enter a hospital without worrying that information about their disease might be disclosed to someone with no need to know or to the public at large.

A hospital that is attentive to appropriate restrictions on data access and use is a better place to receive medical attention. Hospital administrators do not usually harm patients' interests intentionally, either in professional or data terms. But it is not clear that they have always had—or have now—the support and the technology to ensure that patients' data rights are considered and enforced, much less that the hospital can continuously comply. This is, as the conference speakers asserted, not an IT issue *but* IT is the means to the desired end.

ENDNOTES

[1] Ross, Steven; *Creating a Culture of Security*, ISACA, 2011. Is there no end to plugging this book?

[2] I will use health care examples because I attended a conference dealing with personal health information (PHI). However, I believe my point is equally applicable to the protection of all personally identifiable information (PII) across industries.

[3] It should but often does not. This hypothetical payroll system was probably designed by someone other than the developer of the patient care system, so data definitions are often not the same, nor are those entering the data. Steven J. Ross may be the same person as Steven Jay Ross or Steve Ross, but the system has no way of knowing. The endless quest for canonical data is beyond the scope of this article, but is another detriment to privacy.

What Every IT Auditor Should Know About Using Inquiry to Gather Evidence

Tommie Singleton, CISA, CGEIT, CPA, is the director of consulting for Carr Riggs & Ingram, a large regional public accounting firm. His duties involve forensic accounting, business valuation, IT assurance and service organization control engagements. Singleton is responsible for recruiting, training, research, support and quality control for those services and the staff that perform them. He is also a former academic, having taught at several universities from 1991 to 2012. Singleton has published numerous articles, coauthored books and made many presentations on IT auditing and fraud.

Most IT audits—be they assurance-driven, consulting-driven or internally driven—require the IT auditor to assess risk, develop a plan and use that plan to gain evidence about the audit objectives. Inquiry is a procedure commonly used in gathering evidence.

INQUIRY FRAMEWORK

It could be said that there are two kinds of inquiry: personal interviews and questionnaires. There is value in both, and they have some exclusive advantages and disadvantages.

The interview has several advantages over a questionnaire. For instance, in the interview, the auditor can be alert for visual or audible cues about the person's veracity. Research shows that people who are under stress because they are lying generally show it with body language, speech cues or other behavioral traits. Other information may be gathered from the person's behaviors and reactions as well.

The interview also has the advantage of the nature of conversations vs. a dry list of boxes to check. For instance, the interviewer can use open-ended questions. Also, sometimes the interviewer or interviewee gets into a flow of conversation. Be it better recall on the part of the interviewee or more effective questions on the part of the interviewer, this flow often generates more pertinent information. When using questionnaires, a flow is just generally not possible. Interviews are also a more effective technique when the nature of the questions call for insights, assessments and other analytically processed information.

The disadvantages of interviews include the availability of both parties, the ability for the auditor to be physically present with the interviewee, distractions that can occur in the interview location, the time it takes to create the interview questions, the time it takes to transcribe an interview and other resource constraints.

A questionnaire has advantages unique to its nature. The process can be made concise, thus limiting the amount of time the auditee must invest in the process of providing answers. It can use standard, professionally developed questions that are known to be effective. For financial audits, there are providers of audit tools, including questionnaires, for each aspect of the audit that needs information gathered. Thus, the time involved in developing the questionnaire can be minimal, but still relatively effective. The IT audit profession is, in fact, replete with questionnaires related to various types of audits, audit procedures or audit objectives.

One key advantage of questionnaires relates to the nature of the questions. If the IT auditor is trying to gather answers to questions about systems, applications and technologies that are fact-based, a questionnaire works quite well.

The disadvantage of a questionnaire can be the loss of the advantages of an interview; for instance, the information gathered in interviews is generally richer. There is also a temptation for the interviewer's and interviewee's minds to slip into neutral with planned and canned questionnaires, because of the lack of engagement. There are many things about auditors that make them professional and valuable, but none more important than their analytical thinking and mind-set. To become mindless to questionnaires is to forfeit this valuable asset. Therefore, IT auditors need to resist the temptation to copy a questionnaire from last year (or pull it from the audit methodology provider's kit), get answers to the questions this year and check off on the audit plan that this step has been completed—something affectionately referred to as SALY (same as last year). Another potential disadvantage is when the auditee fails to complete the questionnaire, misunderstands questions, or otherwise provides incomplete or incorrect information. In the interview, it is likely the auditor would catch such situations and correct them immediately. Thus, the questionnaire is more costly in correcting information errors.

There is no one perfect way to gather information using an inquiry approach. Consideration should be given to all approaches, and if the questionnaire/checklist is used, care needs to be taken to keep the auditor's and interviewee's mind engaged and to provide an analytical approach to the information being gathered (**figure 1**).

Figure 1—Interview vs. Questionnaire Matrix

Situation	Interview	Questionnaire
Availability of personnel	Can be a detraction	Does not matter
Nature of questions	Open-ended, analytical information	Closed, factual information
Scope of information gathered	Flow, richer, observable cues	Plain, direct facts
Cost of process	Usually higher than questionnaire	Usually less than interview
Information errors	Easier to identify and correct	Costly to identify and correct

INQUIRY EFFECTIVENESS

There are several manners of gathering evidence. One popular framework is: inquiry, observation, examination and inspection/reperformance. These types of tests vary in terms of strength and are generally seen as depicted in **figure 2**.

Figure 2—Testing Strategy

Type of Test	Level of Reliance on Test Results
Inquiry	Little
Observation	Moderate
Examination	Moderate
Inspection/reperformance	High

Thus, the audit objective and the assessed level of risk have an effect on the type of test chosen. In general, the higher the risk, the greater the need for inspection or reperformance as the type of test for gathering audit evidence. Obviously, inquiry is viewed as providing the least amount of assurance and, thus, has a low level of reliance as evidence. There are a variety of reasons why inquiry, or inquiry alone, may be insufficient in developing competent evidence (see **figure 3**).

Figure 3—When Inquiry May Be or Is Insufficient

- The AICPA standards require more than inquiry evidence to satisfy assurance in a financial audit.
- Information provided via inquiry *is not* the actual circumstances.
- Business processes and/or controls that should be in place *are not* operating effectively.
- Access rights are in place that should not be operating.
- Nefarious activities are hidden, but operating to the detriment of the entity.
- The auditor inadvertently disengages his/her analytical mind and misses a key piece of evidence.

For instance, the American Institute of Certified Public Accountants (AICPA) has stated in its technical literature that evidence from inquiry alone is not sufficient in a financial audit. Clearly, an overreliance on inquiry as evidence can lead to an audit with weak quality. Therefore, the IT auditor needs to take care in choosing inquiry as the type of test. Some of the pertinent questions would include: Which audit objectives are suitable for inquiry? How much of the evidence should be via inquiry? Is the type of test and the assessed risk a proper fit?

A specific example in IT may be helpful to demonstrate some of the nuances in inquiry. The following illustrates a situation that is not uncommon: Executives establish standard operating procedures and a sufficiency of controls, then believe those procedures are being done and those controls have operating effectiveness. However, for various reasons, those controls have been changed and are not as effective as designed, and those procedures have been tweaked by well-intentioned (or sometimes malicious) employees and are not functioning as planned.

An example from a real audit involves an interview-type inquiry in which two C-level executives were asked about access controls. When asked who had access to a certain high-risk function, the IT auditors were given a very short list (good news so far). When asked if anyone else could get access to the function, the answer was no one (feeling good about access controls). But when the IT auditors used an inspection test for the access controls—due to the fact that a high level of risk was assessed to this function—they discovered that several other people had access and that a key senior executive actually assigned login credentials and kept a handwritten list of all of them. That fact was unknown to the other executives and apparently to everyone except those who had been granted access—who assumed the credentials process was authorized and standard operating procedure.

Therefore, IT auditors need to be careful about relying on inquiry evidence when obtained from senior managers and executives who may be under the wrong impression about the procedures and controls they designed and believe were implemented. If there is any significance in the difference between design and operations, it could cancel out the assurance that the inquiry *appears* to provide. This possibility exists in almost every IT audit, regarding some aspect of the entity's procedures (business processes) and controls. The further the inquiry participant is from front-line employees and processes, the more likely this scenario becomes. Thus, when conducting an inquiry of senior management or executives either via interview or questionnaire, the IT auditor should take care in confirming the inquiry information; that is, less reliance is placed on inquiry as evidence.

Other dangers include the aforementioned temptation to focus on the answers of a questionnaire and mentally disengage. The previous example shows how that can be devastating in the wrong set of circumstances. However, the evidence gathered in the inquiry was not difficult to confirm with another test type.

A set of dangers could be labeled as: things that should be operating effectively but are not. For instance, as mentioned previously, employees have been known to tweak business processes or controls (manual or IT-dependent controls) to make their job easier, but the end result is a detriment to the overall control system or effectiveness of a business process. The danger here is when two things happen:

1. The employee makes unauthorized adjustments and/or changes to business practices or controls and does not communicate that change to the proper authorities.
2. The change is to the detriment of the overall internal control structure or effectiveness of business processes.

Employees can also simply fail to follow standard operating procedures for business processes or for executing controls (particularly manual controls). It might be unreasonable to expect every employee to perfectly execute every business process and every control every time. The question becomes: What is the impact of those failures individually and/or in the aggregate?

Controls, except for possibly automated controls, may suffer from atrophy. Such a state could develop because employees get careless with manual or IT-dependent controls, and thus, they become less effective.

It could be that, because of external circumstances, business processes have changed and the needs of the system have changed, but the system of business processes and/or controls has not changed and is now becoming less effective. Even automated controls can suffer from atrophy as a result of updates to IT, vulnerabilities that develop and other similar issues.

An IT example would be access rights. It is not uncommon for an investigation of access rights to reveal a host of risk issues. For example, all IT personnel are sometimes granted administrator rights to keep support simple. However, that is a serious violation of best practices and introduces a high risk factor. The same could be said for database administrator rights. In fact, access rights in general sometimes lack a least-privilege approach.

Another group of dangers could be described as: things that are that should not be. These can be seen as a failure to properly carry out the authorized procedures or controls. A good IT example involves the testing of new technologies, especially applications, where an employee is given elevated access rights for the testing, but once testing is completed, the elevated access rights are not returned to the proper level. Thus, the employee now has access rights greater than he/she should have.

A similar situation exists when employees are terminated. Access rights for a terminated employee should be concluded in correlation to that person's date of termination.[1] Deleting access rights for terminated employees is an area of concern in all IT audits where access rights are in scope.

A third category or group of dangers is nefarious activities. Unfortunately, human nature is such that the business community will never successfully eliminate nefarious activities. In fact, the opposite is true today. Never before has there been more risk, more nefarious activities, more cybersecurity issues than today. Just a casual reading of news

or professional literature reveals the common concern in business related to cybercrime and cybersecurity. The greatest threat today comes from the millions of potential intruders who can gain unauthorized access to an entity's system and databases, combined with the vector of spear phishing, and the level of IT expertise possessed by the modern, sophisticated cybercriminal.

There is also the possibility of an entity's own employees conducting malicious or nefarious activities against the employer. For instance, in one IT audit, the IT auditor discovered that a key senior manager had managed to edit the login application and have the login credentials bypassed (if-then-else statement, where if employee # = key manager, skip login). This is an example of a backdoor that allows the intruder access to a wide variety of applications and data. Worse, this situation is not some accident or oversight or poor execution of procedures and controls; it is purposeful and likely intended to conduct harmful activity against the entity.

CONCLUSION

Inquiry has a lot of advantages in an IT audit and has been successfully used millions of times for millions of audits. However, the IT auditor should take into account a couple of factors that can mitigate the reliance upon inquiry evidence. First, care should be taken in the nature of the inquiry—a questionnaire vs. an interview. Second, the IT auditor should take into account factors that could reduce reliance on inquiry evidence (see **figure 3**). But, in the end, it is similar to what auditors have done since the beginning of audits: Collect the evidence, make sure the evidence is reliable and draw audit conclusions. The slippery issues are those about mistakenly relying on inquiry when, with some careful thought, the IT auditor could search out corroborating, or superior, evidence.

ENDNOTE

[1] Sometimes entities will grant the terminated employee access rights to the entity's email for some period of time in order to transition the contacts and sources of email.

Five Questions With...

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA

With extensive experience across the Queensland, Australia, public sector, Tony Hayes is the deputy director-general of the Department of Communities, Child Safety and Disability Services in the Queensland Government, Australia. He has worked on various whole of government projects, change management initiatives, task forces and in-line management positions in many departments in the Queensland Government.

For 11 years, Hayes has also held a number of senior appointments with the Certified Practising Accountants of Australia as a member and national chair of the Information Management and Technology Centre of Excellence. In 2003, he was appointed to the Board of ISACA and the IT Governance Institute (ITGI) and has served on ISACA's Finance Committee and Strategy Advisory Committee.

Hayes is also an adjunct professor and a member of the Business Information Systems Advisory Committee for the School of Business at the University of Queensland.

When not working, Hayes enjoys spending time with his family. His passions include surfing (or anything on the beach for that matter), cooking, gardening and exercise.

With the new challenge as the 2013-14 ISACA international president, Hayes looks forward to working with all board and committee members, chapters and volunteers to begin the delivery of ISACA Strategy 2022 initiatives and ensuring ISACA's place as the global thought leader promoting trust in and value from information and information systems.

Q **As ISACA's incoming international president and the deputy director-general of the Department of Communities, Child Safety and Disability Services in the Queensland Government, Australia, how do you see ISACA growing and adapting to the constantly changing marketplace and needs of its constituents over the next year?**

A Strategy 2022 (S22) provides ISACA with a 10-year aspirational vision for our current and future members, strategic relationships with other associations and enterprises, as well as how we need to continually look at our service delivery going forward.

As a result, S22 provides us with a vision for what I often say are the 'lights on the hill'. Therefore, implementation of the various strategies, projects and initiatives of S22 will ensure ISACA is well positioned and respected as the global thought-leading organisation that promotes trust in and value from information and information systems.

S22 will not be delivered all at once, as each strategy and initiative has been staged and sequenced over the 10-year period to enable proper consideration of costs and benefits and ensure that decisions are well informed by membership and market needs, particularly as each new year will present new technology challenges and opportunities.

Q **Having recently started your new position as deputy director-general of the Department of Communities, Child Safety and Disability Services, please tell us about your new role and responsibilities. What in your past experience best prepared you for this position?**

A After having been in the role of associate director-general of the Department of Communities for the last three years, where I was the senior executive responsible for all service delivery for this agency across the state of Queensland, an opportunity presented to take on this time-limited role to lead a number of major service delivery reforms.

My new role as deputy director-general (projects and reform) is a great opportunity to lead a concentrated effort to change our approach to service delivery on a number of fronts. With significant government priorities to address inefficiencies, reduce costs, ensure that services are more contestable with the broader marketplace and position the state for various national reforms in human services, it was very attractive to me to be involved in these leading-edge initiatives.

Critical in the planning and delivery of these reforms is the provision of quality information sourced from a number of IT platforms. Monitoring our progress and achievement of the key elements of the business case, along with strong programme and project management and governance, will be fundamental to success.

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:

Throughout my career I have been involved in many change management and reform initiatives that have seen new business processes and alternative ways of delivering services to clients internal and external to government. My history as an audit executive responsible for IT, operational/efficiency, financial/compliance and risk audits has been invaluable as a foundation before taking up senior executive roles in corporate and resource management, including oversight over roles equivalent to chief information officer (CIO) and chief financial officer (CFO) in very large enterprises.

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

A Each of these roles has a common base or foundation—that is, the product produced in almost all instances is advice. So, for me, the biggest risk facing these professionals is not the tools or frameworks or methodologies utilised but rather how much notice the board or senior executives take of this advice. The connection and access to senior executives and the way messages are relayed to senior groups by professionals is critical.

My observation is that this is still a challenge for many enterprises as some senior executives do not understand the enormous benefits and utility that can be obtained by understanding and acting on the advice provided by these professionals. Equally, it is incumbent upon the professionals to deliver their services in a manner that garners confidence, trust and value.

So, in summary, building relationships and delivering a highly professional service that is respected and valued by your enterprise is as important as, or maybe more important than, anything else.

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 Being a member of and holding certifications from professional associations such as ISACA have been and continue to be very important to me as I have progressed through the ranks of my audit experience to various senior executive roles. Having up-to-date knowledge of the latest trends, approaches, methods and frameworks always helps to broaden your knowledge base and experience—whether you provide advice or are the recipient of advice and/or the decision maker.

The information and information technology industries worldwide have grown up and matured with their fair share of problems, budget blowouts, time overruns and, in some cases, disasters. However, it must be said that some of the greatest business success stories have also come about through the sound use of information and information technology.

So, for me, it is important that professionals in this area are credible, respected and come with having achieved certain standards and certifications relevant to their professional offering. ISACA credentials and certifications are truly global and are a statement that differentiates true information and information technology professionals from the others.

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

A I can reference many significant and complex projects, reforms and change management initiatives, most of which were enabled by information and information technology. However, the biggest challenge facing us all is getting balance in our lives. I often talk to staff and sometimes university graduates about this very important topic.

I am committed to ensuring a constant balance and adjustment among the most important issues in our lives: maintaining personal relationships, particularly family, professional networks and associations; keeping up to date with your body of knowledge, whatever that might be; and having some time for your well-being emotionally and physically.

> "The biggest challenge facing us all is getting balance in our lives."

That said, the most important issue is knowing when those are out of sync and doing something about it. If this is not recognised, eventually something will come unstuck and all of these balancing items will be affected in some way. Getting the balance is not just the province of senior executives, but it is a priority for everyone to ensure that you can deliver as a professional in your chosen area or specialty.

Feature

Risk and Compliance—For Better or Worse?

Torsten George is vice president of worldwide marketing and products at integrated risk management vendor Agiliance. He also oversees the company's training and technical support groups. George has more than 20 years of global information security experience. He is a frequent speaker on compliance and security risk management strategies worldwide and regularly provides commentary and bylined articles for media outlets covering topics such as data breaches, incident response best practices and cybersecurity strategies. George has held executive-level positions with ActivIdentity (now part of HID® Global, an ASSA ABLOY™ Group brand), Digital Link and Everdream Corporation (now part of Dell).

In today's business environment, many companies are required to comply with multiple industry and government mandates that govern IT security. Being in compliance does not equal being secure. So, what is the relationship among IT security, risk management and regulatory compliance? Can security be improved by shifting from a compliance-driven to risk-based approach?

MARKET DYNAMICS

Compliance with government standards and industry regulations is at the top of a lengthy list of IT security priorities. Unfortunately, the majority of organizations are still using a check-box mentality as part of a compliance-driven approach to security. This method achieves point-in-time compliance certification rather than an improvement of the company's security posture.

The Council of Europe Convention on Cybercrime; emerging legislation in the US, such as the National Institute of Standards and Technology (NIST)'s SP 800-137, the Federal Information Security Management Act (FISMA) of 2002, the Federal Risk and Authorization Management Program (FedRAMP), the Securities and Exchange Commission (SEC) Cyber Guidance, and the formerly proposed Cyber Security Act of 2012; and enforcement of existing regulations by the US Office of the Comptroller of the Currency Regulation Enforcement and the the US Federal Trade Commission (FTC) case against the Wyndham Hotel Group are forcing organizations to rethink the check-box approach. The Wyndham Hotel Group believed that its audit reports would recuse it from having to implement appropriate security controls to protect its customers' data. To steer organizations away from using industry regulations or government regulations as an excuse to take shortcuts, more and more compliance mandates demand better risk management. A good example is the Payment Card Industry Data Security Standard (PCI DSS), which in its second revision introduced the concept of risk correlation associated with prioritization of remediation actions[1] and evidence collection.

The bitter truth is that one can schedule an audit, but one cannot schedule a cyberattack. As a result, organizations have to find ways to streamline governance processes, continuously monitor compliance and their security posture, and correlate these activities to business criticality. By doing so, businesses can create a closed-loop process that encompasses the definition, evaluation, remediation and analysis of an organization's risk posture on an ongoing basis.

SECURITY: THE HOLY GRAIL?

When it comes to determining an organization's security posture, it is a commonly held belief that performing vulnerability management will address any exploits and minimize the risk of a data breach. However, without putting vulnerabilities into the context of the risk associated with them, organizations often misalign their remediation resources. This is not only a waste of money, but more important, it creates a longer window of opportunity for hackers to exploit critical vulnerabilities. At the end of the day, the ultimate goal is to shorten the window attackers have to exploit a software flaw. Therefore, even vulnerability management needs to be supplemented by a holistic, risk-based approach to security, which considers factors such as threats, reachability, the organization's compliance posture and business impact.

Without a threat, the vulnerability cannot be exploited.

Another limitation is reachability—if the threat cannot reach the vulnerability, the associated risk is either reduced or eliminated.

In this context, an organization's compliance posture plays an essential role, as compensating controls can be leveraged to prevent threats from reaching their target. According to the Verizon *2012 Data Breach Investigations Report*, 97 percent of the 855 incidents reported in 2011 were avoidable through simple or intermediate controls.[2] This illustrates the importance of compensating controls in the context of cybersecurity.

RISK: SECURITY'S NEW COMPLIANCE

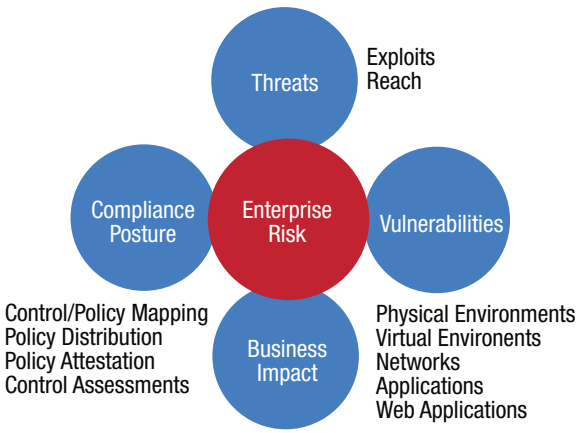
Another factor in determining the actual risk posed by a vulnerability is business impact. Vulnerabilities that threaten critical business assets represent a far higher risk than those that are associated with less-critical business assets.

Altogether, an organization's focus should be on risk and not just security.

To gain insight into their risk posture, organizations must go beyond assessing compliance by taking threats and vulnerabilities as well as business impact into account (see **figure 1**). Only a combination of these three factors assures a holistic view of risk. Compliance posture is typically not tied to the business criticality of assets. Instead, compensating controls are applied generically and tested accordingly. Without a clear understanding of the business criticality that an asset represents to an organization, an organization is unable to prioritize remediation efforts. A risk-driven approach addresses both security posture and business impact to increase operational efficiency, improve assessment accuracy, reduce attack surfaces and improve investment decision-making.

In general, there are four different approaches enterprises can use to tackle security (see **figure 2**).

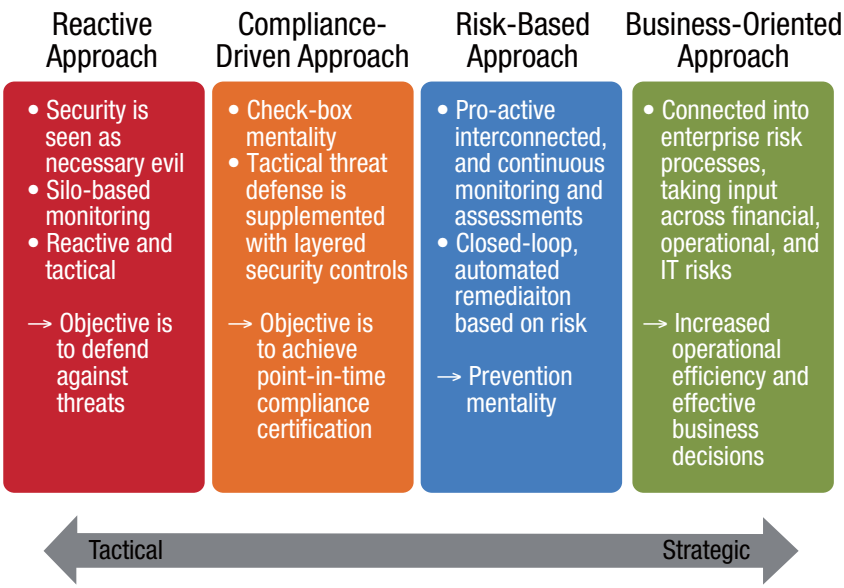
Figure 1—A Holistic View of Risk



Source: Agiliance Inc. Reprinted with permission.

The first concept was prevalent in the 1990s and can be best described as a *reactive approach*, whereby security is seen as a necessary evil. In this approach, silo-based point products are leveraged to monitor the company's security posture. However, the usage of these tools is primarily of a reactive and tactical nature.

Figure 2—Risk: Security's New Compliance



Source: Agiliance Inc. Reprinted with permission.

Once the frequency of data breaches increased and consumer interests were threatened, industry standards and government regulations were introduced and forced a *compliance-driven approach* to security. Here the objective is to achieve point-in-time compliance certification, whereby the tactical reactive approach is supplemented with layered security controls. Since many regulations and industry standards lack the notion of continuous monitoring, many enterprises using this approach adopt a check-box mentality and implement minimum requirements to pass the annual certification audits.

The rising tide of insider and advanced persistent threats, mounting regulatory pressure

and the impact of big security data on an organization's operational efficiency have led many progressive organizations to adopt either a risk-based or business-oriented approach to security. A *risk-based approach* to security assumes a prevention mentality, taking a proactive approach by interconnecting otherwise silo-based security and IT tools and continuously monitoring and assessing the data.

A *business-oriented approach* extends the risk-based approach by connecting into enterprise risk processes, taking input across financial, operational and IT risk factors. The ultimate goal is increased operational efficiency and effective business decision making.

ELEMENTS OF RISK-BASED SECURITY

In general, there are three major elements of a risk-based approach to security: continuous compliance, continuous (security) monitoring, and closed-loop, risk-based remediation.

Continuous compliance includes the reconciliation of assets and automation of data classification, alignment of technical controls, automation of compliance testing, deployment of assessment surveys and automation of data consolidation. When conducting continuous compliance, organizations can reduce overlap by leveraging a common control framework, increase accuracy in data collection and data analysis, and reduce redundant as well as manual, labor-intensive efforts by up to 75 percent.[3]

Applying *continuous (security) monitoring* implies an increased frequency of data assessments (e.g., on a weekly basis) and requires security data automation (see **figure 3**) by aggregating and normalizing data from a variety of sources such as security information and event management (SIEM), asset management, threat feeds and vulnerability scanners. In turn, organizations can reduce costs by unifying solutions, streamlining processes, creating situational awareness to expose exploits and threats in a timely manner, and gathering historic trend data, which can assist in predictive security.

Last, *closed-loop, risk-based remediation* leverages subject matter experts within business units to define a risk catalog and risk tolerance (see **figure 4**). At the same time, a closed-loop, risk-based remediation process entails asset classification to define business criticality, continuous scoring to enable risk-based prioritization, and closed-loop tracking and measurement. By establishing a continuous review loop of existing assets, people, processes, potential risk and possible threats, organizations can dramatically increase operational efficiency, while improving collaboration among business, security and IT operations. This enables security efforts to be measured and made tangible (e.g., time to resolution, investment in security operations personnel, purchases of additional security tools).

Figure 3—Elements of Security Automation in Accordance With NIST

Source: Agiliance Inc. Reprinted with permission.

BENEFITS OF RISK-BASED SECURITY

By leveraging a risk-based approach to security, progressive organizations can reduce risk, reduce costs, improve response readiness and increase risk-posture visibility. A good example is Fiserv, a company that serves the financial services industry with a broad spectrum of payment and account processing solutions such as transaction processing, electronic bill payment and presentment, business process outsourcing, and document distribution services. Fiserv uses a risk-based approach to security[4] and dynamically aggregates and correlates financial, operational and IT key risk indicators (KRIs) from multiple and diverse controls to detect system vulnerabilities so identified risk can be effectively mitigated. This approach has resulted in a reduction of the time it takes to produce risk profiles from six to three months, resulting in efficiency savings

of up to US $500,000. Furthermore, Fiserv was able to save US $1 million in overhead expenses by automating risk assessment efforts while at the same time shortening the policy control process from four to two months, saving an additional US $200,000. In addition, Fiserv achieved increased credibility with its board, management and regulators.

CONCLUSION

Cyberattacks can occur any time—so a solely compliance-driven approach to security is no longer effective. Instead, a risk-based approach to security as recommendedby NIST in SP 800-137 (among others) is the best approach.

When applying a risk-based approach to security, organizations must automate many otherwise manual, labor-intensive tasks. This, in turn, results in tremendous time and cost savings, reduced risk, improved response readiness, and increased risk-posture visibility.

[1] PCI Security Standards Council, *Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0*, October 2010

[2] Verizon, *2012 Data Breach Investigations Report*, A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Policy, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service, April 2012

[3] Agiliance, "Managing Security Risk for NERC/FERC Compliance," Case Study Results, 2010

[4] *CSO Magazine*, "GRC's ROI: Fiserv Gets a Handle on Governance, Risk and Compliance," April 2012

Figure 4—Closed-loop, Risk-based Remediation

Source: Agiliance Inc. Reprinted with permission.

Man in the Browser—A Threat to Online Banking

Dauda Sule, CISA, is the marketing manager at Audit Associates Ltd., a consultancy firm that specializes in designing and organizing training programs pertaining to auditing, fraud detection and prevention, information security and assurance, and anti-money laundering. Sule has five years of experience in the Nigerian banking industry and as a systems security and assurance supervisor at Gtech Computers.

The popularity of online banking has been on the rise. In 2005, Bob Sullivan of MSNBC quoted research figures from the Pew Internet and American Life Project, which showed that 53 million US citizens were banking online in 2004, and that online banking was the fastest growing Internet activity.[1] Now about eight years later, the customers subscribing to online banking services have increased worldwide—accompanied by threats and vulnerabilities. Hackers, fraudsters and other individuals with malicious intentions present numerous threats to online banking. These adversaries have led banks to adopt security countermeasures. Countermeasures adopted include (but are not limited to): ensuring that customers use strong passwords, providing virtual keyboards for entering login passwords, Secure Sockets Layer (SSL) encryption, sending customers information on how to avoid falling prey to malicious attackers and implementing two-factor authentication. One method adopted by adversaries to counter banks' security measures for online banking is man-in-the-browser (MITB) attacks, which can grant success to an attacker despite the aforementioned countermeasures, especially two-factor authentication.

TWO-FACTOR AUTHENTICATION

Many individuals have come to view two-factor authentication—the use of tokens and one-time passwords (OTPs)—as the ultimate solution in online banking security measures, a sort of holy grail for online banking security. Why is that so?

Fraud figures decreased significantly with the advent of two-factor authentication.[2] A hacker, for example, might be able to crack a customer's login password, regardless of its strength, using commonly available tools, or could obtain login credentials through spear phishing, but if a token is required to effect a transaction, hackers would be unable to proceed unless they are in possession of the token. In the case of OTPs being received as a text message (via SMS) on a customer's mobile phone, the hacker would have to have access to the mobile phone as well. (A hacker could also hack into the mobile phone; however, the probability is low that this type of attack would be used.) Hence, two-factor authentication has resulted in a significant reduction in the possibility of fraud being successful—providing a feeling of security for both the bank and the customer.

Then, MITB attacks came along.

MAN-IN-THE-BROWSER ATTACKS

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] Malware, especially Trojans, is used to infect the browser. The malware is normally installed when a user clicks on an applet on a web site that he/she is duped into clicking because it claims that an update or other similar action is needed.[4]

MITB malware is mostly undetectable by current antivirus software, although it may be detected if protection levels are set very high, which would also inhibit many innocuous programs. MITB modifies a user's content when an online banking site is visited by adding extra fields to the page in order to compromise second authentication mechanisms.[5] In an MITB attack, the customer initiates a transaction, the attacker modifies the transaction using compromised credentials, the extra fields added by the malware alert the attacker and give the hacker control of the online banking interface, consequently manipulating the statement and account balance to reflect the customer's intended transaction. Once the user uses a token to generate an OTP or receives it in a text message, the user enters the code and unknowingly authorizes the manipulated transaction thinking it was the correct one.

An illustration[6] of this scenario is the fictional Mr. Ojo who, with a balance of US $2,500 in his account, logs into his bank's online banking site to make a transfer of US $500 to his wife, who holds account number 12345. An MITB

attacker intercepts the transaction and transfers US $2,000 to an accomplice, who has account number 54321. Data are manipulated to show the customer that he is transferring US $500 to account 12345 and the balance left in his account is US $2,000. To complete the transaction, Ojo needs to enter the OTP sent to his mobile phone; when completed, his online banking dashboard shows that he has successfully transferred US $500 to account 12345 and his balance is US $2,000. He receives an SMS alert to that effect, and his month-end statement says the same. Unfortunately, in reality, Ojo authorized a transfer of US $2,000 to account 54321 and his available balance is US $500.

MITB attacks are expensive to carry out; therefore, they are usually performed by well-funded and organized criminals.[7] These criminals mostly target corporate account holders with high-volume transactions.[8]

MITB MITIGANTS

There are various methods for combating MITB attacks. The most effective weapons against MITB attacks are education and awareness. For example, MITB malware often requests logon credentials and a second-factor authentication mechanism to "train a new security feature" in order to compromise an account.[9] Banks should inform their customers not to pay heed to such requests or seek further clarification from the bank before clicking on such a pop-up request. Customers should also generally avoid clicking update requests for any software without confirming the genuineness of such prompts. Some telltale signs of an MITB attack in progress include transactions taking longer than usual, a system slowing down and logon credentials being requested where they were not before.[10]

Another 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 to be consummated and requiring a confirmation within the next few minutes to accept it. It may be that the confirmation message comes with the OTP and entering the OTP is the way to confirm that the transaction is good. In the case of customer Ojo, he would receive an SMS with the OTP stating that he is about to transfer the sum of US $2,000 to (the hacker's accomplice's) account 54321. This would alert Ojo of the fact that something is wrong, and he can then stop the transaction and report it to his bank. However, this measure would be at risk if the attacker also compromises the customer's mobile phone and modifies the confirmation message that would enable the customer to complete the transaction. Additionally, the attacker may also modify the confirmation message by means of the malware, as he did the statement and balance on the account.

Behavioral pattern monitoring can also provide an adequate deterrent to the success of MITB attacks. This involves server-side monitoring of customers' transactions. Changes in the normal pattern of transacting, location within a session (e.g., change in IP address) or having multiple sessions within a very short time frame are possible indications of a criminal action, at which time the bank would hold the transaction and alert the customer of the possible compromise.[11] Criminals and other malicious individuals are always developing means to ensure that they are at least one step ahead of their targets; therefore, there is a need for constant monitoring and testing to avoid having that gap in any transaction.

CONCLUSION

A combination of customer education and awareness, use of confirmation alerts, and behavioral monitoring can provide an effective protection from MITB attacks and provide some margin of safety for online banking. These suggested measures of facing MITB are, by no means, exhaustive or infallible; other viable solutions are available.

> "The first line of defense remains awareness."

Further research can be performed by banks and information security experts to solve the problem and ensure better protection against MITB attacks. The first line of defense remains awareness: banks educating their customers to avoid clicking on unusual requests claiming to be required for some form of update or the other. Customers should always seek clarification from their banks when they observe something different from what they are used to in their online

banking interface. They should also raise alarms if their online banking transactions appear to be taking longer than usual to consummate, as this could be an indication that an MITB attack is in progress.

For their part, banks should also be more observant of customer transactions by closely monitoring behavioral patterns of customer transactions. This would enable them to track down any anomalies. Summarily, extra vigilance by both customers and banks can go a long way in mitigating against MITB attacks on online banking transactions.

REFERENCES

EMC Corporation, "*RSA Offers Advanced Solutions to Help Combat Man-In-The-Browser Attacks*," USA, 2010, *www.rsa.com/press_release.aspx?id=10943*

Beaver, K.; J. Shaw; *Multifactor Authentication for Dummies*, Quest Software Edition, Wiley Publishing Inc., USA, 2011

Chickowski, Ericka; "Man in the Mobile Attacks Highlight Weaknesses in Out-of-band Authentication," 2010, *www.darkreading.com/authentication/167901072/security/application-security/227700141/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication.html*

PR Newswire, "Winning the Fight Against Man-in-the-Browser—Entrust IndentityGuard Mobile Now Available," 2012, *www.prnewswire.com/news-releases/winning-the-fight-against-man-in-the-browser---entrust-identityguard-mobile-now-available-100753374.html*

HSBC India, "Online Security," 2012, *www.hsbc.co.in/1/2/personal/internet-and-self-service-banking/online-security*

Informa PLC, "HSBC's New OTP Device for Online Banking Customers," Banking Technology, 2011, *www.bankingtech.com/bankingtech/article.do?articleid=20000201121*

Moskalyuk, A.; "Online Banking Usage Highest Among 18-24 year olds," 2012, *www.zdnet.com/blog/itfacts/online-banking-usage-highest-among-18-24-year-olds/8606*

Owen, Nick; "Does Two-factor Authentication Need Fixing?," 2012, *www.infosecisland.com/blogview/21827-Does-Two-Factor-Authentication-Need-Fixing.html*

Sengupta, Somini; "Computer Scientists Break Security Token in Record Time," 2012, *http://bits.blogs.nytimes.com/2012/06/25/computer-scientists-break-security-token-key-in-record-time/*

Sharp, John C.; "Man in the Browser Attacks—Worse Than Viruses?," 2008, *http://authentium.blogspot.com/2008/06/man-in-browser-attacks-worse-than.html*

ENDNOTES

[1] Sullivan, Robert; "Click! Online Banking Usage Soars," MSNBC.com, 2005, *www.msnbc.msn.com/id/6936297/ns/business-online_banking/t/click-online-banking-usage-soars/#.T_f1KbXZCV8*

[2] Kelly, Spencer; "Hackers Outwit Online Banking Security Systems," BBC.com, 2012, *www.bbc.com/news/technology-16812064*

[3] TriCipher Inc, "Threats: Man in the Browser," 2009, *www.tricipher.com/threats/man_in_the_browser.html*

[4] Sharp, John. C.; "Man in the Browser Attacks—Worse Than Viruses?,"2008, *http://authentium.blogspot.com/2008/06/man-in-browser-attacks-worse-than.html*

[5] Prince, B.; "Understanding Man-in-the-Browser Attacks Targeting Online Banks," 2010, *http://securitywatch.eweek.com/exploits_and_attacks/understanding_man-in-the-browser_attacks.html*

[6] The illustration is entirely fictitious; names and figures used do not refer to any existing people.

[7] Rouse, Margaret; glossary, SearchSecurity.com, 2006, *http://searchsecurity.techtarget.com/definition/man-in-the-browser*

[8] Entrust Inc., "Defeating Man-in-the-Browser: How to Prevent the Latest Malware Attacks Against Consumer and Corporate Banking," 2010, *http://docs.bankinfosecurity.com/files/whitepapers/pdf/315_WP_MITB_March2010.pdf*

[9] Tarantola, Andrew; "New 'Man in the Browser' Attack Bypasses Banks' Two-factor Authentication Systems," 2012, *http://gizmodo.com/5882888/new-man-in-the-browser-attack-bypasses-banks-two+factor-authentication-systems*

[10] *Op cit*, Kelly

[11] *Op cit,* Entrust Inc.

Navigating the Path From Information Security Practitioner to Professional

Kerry Anderson, CISA, CISM, CRISC, CGEIT, CCSA, CFE, CISSP, CSSLP, ISSAP, ISSMP, is an information security and electronic records management consultant with more than 15 years of experience in information security. Anderson has spoken at numerous events and authored articles for industry journals. She is an adjunct professor in Clark University's Cyber Security Graduate Program (Worcester, Massachusetts, USA).

"I am an information security practitioner, not an information security professional." There is a profound difference between the two. A practitioner is defined as "one who practices something, especially an occupation, profession or technique." A professional is defined as "a skilled practitioner; an expert."[1] The principal differentiators between the two terms are the degree of experience and knowledge. In an ideal situation, practitioners would progress from one level to another after acquiring specific expertise in each successive position or assignment. Unfortunately, developing core competencies is often not a linear process. It may require some proactive effort on the part of the practitioner to gain the necessary expertise for the desired career objectives.

To pursue a career in information security, practitioners need to acquire core competencies in specific areas. The core competencies required for a profession make up its competency model. It is the competency model and its pursuit that distinguish between a novice and an expert within a profession. The acquisition of core competencies is necessary to advance to the next level. This seems fundamental, but may be more difficult to accomplish because of increasing specialization within the information security profession.

An information security practitioner must acquire core competencies to develop a holistic perspective to effectively manage security within today's global and highly interconnected world. Core competencies develop at different career stages and include not just technical knowledge, but other skills required to become proficient within a profession. New information security specializations require not only strong competencies in core areas to manage the increasingly complex architectures, but acquisition of new competencies to remain relevant.

THE CORE COMPETENCY MAP

A map is an excellent model for career development. It provides mechanisms for setting a course and adjusting it as necessary due to unanticipated circumstances. There are four steps in a hypothetical core competency map (**figure 1**).

This process is reiterative for two reasons. The first is that information security exists within a dynamic technology environment; skills must be renewed to avoid career obsolescence. For

Figure 1—Core Competency Map

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:

example, many of the career options that are in demand today, such as cloud security engineer, did not exist a few years ago. The second reason is that the practitioner also exists within a dynamic environment. Career direction may need to evolve to accommodate changes in personal circumstances, interests or ambitions. Over the last few years, many practitioners have found it necessary to refine their careers.[2]

STEP 1: DETERMINE CURRENT CAREER PATH

The process starts with determining one's current career location. The basic premise is that people need to know where they are now to figure out how to get to the desired destination. Evaluating competency levels is critical. For newcomers to the security profession, this may be clear-cut; however, for individuals who are experienced or those making a career shift, this may require some time to determine the current mastery of specific core competencies.

STEP 2: DECIDE ON A MEDIUM- TO LONG-TERM CAREER GOAL

Individuals should devote some time and thought to determining where they see themselves going over the next five to 10 years by considering tough questions about interests, personal temperament and career challenges desired. This step often requires research to evaluate career options, including:

- Information interviews
- Labor projections

Figure 2—Information Security Proficiency Realms

Realm	Explanation
Security technology	This proficiency realm includes knowledge, skills and experience related to security technology. At the entry level, the focus is on developing a broad understanding with an emphasis on technical competency. At more advanced levels, experiences and skills meet specific expertise, such as access management, cryptography, operational management, application development, security architecture, communication (voice/data), personnel, and physical and environmental security.
People management	This proficiency realm includes knowledge, skills and experience related to effectively communicating information, influencing, persuading and negotiating agreements at all levels of an organization. Proficiency in this realm includes written and oral communications skills. All practitioners need to develop strong soft skills to communicate ideas, promote personal visibility, advance relationships, create support for initiatives and encourage behavioral changes to build a culture of security within the organization.
Risk management	This proficiency realm includes understanding, developing and managing a risk-based approach to information security programs. It includes proficiency in the identification, evaluation and remediation of risk, vulnerabilities and threats. Skills in this realm include risk analysis and identification of potential controls to mitigate identified risk. At the entry level, risk management is the internal focus. At higher levels, the practitioner incorporates external risk concerns, emerging technology risk vectors and third-party relationships.
Information technology	This proficiency realm includes knowledge, experience and skills related to the development, testing, implementation, management and decommissioning of applications and their supporting technical infrastructure. Competency in this realm includes working knowledge of hardware, software and networks, as well as their interrelationships. At lower proficiency tiers, IT skills revolve around specific technologies and involve operations. At higher proficiency levels, the level and scope of skills extend across multiple IT areas with increased attention on integration and risk management.
Information security management	This proficiency encompasses an understanding of security theory, principles, methodologies, compliance and governance. It provides the connectivity between technology and business functions required to manage the security risk inherent to the organization. This requires training and experience to apply security management to real-world situations. It is in this realm that many practitioners may transition into information security professionals. At the entry level, practitioners may apply well-documented techniques to manage common risk factors. Highly proficient professionals develop or adapt information security management techniques to emerging technologies or to a unique set of circumstances.

- Job trend predictions
- Survey of job postings to determine common position requirements

STEP 3: DEVELOP A PLAN

This step has two tasks. The first step is to determine one's existing skill set and experience. The next is to develop a strategy to acquire the necessary proficiencies to prepare for a desired career objective. The objective is to be prepared to assume career opportunities when they emerge. To quote Benjamin Disraeli, "One secret of success in life is for a [person] to be ready for [his/her] opportunity when it comes."[3]

Task 1: Assess Proficiency

This involves making a determination of competency levels against the proficiencies necessary to move to the next career step. The discrepancy between existing skills and knowledge level and the suggested proficiency level represents a gap in competency within an area. A simple approach might be to gauge proficiency using years of experience based on four categories:[4]

- **Entry-level practitioner**—Three or less years of information security experience
- **Mid-level practitioner**—Four to seven years of information security experience
- **Senior-level practitioner**—Eight to 10 years of information security experience
- **Executive/expert professional**—10-plus years of information security experience

These levels indicate the amount of skill or experience a practitioner has pertinent to a specific domain and represent an increase in responsibilities from the entry-level practitioner to the executive/expert professional.[5] The information security proficiency realms are identified in **figure 2**.

Task 2: Strategize How to Create a Proficiency Acquisition Plan

The objective of this task is developing a strategy to acquire the necessary mastery in each proficiency realm to overcome core competency gaps that would prevent the individual from achieving the desired job role. This allows practitioners to concentrate on professional development activities that best suit their career objectives. It is important to understand that there is no right way to pursue desired skills, experience or knowledge. Developing a personalized plan is dependent upon the experience, training and education of the individual involved. Depending on the job level, career track, specialization and position objective of the individual creating the plan, different proficiency acquisition strategies might provide the appropriate vehicle for professional development. Any plan should:

- Identify proficiency gaps between current core competency levels and those essential to attaining the next progressive rung on the individual's career ladder
- Provide a communication vehicle for career-planning discussions
- Offer different options for acquiring the required skills and experience

There are different channels to closing the identified gaps between current and desired proficiency levels. The decision on how to close the gap is based on the individual's needs and other attributes for the various development alternatives, which include:

- Costs of the development option
- Depth of proficiency desired (basic familiarity or different levels of expertise)
- Time frame to complete
- Availability of reimbursement or financial assistance from the employer
- Work schedule
- Travel to participate in development option

Gaining specific expertise, especially in highly technical domains, may require a combination of multiple options to acquire a specific proficiency. Some alternative ways to close the proficiency gap include:

- **Professional certification**—Studies have shown a continuing trend toward higher salaries for certified IT security professionals.[6] Different studies have shown various security-related certifications as being among the highest paying IT certifications.[7,8] The requirement or preference for certified practitioners is frequently found in position postings.[9] It is no accident that certification appears to be the top development choice for many practitioners, specifically the Certified Information Systems Auditor® (CISA®) and Certified Information Systems Security Professional (CISSP). Practitioners may want to do a broader survey of available certifications beyond the best-known options and consider more focused certifications based on their career objectives and experience. Certifications in governance, secure development, forensics and fraud are just a few of the

alternative certification focus areas currently available that offer practitioners an opportunity to focus on specific career paths. Some certifications offer growth path by providing additional concentrations on top of the basic certification to allow practitioners to distinguish themselves in a particular security practice area.Some practitioners are electing to combine certifications, such as vendor and traditional security certifications, to differentiate themselves as a "renaissance security professional."[10] Coined by J.J. Thompson, this term describes information professionals who have attained a set of well-rounded skills that include a variety of business and technical knowledge and experience. Diane Morello, a Gartner vice president, called this a "hybrid professional."[11] According to Morello, the hybrid professional emerged because the "intersection of business models and IT requires people with varied experience, professional versatility, multidiscipline knowledge and technology understanding." According to Forrester's white paper, "The Evolving Security Organization," the hybrid professional role allows information security practitioners to emerge from the siloed role to become business facilitators.[12]

- **Advanced academic options**—At a number of chief information security officer (CISO) summits,[13] participants have discussed advanced academic degrees as a professional development option. In 2003, the US National Security Agency (NSA) and Department of Homeland Security (DHS) jointly created a program to promote advanced academic degrees with a focus on information security.[14] Over the last decade, the number and variety of these programs has flourished; however, practitioners should examine the different academic degree programs based upon their career aspirations. These programs offer a specific focus area or provide a generalized approach to the field of study. Another option to pursue is obtaining graduate degrees in business, finance or law to define a unique career path. The downside to academic alternatives is that they require a substantial commitment of both time and finances to pursue. Based on an informal survey of position postings, the requirement for graduate degrees is becoming a more common requirement or preference by employers for more senior jobs.
- **Self-study**—Many professional organizations and educational providers offer a myriad of self-study courses and materials. A lot of material is available online at a reasonable cost or free. In addition to these web-based programs, books remains a popular way for practitioners to acquire knowledge. The downside to this option may be documenting this approach to employers. Motivational speaker, Brian Tracy, recommends that professionals devote one hour a day to reading.[15]
- **Enhancing people skills**—Information security associates need people skills as a core competency to maintain career momentum and avoid a resume-generating event (RGE). People skills complement technical skills and build credibility with business counterparts. In speaking with senior information security professionals over the last 10 years, a common theme is the need for technically proficient practitioners to develop stronger communication skills, such as selling, negotiation and presenting. While there are many professional courses aimed at these objectives, some practitioners acquire these skills by getting outside of their comfort zones, such as presenting at conferences or teaching courses (internally and externally). Other options include sales training or public speaking groups.
- **On-the-job experience and mentoring**—Not all skills come from a book or classroom—sometimes there is no substitute for real-world experience. One of the best strategies for gaining the necessary proficiency is finding a mentor or subject matter expert (SME) to initially shadow and then work closely with to assume a larger part of the tasks required to do an assignment. A good example of this is learning to perform vendor security risk assessments. The apprentice may start out just accompanying a skilled auditor or risk assessor. In future engagements, apprentices may assume different tasks until they are ready to fly solo, with the mentor evaluating their professional competency. This strategy is equally applicable to information security professionals looking to refresh their skills or become acquainted with another way of approaching an assignment. Another excellent option is to assume a mentoring role for another practitioner.

STEP 4: DO REGULAR STATUS CHECKS

It is critical to assess progress. It is easy to get off course or to lose momentum as the workplace might carry us in unwanted directions. There are a few red flags to career path stagnation including the following:

- No further development of skills and abilities
- Being rarely selected for new teams or projects

- Losing that *joie de vivre* for the job
- Not engaging in any career development activity in more than a year
- Calculating days until retirement

While the economic downturn has negatively affected career development for many with more limited options for professional development due to reduced training budgets, it is essential, even in tough job markets, to remain relevant and current in a chosen endeavor, even if it is just by reading books or attending low-cost training opportunities. On a regular basis, such as every six months or annually, review progress against the plan and revise as necessary. Core competency development plans need to remain a vital and living document.

CONCLUSION

What does one make of the colleague with limited skills despite 20-plus years of experience? Some might say, "He has one year of experience repeated 20 times."[16]

Core competencies do not remain static, especially in technically focused fields like information security. One must never be finished learning. In his classic book *The Seven Habits of Highly Effective People*, Stephen Covey describes a habit called "sharpening the saw," which means to continually learn new things and acquire different experiences.[17] It is similar to the Japanese Kaizen improvement philosophy, which describes improvement or change for the better with focus upon continuous improvement of processes. Stephen Covey once said, "Begin with the end in mind."[18] This idea remains true. Information security practitioners and professionals always have the prerogative to adjust their desired career destination, and the core competency model described here can assist in altering the route to that end.

> "One must never be finished learning."

ENDNOTES

1 Merriam-Webster Dictionary, *www.merriam-webster.com*

2 Newman, Rick; *Rebounders: How Winners Pivot From Setback to Success*, 2012

3 BrainyQuote, *www.brainyquote.com/quotes/quotes/b/benjamindi130016.html*. Benjamin Disraeli (1804-81) was a British statesman.

4 These levels are based on the author's survey of job postings for information security positions.

5 This model was adapted from the ARMA Records and Information Management Core Competencies (2008), as well as the author's survey of job postings for information security positions.

6 Vijayan, Jaikumar; "Salary Premiums for Security Certifications Increasing, Study Shows," *ComputerWorld*, 9 July 2007, *www.computerworld.com/s/article/9026624/Salary_premiums_for_security_certifications_increasing_study_shows*

7 Muller, Randy; "15 Top Paying IT Certifications for 2012," Global Knowledge, January 2012, *www.globalknowledge.ca/articles/generic.asp?pageid=3159&country=Canada*

8 Gupta, Upasana; "Top 5 Certifications for 2012," GovInfoSecurity.com, 2 December 2011, *www.govinfosecurity.com/top-5-certifications-for-2012-a-4291/op-1*

9 Based on the author's own survey of position postings over the last few years

10 Bedell, Crystal; "The Renaissance Security Professional: Skills for the 21st Century," (ISC)²

11 Gartner, "Gartner Warns of a Looming IT Talent Shortage," 2008, *www.gartner.com/it/page.jsp?id=600009*

12 Kark, Khalid; Bill Nagel; *The Evolving Security Organization*, Forrester, 26 July 2007

13 The author has attended more than 50 security-focused events, including five CISO summits, at which the topic of professional development and advanced degrees were discussed.

14 National Security Agency, "National Centers of Academic Excellence," *www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml*

15 Tracy, Brian; "One Hour Makes All the Difference," *www.briantracy.com/blog/personal-success/one-hour-makes-all-the-difference/*

16 This quote is from the author's brother. The author found several references to similar quotes, including the recent book *Geeks, Geezers, and Googlization: How to Manage the Unprecedented Convergence of the Wired, the Tired, and Technology in the Workplace* by Ira S. Wolfe.

17 Covey, Stephen; *The Seven Habits of Highly Effective People*, Free Press, 1989

18 *Op cit*, Covey

Feature

Key Elements of an Information Risk Profile

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC. Pironti has designed and implemented enterprisewide electronic business solutions, information security and risk management and information technology strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key customers in numerous industries. He frequently provides briefings and acts as a trusted advisor to senior leaders of numerous organizations on information security and risk management and compliance topics and is also a member of a number of technical advisory boards for technology and services firms.

Information risk has become a top-of-mind issue for many business leaders and information risk management security (IRMS) professionals. Largely driven by a misunderstanding of each other's activities and motives, these two groups have historically had challenges interacting with each other. That is, business leaders recognize and embrace the need to take risk and often incent their constituents to take it as well in order to achieve business goals; conversely, IRMS professionals are charged with minimizing risk and ensuring their organization's information infrastructure and associated data assets are properly protected. The best way for these parties to reduce friction and meet their individual requirements is to mutually develop and maintain an information risk profile that they both can use to guide their respective activities.

An information risk profile documents the types, amounts and priority of information risk that an organization finds acceptable and unacceptable. This profile is developed collaboratively with numerous stakeholders throughout the organization, including business leaders, data and process owners, enterprise risk management, internal and external audit, legal, compliance, privacy, and IRMS.

ESTABLISHMENT OF DUE CARE

In the legal community due care can be defined as the effort made by an ordinarily prudent or reasonable party to avoid harm to another by taking circumstances into account.[1] When applied to IRMS, due care is often considered a technical compliance consideration and standards such as the Payment Card Industry Data Security Standards (PCI DSS) or National Institute of Standards and Technology (NIST) guidelines are often referenced. While these standards can be effective at providing broad guidance, an organization must develop its own view of due care and its own capability to implement and maintain skills to support this view. An information risk profile can be an invaluable tool to assist leaders and decision makers in establishing this guidance and effectively communicating their information and data risk appetite and expectations.

ALLOWING DECISION MAKERS TO MAKE DECISIONS

Typically, friction exists between decision makers and IRMS professionals due to their misperceptions of each other. Business leaders and decision makers often view IRMS requirements and professionals as obstacles in their path to success. At the same time, IRMS professionals often view business leaders and decision makers as individuals who are not informed enough to understand the value of their activities and the associated requirements. The detailing and documenting of the organization's information risk appetite and expectations remove the often-ubiquitous subjective assumptions that IRMS professionals use to guide their actions and activities.

IRMS professionals who effectively leverage the information risk profile now have a solid foundational tool. They can reference the information risk profile that was developed and endorsed by the organization's business leaders and decision makers. If IRMS professionals are effective in demonstrating their guidance and the actions align with the profile, the business leaders and decision makers are compelled to seriously consider them and either adjust the organization's information risk profile to accommodate the requests or modify their requirements to be in alignment. This creates an opportunity for IRMS professionals to engage in consultative and collaborative activities. Together, they can develop a plan that provides a positive outcome and meets requirements while still aligning with the organization's information risk management expectations.

LINKAGE TO ERM ACTIVITIES

Enterprise risk management (ERM) is an evolving and important concept within many

organizations and includes information risk management as one of its functions. The use of an information risk profile is often an effective way for traditional security professionals to integrate with this concept. The profile provides important insights and guidelines associated with information risk identification and management. The ERM function can then leverage this information as it calculates overall enterprise risk and develops control objectives and management practices to effectively monitor and manage it. The structure of the profile provides a framework that easily and logically organizes data for the organization to leverage as needed.

INFORMATION RISK PROFILE STRUCTURE

An organization's information risk profile should be structured and formatted in a fashion that quickly demonstrates its value and intent to the organization, is easily understood and applicable to the organization as a whole, and is viewed as useful and beneficial to its leaders and stakeholders. The following can be useful in meeting these goals.

Guiding Principles and Strategic Directives

An organization's information risk profile should include guiding principles aligned with both its strategic directives and the supporting activities of its IRMS program and capabilities. This information should be listed early in the profile to allow the reader to understand its context and intent. Common guiding principles include the following:

- Ensure availability of key business processes including associated data and capabilities.
- Provide accurate identification and evaluation of threats, vulnerabilities and their associated risk to allow business leaders and process owners to make informed risk management decisions.
- Ensure that appropriate risk-mitigating controls are implemented and functioning properly and align with the organization's established risk tolerances.
- Ensure that funding and resources are allocated efficiently to ensure the highest level of information risk mitigation.

Information Risk Profile Development

Transparency is a key aspect to the success and adoption of an information risk profile. The risk profile's accuracy and credibility may be called into question if the methods, practices, source materials and intelligence—as well as individuals involved in its development—are not provided as part of the document. This information can be referenced as part of an appendix to the document and include links to the materials themselves.

Business-state Representation of Information Risk

The information risk profile should include a current-state analysis of identified information risk factors that have a reasonably high probability of occurrence and would represent a material impact to business operations if realized. The descriptions of risk should be brief and expressed in language that is recognized and understood by both business- and technology-oriented personnel.

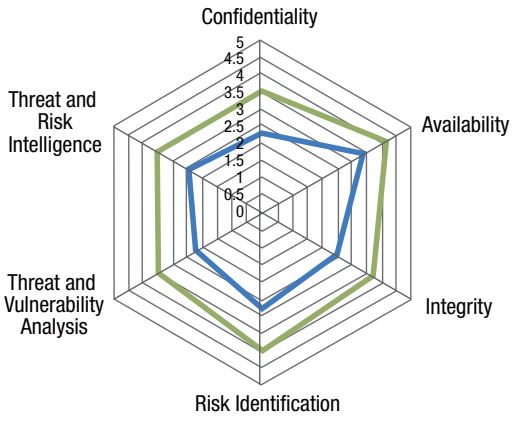
The current-state representation should also include the organization's IRM views, expectations and requirements. This should include identification and analysis of the opinions of business leaders and stakeholders and their views on information risk and security, a description of current business conditions, current threat and vulnerability analysis outcomes, and expectations of external parties (i.e., customers, partners, vendors, regulators). This can also assist in the development of future-state objectives and requirements.

Future-state Objectives and Requirements

The future-state objectives and requirements identify the ideal state of information risk management for the organization and general information risk appetite and tolerance. This includes key IRMS-related initiatives that are in progress or are soon to be initiated; their associated timelines for completion; and a brief summary of the initiative's owners, key dependencies, and expected level of information risk reduction at milestone points and at completion.

An effective way of evaluating and communicating the future-state objectives and requirements is to use a capability maturity model (CMM) approach. An assessment of key functions and capabilities for the current and future states using CMM can help an organization easily identify areas of required focus and investment for functions, capabilities and services that are required. Using a radar chart format (**figure 1**) to represent these data is an effective way of communicating the information and is easily understood by a broad audience.

Figure 1—CMM Radar Chart



Data Classification Levels and Designations
5—Confidential—restricted
4—Confidential—customer-or compliance-related
3—Proprietary
2—Internal use only
1—Public

Key Business Processes and Capabilities

Organizations often have numerous business processes and limited resources and bandwidth to protect them. It is important to identify the organization's key business processes and capabilities within the information risk profile—those that, if impacted negatively, could cause a material impact to the operations of the business. Often they can be separated into business support functions (i.e., payroll and benefits, messaging and communications, finance) and production (i.e., revenue generating, regulated, contractually required).

An easy but often overlooked source for a listing of these processes and capabilities is an organization's business continuity and/or disaster recovery plans. These plans typically include not only the key business processes, but also rank their level of importance to the organization. They also provide valuable insights into the recovery time and recovery point objectives that are often considered in risk calculations.

Key Data Elements

Key data elements that are identified and defined in the risk profile often include intellectual property, transaction data, financial data, nonpublic personal information, customer data, human resources information and other sensitive data assets. Defining the key data elements ensures users that the information risk profile provides a data dictionary that offers a clear understanding of the data element as well as its value to the organization.

Identification of Data Owners and Stakeholders

All data and information within an organization should be associated with a data owner and one or more stakeholders. Identifying and evaluating ownership attributes is important because the owners and stakeholders are responsible for their information risk management decisions. This activity can also assist in the identification of dependencies that can affect the risk appetite for data assets, especially in situations where they are required for one or more critical business functions or processes.

Identification of Business Value

The value of information is often misunderstood and based on subjective perceptions of data owners or evaluators instead of meaningful analysis and calculation. A basic principle of information risk management is that the cost to protect information should not exceed its value. To assess the value of information, it is often easier to identify, communicate and monitor the value of processes, rather than data assets. Processes can be attached to activities of the organization, such as revenue generation, core and general operations, and achievement of strategic business goals. The information risk profile does not need to quantify the exact value of data assets, but does need to establish a general representation of value to allow for the definition of appropriate levels of classification and control.

Data Classification Schema

To simplify information management, it is important to classify data into easily understood containers (see **figure 2**) associated with control objectives and requirements that identify data-handling requirements. This classification schema should be as simple as possible in order for it to be useful to the information risk profile and general activities of the organization.

The information risk profile should include the organization's data classification schema and a summary of the control requirements and objectives associated with it. It is recommended that data classification schemas contain between three and five levels of definition that contain

progressively stronger and more comprehensive control objectives and requirements as they ascend.

Figure 2—Data Classification	
Level	**Designation**
5	Confidential—restricted
4	Confidential—customer- or compliance-related
3	Proprietary
2	Internal use only
1	Public

Risk Levels and Categories

Risk levels and categories provide a framework that can be used to organize and communicate information risk in an easily recognizable format. Risk levels provide a scale to represent the level of material business impact that would result if a risk were to be realized. The categories help to define the type of impact that would likely materialize. To be useful, the levels and categories should be simple and easily understood.

The following are examples of information risk levels:

- **High**—Severe material compliance, legal and/or financial consequences; significant material impact on critical business processes and/or business operations; loss of customer trust and/or damage to brand reputation
- **Medium**—Significant material compliance, legal or financial consequences; substantial material impact on key business processes and/or business operations; weakened customer trust and/or brand reputation
- **Low**—Negligible to no material compliance, legal and/or financial consequences; minimal material impact on key business processes and/or operations; insignificant change in customer trust and/or brand reputation

The following are examples of information risk categories:

- **Confidentiality**—The disclosure of sensitive information to unauthorized individuals or systems
- **Integrity**—Impact to the accuracy and consistency of data and information
- **Availability**—Effect on the ability to access capabilities and associated data and information

By using this method of level setting and categorization, key business processes can then be presented in the form of a heat map (see **figure 3**) to visualize the associated information risk levels.

Figure 3—Current Information Risk Levels by Key Business Processes			
Key Business Processes	**Confidentiality**	**Integrity**	**Availability**
Payroll and benefits	High	High	High
Credit and collections	High	High	High
Web presence	High	High	Medium
Billing and receivables	Medium	Medium	Medium
Supply chain management	Medium	Medium	Low
Messaging and communications	Medium	Low	Low
Procurement and payables	Low	Low	Low

MATERIAL BUSINESS IMPACT CONSIDERATIONS

Material business impact considerations are a vital element of any information risk profile. They provide the equivalent to pain charts—commonly used in health care environments. A pain chart typically uses a numerical or graphical scale and allows a health care provider to understand the level of pain and discomfort that a patient is experiencing in order to respond with the appropriate level of care. In the information risk profile, the material business impact considerations identify the impact an incident or loss has in terms that are easily understandable and recognizable by the organization. These considerations should span a number of categories including financial, productivity, availability, reputation, compliance, partner and supply chain, and customer. Here are some example material business impact considerations for an organization that has annual revenues of US $500 million:

- **Financial:** An immediate and unplanned loss equal to or greater than the following list would represent a material business impact to the organization:

Material Business Impact	Financial Loss Amount
Catastrophic	US $100,000,000 and above
Major	US $5,000,000 to $99,999,999
Moderate	US $1,000,000 to $4,999,999
Minor	US $100,000 to $999,999
Negligible	Less than US $100,000

- **Productivity:** An immediate and unplanned loss of employee productivity equal to or greater than the following list would represent a material business impact to the organization:

Material Business Impact Category	Employee Productivity Percent Loss
Catastrophic	85% and above
Major	40 - 84%
Moderate	20 - 39%
Minor	10 - 19%
Negligible	1 - 9%

- **Availability:** An immediate complete or partial lack of availability of one or more key business processes and associated information assets and supporting systems would represent a material business impact to the organization:

Material Business Impact Category	Time of Unavailability (Partial or Full)
Catastrophic	8 days and beyond
Major	73 hours - 7 days
Moderate	9 - 72 hours
Minor	2 - 8 hours
Negligible	Less than 2 hours

IDENTIFIED KEY INFORMATION RISK AND MITIGATION CAPABILITIES

The identification of known key information risk and mitigation capabilities provides a high-level perspective on the current information risk posture of the organization. These change and evolve over time and should be revisited as part of the annual update cycle for the information risk profile. The following are examples of key information risk:

- Limited visibility into information infrastructure and sensitive data assets
- Minimal governance and compliance enforcement for third-party processing, storage and use of sensitive data assets
- Lack of a trust-but-verify control structure to limit impact of insider threats
- Limited capability to perform and maintain threat and vulnerability analysis of key business processes and activities
- Lack of a risk-conscious and security-aware culture
- Limited IRMS considerations in product and application development life cycle and technology operations
- Negligible information risk intelligence gathering, processing and communication capabilities

Examples of identified risk mitigation capabilities include:

- Expectation of employee adherence to IRMS policies and standards
- Basic technological security controls (e.g., firewall, intrusion detection, data encryption, antivirus)
- Insurance coverage of US $20 million to mitigate incident response and recovery costs for damage to information systems and data
- Basic business resiliency capabilities maintained (command and control, incident response, business continuity, disaster recovery), reducing the impact if a risk is realized

Individually, these data points provide limited value to the organization. When they are assembled together, properly endorsed and kept current, they can provide a holistic view of the organization's perspective associated with information risk management.

ENDORSEMENT AND UPDATES

For the information risk profile to be meaningful to the organization, its leadership and stakeholders must agree upon and endorse it. It is important to identify in the document who endorsed the profile and when it was released. This can be done through a document change management control table. The information risk profile itself should be reviewed, at a minimum, on an annual basis or as business conditions change that have a potential impact on the information risk appetite of the organization.

CONCLUSION

An information risk profile is critical to the success of an organization's information risk management strategy and activities. It provides valuable insights into an organization's information risk appetite and expectations for information risk management. Information risk and security professionals and programs that effectively leverage this information in their actions and activities can be confident in their alignment with business requirements and expectations.

REFERENCES

National Institute of Science and Technology (NIST), Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," 2010

International Organization for Standardization (ISO), ISO 27005:2008, *Information technology—Security techniques—Information security risk management,* 2008

ISACA, COBIT® 5, USA, 2012

ISACA, Risk IT, USA, 2009

ENDNOTE

[1] US Legal Inc., definition of "Due Care," *www.uslegal.com*

What Is Your Risk Appetite?

Mukul Pareek, CISA, ACA, AICWA, PRM, is a risk professional based in New York, USA. Pareek is the copublisher of the Index of Cyber Security (*cybersecurityindex.org*) and the author of a risk education web site, *www.RiskPrep.com.*

As a risk manager, knowing the organization's risk appetite means knowing how much risk the organization is comfortable bearing. In the financial world, risk appetite is almost always expressed explicitly, in the form of value-at-risk limits, and limits on concentration risk, counterparty exposures, liquidity, leverage and so on. This explicit expression takes the form of money units—dollars and cents, for example—making everything fairly objectively measurable and reportable.

For risk managers responsible for operational risk, such explicit statements of risk appetite are difficult to enunciate. Risk, in these contexts, is often measured in terms of being high, medium or low, or a similar subjective scale, with a great deal of reliance on the risk manager's judgment.

Risk appetite then takes a loosely accepted understanding that the highest-rated risk factors are to be addressed first, but without clearly stating if they are either acceptable or unacceptable for the organization to hold. This is in stark contrast to thresholds for financial risk, where breaching a limit requires almost immediate risk reduction with escalation and communication happening automatically.

CHALLENGE FOR THE TECHNOLOGY RISK MANAGER

For the technology risk manager, the challenge is similar in that clear boundaries for the extent of information-systems-related risk that management is willing to keep are undefined. Explicit statements of risk appetite rarely exist. Decisions on whether to live with a risk or mitigate it are largely based on judgment and, often, on what resourcing and budgetary situations permit in any particular situation. Knowing the organization's risk appetite means being clearly aware of the nature and kinds of risk that are acceptable, those that are unacceptable, and those that are acceptable only after executive review and approval.

> "Explicit statements of risk appetite rarely exist."

SETTING RISK APPETITE IN A TECHNOLOGY RISK CONTEXT

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines risk appetite as "the amount of risk, on a broad level, that an organization is willing to accept in pursuit of value."[1] ISACA defines risk appetite in a similar way as being "the amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission."[2] However, because the *amount of risk* is not a discrete threshold against which a technology risk manager can objectively evaluate individual findings or the risk, a formal approach that states the risk appetite in terms of the risk actually encountered needs to be developed.

Articulating the risk appetite involves setting the standard against which assessed risk is compared with a view to making a decision on avoiding, mitigating or holding risk. But, as ISACA's definition of risk appetite states, risk appetite has relevance only within the context of the organization's mission. The risk that would be acceptable for an organization focused on increasing market share would be different from one that places a higher priority on protecting reputation, which, in turn, would be different from an organization that seeks to provide superior customer service. The business managers involved in codeveloping and setting the risk appetite need to be those whose responsibilities relate directly to the organization's mission and whose business processes IT supports.

Of course, an organization may have multiple objectives, not all of which are equally important. In fact, defining, communicating and gaining acceptance for an explicitly stated risk appetite from business managers can be a great engagement opportunity for the risk manager. Resourcing and funding discussions can also benefit from a focus on whether a given risk exposure is above or below the risk appetite.

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:

RISK RATINGS AND RISK APPETITE

So how does one express risk appetite? A lazy way may be to relate it to the results of risk assessments. For example, one could express risk appetite as a simplistic statement saying that the organization is comfortable living with risk rated medium or low, but not with risk rated high or critical. The trouble with this approach is that it lacks clarity and specificity, and, therefore, it is open to challenges by business managers and technologists alike. It is not specific because it focuses on a rating that is one level removed from the risk itself and, as an abstraction of the seriousness of the underlying issue, represents the technology risk manager's perspective, which may not be shared by others.

A formal statement of risk appetite should establish the objective scale against which the risk could be measured and compared, and the risk rating determined thereafter. The formal statement of risk appetite could then provide the rationale as to why a particular rating is assigned to a finding, as opposed to the rating determining if the finding falls outside of the acceptable risk threshold.

Risk ratings and rankings are widely used in organizations, yet countless hours spent arguing with auditees on why something should be high instead of medium (or the other way around where the auditee has a self-interest in pushing a pet project) illustrate that such assessments make auditees miss the risk perspective. Further, risk ratings are often disconnected from the organization's purpose and are difficult to act upon, as senior management may not sponsor the efforts required to remediate or address the risk factors classified in this manner. For this reason, issues and findings, even those rated high, tend to live on far longer than they should. Therefore, using risk ratings as the surrogate for expressing risk appetite is not a good idea. This does not mean that the risk rating is no longer relevant, only that it follows and uses the results from a measurement against the statement of risk appetite as one of the inputs in its determination.

Explicitly setting the risk appetite allows the risk manager to state with clarity and authority which kinds of risk are acceptable and which are not. It is then possible to hold accountable groups that are responsible for addressing risk that goes beyond the organization's risk appetite. Decisions are also less open to organizational debate because issues are being measured against agreed criteria, as opposed to being assigned a risk rating that needs to be continually justified and defended.

EXPRESSING RISK APPETITE

So how does a statement of risk appetite manifest itself in a practical way? Is it a lofty statement of good intentions that is high on the acceptance scale, but low in implementation quality? Or is it so detailed that it includes every possible risk that exists in an organization's risk universe? A high-quality statement of risk appetite is probably somewhere in the middle. One way to think about it would be to consider the ways a risk would be realized, and then think about the classifications, attributes or characteristics that the risk realization paths bear. Risk appetite can then be expressed in statements that are clear, are stated in a way that supports protecting the achievement of business objectives and are agreed to by senior management.

Figure 1 provides examples of statements of risk appetite stated in binary terms as being acceptable or not. The examples focus on cybersecurity risk, though the analogy may be extended to other kinds of IT risk, of which cybersecurity risk is a subset. As organizations mature, these statements of risk appetite may be explicitly tied to operational and financial performance objectives. That linkage is not demonstrated in the examples provided in **figure 1** for reasons of brevity, and it is assumed that if a risk is unacceptable, it is because it impacts the organizational objective in an unacceptable manner.

Figure 1—Example Statements of Risk Appetite			
Risk Manifestation	**Asset/ Business Impacted**	**Appetite**	**Action**
Vulnerabilities			
Remote code execution vulnerabilities in technologies hosting customer data	Customer franchise	No appetite	Fix immediately
Vulnerability requiring no authentication to exploit on customer web site	Business reputation	Acceptable with senior management agreement	Prioritize and fix
Vendors			
High-risk data shared with vendor missing baseline data leakage controls	Client franchise	No appetite	Cease business with vendor
Low-risk data shared with vendor missing baseline data leakage controls	Internal data	Acceptable	No action
Applications			
No protection against SQL injection on intranet application	Internal applications	Acceptable	No action
Cross-site scripting vulnerability in Internet-facing customer application	Profitability targets	No appetite	Fix immediately

In the same way, risk appetite could be stated for other technology risk issues; for example, whether or not an IT general control weakness qualifies as a material deficiency could provide the test for the risk being acceptable or unacceptable.

BUILDING ON THE FOUNDATION

Over time, the simplistic risk appetite statements may need to develop into more complex and better stated frameworks that include a number of different, related elements:

1. **The cost of risk avoidance or mitigation**—A missing element in **figure 1** is the question of the cost of risk avoidance or mitigation. What if the medicine is worse than the ailment? For example, what if the business faces an unacceptable level of risk when measured against the stated risk appetite, but the cost of the cure is something the business cannot bear or there are consequences that are equally unacceptable? Clearly, the nature and effects of dealing with the risk need to be considered and incorporated into the statement of risk appetite.
2. **The core risk**—At the most detailed level, there could be at least as many risk factors defined as there are controls. This would make the task of assigning an appetite statement to each of them quite daunting and practically impossible, given that the business environment and, therefore, the controls that organizations adopt as a response are rarely static. What is required is the generalization of the specific risk into a more easily understood and higher-level risk. Continuing the example of cybersecurity risk, risk could be distilled into a handful of factors (such as remote code execution, privilege escalation, denial of service and asset theft) and the organization could have a risk appetite statement for each.
3. **Connection to business objective**—Each risk should have a clear connection to business objectives, which should be clearly brought out as part of stating the core risk. Business objectives could include, for example, profitability, reputation, compliance, cost control and customer experience. These should be discussed with business executives as part of the exercise to formulate the organization's risk appetite.
4. **Graded scale for expressing risk appetite**—While the binary expression of risk appetite illustrated previously may be a good and easy way to get started, it is more of a first step in the process. As managers consciously realize the limits of their risk tolerance, a more nuanced and graded expression of risk appetite, perhaps along a sliding scale, can be put in place. This would include gradations such as "acceptable" on one end of the scale, following through with "reluctant to accept," "averse" and "unacceptable" at the other end.
5. **Authority for risk decision making**—The moment the organization moves to a higher level of maturity than expressing risk appetite on a binary scale, questions of communication and escalation arise. Some of the statements of risk appetite may require submitting the risk for consideration by a named risk decision-making authority, which could be a risk committee or a senior manager. These downstream processes need to be defined as part of managing the risk appetite statement.
6. **Risk aggregation**—Risk may need to be considered together in its totality. What may seem acceptable as a stand-alone

risk may not be acceptable when considered together with other risk factors. The organization's risk appetite may need to make an allowance for considering risk in aggregation in terms of its impact on business objectives.

CONCLUSION

Understanding the need to ascertain and express risk appetite is a task of self-discovery for any organization. It helps crystallize the organization's true attitude toward risk and forces a hard look by senior management at how far it is willing to let the organization walk on the technology risk plank. Risk appetite should answer the question as to which risk factors the organization is comfortable bearing and which it is not. It should transform risk discussions by making irrelevant the likely different interpretations of what is acceptable to live with each time a risk assessment or audit is performed.

To summarize, the following points are worth keeping in mind:

1. In the end, risk appetite is a position adopted by members of senior management in pursuit of their objectives. It is their opinion and point of view, and that is how it should be presented to the rest of the organization—not as a *diktat* from the technology risk manager.
2. Risk appetite is not static. As the risk landscape evolves and the business environment shifts, risk appetite must adjust. The adjustment frequency may be annual or more often, depending on how fast the organization moves and is affected by technology risk.
3. The expression of a risk appetite is not a one-size-fits-all exercise. Frameworks can help, but each organization has to lay down its own path in line with its risk tolerance and decide how formal, detailed and mature its statement of risk appetite should be.
4. If a linkage to the organization's objectives cannot be established because it appears too far-fetched, perhaps the right business executives are yet to be consulted. Technology supports the organization; therefore, its risk appetite must be determined by the organization.
5. When bad things happen in the world of technology, business and executive managers often express surprise. Developing a statement of risk appetite in partnership with business executives can help set expectations, drive engagement and avoid surprises.
6. Risk appetite should be actionable in a way that analysts or auditors working for the technology risk manager can use it as part of their day-to-day battles. It should remove uncertainty on senior management's perspective on issues and findings.
7. Technology risk managers should own and manage the process of setting and communicating risk appetite. In doing so, they should consult with the right groups in their organizations; propose, draft, communicate and revise the statements of risk appetite with senior management; and obtain senior management's approval and authorization.
8. Judgment is critical when laying down risk appetite, and more so when applying it. Risk appetite should provide strong guidance, yet allow judgment to be exercised in situations where management's intent appears to be different.

ENDNOTES

[1] Rittenberg, Larry; Frank Martens; *Thought Leadership in ERM, Enterprise Risk Management, Understanding and Communicating Risk Appetite*, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2012, *www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf*

[2] ISACA, Glossary, Risk Appetite, *www.isaca.org/glossary*

Quantifying Information Risk and Security

Ed Gelbstein, Ph.D., has worked in IT for more than 40 years and is the former director of the United Nations (UN) International Computing Centre, a service organization providing IT services around the globe to most of the organizations in the UN System. Since leaving the UN, Gelbstein has been an advisor on IT matters to the UN Board of Auditors and the French National Audit Office (Cour des Comptes) and is a faculty member of Webster University (Geneva, Switzerland). A regular speaker at international conferences covering audit, risk, governance and information security, Gelbstein is the author of several publications. He lives in France and can be reached at *ed.gelbstein@gmail.com.*

Conducting risk assessments and the calculation of a return on investment (ROI) on information security is challenging. ISACA's Risk IT[1] framework defines IT risk as "The business risk associated with the use, ownership, involvement, influence and adoption of IT within an enterprise."[2] That said, managing risk requires predictions, assumptions and guesses.

COBIT® 5 for Information Security addresses governance issues that were missing in previous publications, standards and good practices. While it provides many indicators and suggested metrics, quantifying information security in business terms remains difficult.

The impact of security events on the business relies on knowledge of incidents, the IT systems and services that are essential to support business processes, and the assessment of the impact of their malfunctions on business operations. Acquiring such knowledge relies on business process owners—they are the only ones who can assess and quantify the operational, financial and regulatory impact of disruptions. The impact on reputation remains hard to calculate withany accuracy.

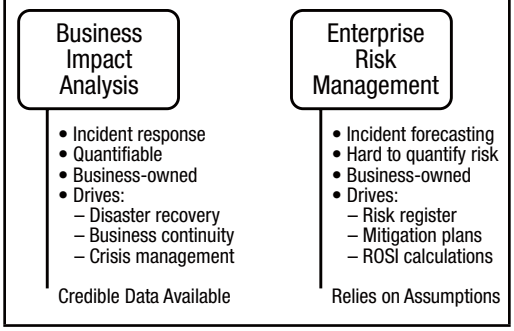
A well-developed business impact analysis (BIA) should reflect how business operations are impacted and how time affects such impact, as this is rarely a linear function. A 10-minute service interruption may have a negligible impact while the same service interruption extended over three days may prove catastrophic to the business.

As BIAs are based on available and credible data evaluated by individuals familiar with specific business processes, they allow the impact to be assessed in a plausible manner. Even if the numbers are not accurate, they can be accepted as "reliable enough."

The outcome of BIAs should be a set of well-designed, tested and updated plans (incident response, disaster recovery, business continuity and crisis management). The effectiveness of such plans can determine the difference between survival and business failure.

Enterprise risk management (ERM), of which IT risk is a component, arose from different concerns relating to a risk-based approach to management that integrates aspects of internal control and strategic planning and includes, among other things, regulatory compliance. Like understanding impacts, ERM should be owned by business managers. **Figure 1** illustrates the main differences between BIA and ERM.

Figure 1—Differences in the Scopes of BIA and ERM



Two disciplines—information risk management and information security—have migrated from their specialized niches into the wider field of enterprise management.

Risk assessments and the calculation of ROI for information security are linked topics. The discussion that follows examines how and why. Information security practitioners are expected to master both disciplines and this article attempts to describe the many trappings these topics contain.

INFORMATION RISK MANAGEMENT

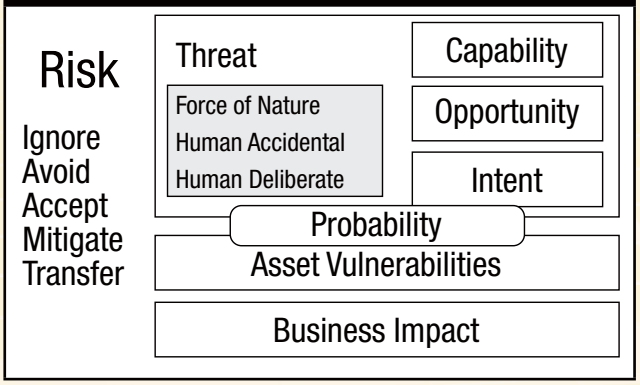
Information risk management (IRM) came to the attention of business managers through the following factors:

- The convergence of increasing dependency on information technology in enterprise operations
- The mission-critical nature of many information systems and services
- The reliance on an open global network (the Internet) and its side effects (notably cybercrime and malicious software of unknown origin)

• Increasing concerns about the militarization of cyberspace and the potential for cyberwar and cyberterrorism

ISACA's *The Risk IT Framework* and *The Risk IT Practitioners Guide* provide a comprehensive, well-thought-out and articulate set of processes. Chapter 4 of *The Risk IT Practitioners Guide* is devoted to communicating and describing risk. It recognizes that qualitative assessments are simple to carry out and that quantitative assessments require not-readily-available (if at all) data. **Figure 2** presents the five strategies to deal with individual risk and the components of a risk assessment. This is simple and concise view regarding risk assessment. A more comprehensive view of this topic can be found in *The Risk IT Framework*.

Figure 2—Factors to Consider When Assessing Risk



THREATS

Until the 1990s, risk practitioners focused on the threats presented by forces of nature, such as hurricanes and earthquakes. As information technologies became ubiquitous, it became necessary to address incidents arising from accidental human activities (such as incorrectly configuring a device and undetected software errors). Deliberate actions ranging from avoiding a test to save time to fraud and sabotage also had to be added to the threat landscape. Ignoring these risk factors may not be a prudent course of action. Deliberate human threats can be the biggest challenge, particularly for critical infrastructures because:

• Such actions are unpredictable, not random. Thus, statistical analysis of past events cannot help.
• The individuals behind these threats are unknown, rarely identify themselves, and may be external or internal. Good intelligence is essential, but hard to find.
• A malicious insider with the capabilities, motivation and opportunity to interfere with information systems and data could remain undetected for a long time (if ever detected).

In the absence of supporting data to calculate and quantify the probability of a deliberate human attack on information assets, risk assessors can, at best, rely on their knowledge of the enterprise, its culture and people, and their experience. In the absence of reliable intelligence regarding such attacks, a qualitative assessment is more or less an informed guess. Whether or not this is good is subjective and different for each enterprise depending on its nature.

ASSET VULNERABILITES

The rapid innovation in IT has added complexity to vulnerability management for several reasons.

The Growing Complexity of IT Products

Operating systems (OSs) are one example. When IBM introduced System 360 in 1967, it became the largest software project at the time, totaling an estimated one million lines of code. Delivered a year late, its cost was four times the initial budget and it was full of errors that took years to eradicate.[3] In 1969, IBM acknowledged that each release of this software had about 1,000 errors and this number was reasonably stable.[4]

Microsoft introduced Windows 7 in 2009 (and replaced it with Windows 8 in 2012). The original release of Windows 7 contained an estimated 50 million lines of code (50 times the size of System 360). Microsoft has not disclosed the number of errors of the original release version of Windows 7 and no reliable information on this could be found from other sources. However, hot fixes for Windows 7, many of which are labeled *critical*, are issued on a weekly basis.[5]

Such complexity can be found in virtually every other product, including servers, routers, tablets and smartphones. This is also true for downloaded mobile applications ("apps") and enterprise applications. It should be assumed that every piece of equipment and software has vulnerabilities (some known and others yet to be discovered) that can, and most likely will, be exploited with malicious intent.

To add to the problem, the current software ecosystem is small and some components are used all over the world (e.g., Windows, Android, Java). The errors in these systems are constantly being investigated and reported. The reports give

potential attackers a significant advantage because the scale of complexity of installing and testing all error fixes takes time and not all are implemented.

Time to Market

The recent wave of technical innovation is driven by the competitive nature of the IT industry. Its innovative culture encourages designers and vendors to bring their products to the attention of potential customers as early as possible. Some innovations are presented at trade exhibitions and are, at best, beta versions. Some are marketed early, possibly without full code reviews, testing and other quality assurance processes.

> "It should be assumed that every piece of equipment and software has vulnerabilities."

The hundreds of thousands of apps for smartphones and tablets that end users can download and install make the assessment of security of such devices extremely complex if not impossible.

End-user license agreements (EULAs) for packaged software limit the vendor's liabilities and describe warranty disclaimers when the software causes damage to the user's computer or data. These lengthy and complex agreements are hard to read and understand, are nonnegotiable, and must be agreed upon as a condition for installing the software.

Innovative products can become objects of desire for individuals. In recent years, organizations have been under pressure to allow employees to choose their preferred technologies for work-related home and mobile use and this has undermined the technical and security enterprise architectures.

Imperfections in technology, such as errors in design and manufacturing, appear gradually and some remain undiscovered (to become zero-day deliverables once discovered). Typically, the vendor offers a solution that could, and often does, introduce new errors.

Vulnerabilities

In addition to imperfect technologies used by imperfect people, the corporate use of information technologies relies on numerous processes (for a detailed description, refer to COBIT 5 and its companion publication *COBIT 5 for Information Security*). Vulnerabilities arise through:

- The extent to which these processes are implemented (Small organizations relying on internal resources are rarely able to implement all the processes listed in COBIT and those that are implemented may not be at a sufficiently high level of maturity to meet requirements.)
- The degree to which the processes follow the guidelines of established good practices such as the Information Technology Infrastructure Library (ITIL), the Data Management Body of Knowledge (DMBOK), the Software Engineering Body of Knowledge (SWEBOK) and the Project Management Body of Knowledge (PMBOK), as appropriate
- The level of compliance with these processes in practice, which is defined by the size and competencies of those who apply them. Time pressures, absences and lack of knowledge conspire to create shortcuts. Every exception should be treated as a vulnerability. This is defined by the organization's culture and the competencies, motivation and dedication of those applying the processes.

A sound assessment of vulnerabilities in technology, processes and staff is a prerequisite to effective risk assessment. Such vulnerabilities need to be related to their criticality to business processes and the impact these may cause when exploited by a specific threat.

PROBABILITY

A widely accepted definition of information risk states that it is "the potential that a specific threat will exploit the vulnerabilities of an asset." Many publications on risk present the formula as: Risk = Probability x Impact. However, the word *probability* is frequently replaced by *likelihood*. Beware! These two words do not mean the same thing. Probabilities have numerical values derived from statistical analysis. Statistics is a formal discipline using somewhat complex mathematics. This discipline is not well understood and statistics are often misused. This was recognized in the 19th century by the statement: "Lies, damned lies and statistics."[6]

Statistics include two basic categories: *descriptive* and *inferential*. Descriptive statistics reflect past events and require sufficient data to meet specific requirements. Inferential statistics are predictive and use past data and mathematical formulae to support projections into the future.

Inferential statistics include those that can be calculated with some degree of accuracy. This is the case in games of chance

such as dice and roulette. Casinos have relied on such statistics for a long time. "The gambling known as business looks with austere disfavor upon the business known as gambling."[7]

Inferential statistics and event intelligence are also used by insurance companies for the calculation of premiums for common events (e.g., driving a car, burglary, death). Insurance companies have the option of transferring the risk of a rare event to a reinsurance company or consortium. Some of the latter have lost vast amounts of money because statistics have limitations when it comes to events that are so rare that there is no reliable past data (e.g., explosion of a super-volcano). Venture capitalists and investors willing to gamble can become rich by betting early on the success of an innovator, e.g., the emergence of Google in 1998.[8]

Information security likelihood is, at best, events that can occur with uncertain frequency and magnitude. Therefore they require an informed guess (and more often a gamble), subject to the evaluator's knowledge, experience and degree of paranoia (or optimism) when dealing with uncertainty.

Stating that likelihood of the manifestation of a threat may be low, medium or high and creating a risk matrix with little boxes colored green, yellow or red is a step forward—as long as all parties involved understand the subjective nature and agree on the assumptions and ratings made. Such matrices are often referred to as heat maps and can be misleading by themselves. Good practices require heat maps to be related to the organization's risk criteria to determine whether a given level of risk is acceptable (risk appetite).

Risk matrices can be used to create a risk register, ranked by impact (which requires a robust BIA to provide such information) and where the appropriate risk strategy (e.g., ignore, accept, avoid, mitigate, transfer) is made explicit, together with accountability for its implementation if the chosen strategy is one of mitigation. It is at this point that a link to the estimation of the ROI of mitigation measures appears.

A contrarian note: A bureaucratic approach to risk assessment is sometimes practiced, for example:

- Bringing in consultants to run short workshops for managers on how to build risk matrices
- Asking managers to carry out a threat/vulnerability analysis that identifies what can disrupt the operations for which they are responsible, ideally as a one-page document. An impact assessment is not included beyond categories such as low, medium and high. It is rare to find references to "catastrophic."
- Another person (sometimes titled risk manager) collecting all these one-page documents and filing them in a thick folder. Little or no effort is made to identify dependencies or quantify and rank impacts.
- Filing the thick book and telling the auditors that "a comprehensive risk assessment has been completed"
- Doing nothing until an event occurs and then finding someone to blame. If or when a security event happens, it is probable that blame will be attached to someone, but not necessarily to the person who initiated and supported the bureaucratic approach.

In the absence of supporting data to calculate and quantify the probability of such an attack on information assets, risk assessors can, at best, rely on their knowledge of the enterprise, particularly its culture and people. A qualitative assessment is more or less an informed guess. It is, however, a major step forward from doing nothing.

IMPACT

The analysis of security events on the business is an essential component of risk management, as senior managers can estimate outcomes in financial terms and provide sensible answers to questions such as:

- How much could a security incident cost the business and other components of its supply chain?
- What would be the impact of a security incident on the organization's business operations, reputation and compliance requirements?

A BIA is a prerequisite for the development and invocation of disaster recovery, business continuity and crisis management plans. The critical success factors for a BIA include being:

- Owned by the business unit and/or functional managers
- Quantitative
- Regularly updated
- Validated by executives
- Reviewed and approved by the audit committee

Some organizations collect data on incidents and use them to estimate the incident's impact. For example, the cost of downtime has been the subject of numerous publications over the years in addition to the cost of stolen intellectual property. There are, however, other domains in which such costs are difficult, if not impossible, to estimate accurately. A number being agreed upon by a group of senior managers represents progress, and thus, the number does not need to be accurate.

RETURN ON SECURITY INVESTMENT

As security incidents do have business consequences, organizations recognize that appropriate actions must be taken to deter, prevent and/or mitigate their impact and this requires resources—people, processes and technologies. How much should an organization spend on information security to protect its information assets? This is a derivative of an older question: How much should the organization spend on information technology to carry out its business?

Despite numerous publications and frameworks (including ISACA's Business Model for Information Security [BMIS]), this question continues to be debated, mainly due to the intangible and speculative nature of most investments in this area as well as an inability to deal with uncertainties.

It would be hard to argue against carrying out an ROI calculation for an IT security project such as the installation of barriers and door controls in a building. Such a project would have a substantial cost (and duration), be very visible, and require organizational and procedural changes.

ROI is best used for the comparative evaluation of alternative solutions to a business issue. Such a calculation must be comparable in terms of the cost factors included and in the assessment of the benefits for alternative proposals likely to have different functionalities, costs and timescales. An ROI for a single option is of little value as it is easy enough to come up with justification for expenditures.

The final decision may include factors other than ROI, for example, the experience of similar installations in other organizations, the vendor's support capabilities and warranties.

Expenditures on information security add a philosophical dimension:

- When are these really investments or just the cost of doing business?
- Would it be right to classify the cost of fire insurance for the business's offices as an investment?
- Is the purchase of antivirus software an optional item?

Discussions with many security professionals reveal that they regard these as operational expenses. However, they are increasingly being asked to provide a return on security investment (ROSI) to support their budget requirements.

There are many publications on this topic.[9, 10, 11] Some have generated controversies, for example, several articles by Bruce Schneier, a well-known, respected and published security expert in the UK, who stated, "(ROSI)'s a good idea in theory, but it's mostly bunk in practice."[12] Leaving aside the issue of investment vs. the cost of doing business, the contrarian views reflect the experience of many years of preparing business cases for executives focused primarily on financial numbers, rather than on what was "sensible" and/or "good for the business." Either trusting or naive, these executives failed to realize (even when told) that the numbers were completely fictional and quite possibly wrong.

First, the easier component to evaluate is cost. Those who have experience in IT (and other) projects are aware that cost and timescale estimates are always optimistic. Besides, other than the initial cost of the product or service, there are many cost components that may be easily forgotten when preparing a business case, an ROI or ROSI analysis, for example:

- The cost of preparation of a request for proposals and their subsequent evaluation (sometimes assisted by consultants)
- The internal costs of the procurement process, including legal reviews
- The delivery, installation and configuration of the procured items
- The training of those who need to operate, maintain and support the procured items
- The projected life of the item (to reflect rapid obsolescence and the short life expectancy of many vendors)
- A long list of recurring items such as license renewals, maintenance, installation and testing of updates

An experienced practitioner should be able to create a comprehensive list and put numbers to it with, optimistically, a margin of ±30 percent (rarely an underestimate).

Assessing the benefits (the actual return) relies entirely on creativity as these are in the future and are either guesses or truly unpredictable. Uncertainty ensures that there will be several unintended consequences. They also rely on the validity of many assumptions such as:

- The quality of the delivered and installed item and the vendor's descriptions of its functionality are complete and true and the product does not contain errors or faults
- The item has been appropriately configured; in practice more of an aspiration than a demonstrable fact
- The item is appropriate to mitigate one or more of the identified risk factors and the analysis of impact on the business provides quantitative financial assessments of the business's exposure
- The benefits have an identified business owner who is accountable for their delivery

- The timescales exist for achieving such benefits

Executives should be aware that when requesting a ROSI to justify an investment, the numbers may not be accurate and are possibly erroneous.

CONCLUSION

This article presents a contrarian view of two disciplines that have acquired much visibility and caused information security practitioners to spend considerable time searching for answers to questions from executives who need to decide on expenditures intended to mitigate information risk. While the questions are legitimate and should be asked, some of the most popular risk management methods are no better than astrology (with apologies to those who read their horoscope).

Practitioners are, therefore, faced with a significant challenge: the inability to provide robust numbers to demonstrate that risk is correctly assessed and that the measures taken to strengthen security are appropriate and add value to the organization. Two actions that help meet this challenge follow:

- A sound assessment of vulnerabilities in technology, process and people is a prerequisite to effective risk assessment. Such vulnerabilities need to be related to their criticality to business processes and the impact these may cause when exploited by a specific threat.
- An up-to-date and validated analysis is a prerequisite for the development of incident response, disaster recovery, business continuity and crisis management plans. These should be regularly tested, for example, when there are changes in the environment, their results analyzed for lessons learned, and the plans modified accordingly. When this is not the case, the organization may not be able to survive a disruptive incident.

The article also discusses elements that, although not quantifiable, should be explicit in discussions with senior management:

- In the absence of supporting data to calculate and quantify the probability of a deliberate human attack on information assets, risk assessors can, at best, rely on their knowledge of the enterprise, particularly its culture and people. A qualitative assessment provides a more or less informed guess.
- Errors in design and manufacturing appear gradually and some remain undiscovered (to become zero-day deliverables when discovered). Typically, the vendor offers a solution that could, in turn, introduce new errors.
- The use of probability theories and other statistical techniques to quantify information security is, at present, not a viable approach due to the absence of sufficient data. Therefore, the use of *likelihood* is likely to continue. However, it should not be forgotten that this is little more than a guess.
- When it comes to evaluating ROSI, given that there is room for considerable creativity in conducting such analyses, an experienced practitioner could well ask: Does the enterprise have any particular number in mind?
- Forecasting is not an exact science.

ENDNOTES

1 With the release of COBIT 5 in 2012, key elements of Risk IT have been incorporated in COBIT. *COBIT for Risk* is expected to be released in September 2013.

2 ISACA, *The Risk IT Framework*, USA, 2009, *www.isaca.org/riskit*

3 Ensmenger, Nathan; *The Computer Boys Take Over (History of Computing)*, The MIT Press, 2010

4 NATO Science Committee, Software Engineering Techniques, in a report of a conference, April 1970, p. 15

5 Cowart, Robert; Brian Knittel, *Microsoft Windows 7 In Depth*, Que Publishing, 2009

6 Twain, Mark; "Chapters From My Autobiography," 1906, in which Twain attributes the phrase to Benjamin Disraeli (UK Prime Minister)

7 Bierce, Ambrose; *The Devil's Dictionary*, 1906

8 This is the essence of the book *The Black Swan* by Nassim Taleb.

9 Gordon, L.; M. Loeb; *Managing Cybersecurity Resources: A Cost-benefit Analysis*, McGraw-Hill, 2005

10 Singh, Jaspreet; "Pay Today or Pay Later: Calculating ROI to Justify Information Security and Compliance Budgets," *Information Systems Control Journal*, vol. 3, 2008, *www.isaca.org/archives*

11 Anderson, Kent; "A Business Model for Information Security," *Information Systems Control Journal*, vol. 3, 2008, *www.isaca.org/archives*

12 Schneier on Security, "Security ROI," 2 September 2008, *www.schneier.com/blog/archives/2008/09/security_roi_1.html*

Readability as Lever for Employees' Compliance With Information Security Policies

Franz-Ernst Ammann, Ph.D., is employed by Deutsche Telekom AG. Ammann previously worked in IT strategy and conducted related assessments on the German Act to Modernize Accounting Law (BilMoG).

Aleksandra Sowa, Ph.D., ITCM, , is employed by Deutsche Telekom AG. Sowa initiated the Horst Görtz Institute for Security in Information Technology, a European university-based institution for interdisciplinary research in the field of IT security, and worked as an auditor in the financial services industry.

Information security policies are part of the internal formal regulatory framework for information security and thereby part of an organisation's information security governance. The purpose of information security policies (policies that involve guidelines and requirements) is to guide decisions and actions within the organisation towards a desired outcome. These policies are understood to be principles or rules that inform, enable and obligate. Therefore, people, not policies, ensure the appropriate and adequate level of security for systems, infrastructure and data.

Employees are frequently identified as the key vulnerability to a company's information security and a cause of numerous security incidents.[1] However, employees can comply only with policies they understand. Readability is key to understanding policies and it is dependent on the education of the target audience—all employees with access to technology, in this case.

IMPACT OF SECURITY POLICIES

Despite the pivotal role that security policies have on auditing information security compliance and on the design and operation of information systems, relatively little effort is invested in the evaluation and assessment of the policies themselves. Information security policies are less frequently the focus of internal auditor examinations than the information systems, processes and controls designed according to these policies.

Security policies are important for design decisions regarding infrastructure, systems and processes of IT. They describe control objectives and define standard security measures. Information security policies address constraints on people's behaviour and processes. Serving as a management tool and internal benchmark for design and operation of information systems, they are firmly rooted in the organisation's governance framework. Internal and external IT auditors take security policies into account to evaluate compliance of the internal regulatory framework with external norms, standards and general—national and international—regulatory frameworks. While auditing the effectiveness of security measures, auditors usually take into account how consistent the implemented measures are with the security policy requirements.

Information security auditors are highly professional and well-trained personnel. They are practiced in reading and interpreting security policies. Their understanding goes far beyond that of the average employee. There is risk even if things are running well after a first-time roll out of policies. First-wave implementation teams frequently communicate with the creators of policies rather than with the staff who are involved in the established process. Policies in the context of information security effectiveness and compliance may prove to be useful to determine whether the information in the policy reaches its audience; thereby, the policy may avoid ineffective execution of controls. When security incidents occur, the root cause may be the security policy itself, i.e., the fact that the staff has not been able to understand it.

QUALITY OF INFORMATION SECURITY POLICIES

What makes a good information security policy? Its quality, obviously. The term "quality" covers a variety of aspects including relevance, completeness and applicability. For example, in the case of a hard-to-grasp policy that is implemented by experienced and skilled staff, while the result—the realized security level—may be good, it does not provide evidence of the quality of how the policy is written. Rather, the end result is due to the experience and skill of the people who implemented it and, ultimately, compensated for the quality deficits of the hard-to-grasp policy.

The result is, in fact, an assessment of the interaction between policies and people. That is, if information security auditors confirm

that controls and security measures are working effectively in compliance with the policy, this must be understood as indirect proof of the working interplay of the security policy and the people in charge at that time. In the opposite case, ineffective or inadequate controls and security measures may directly indicate a not-so-good policy.

The matter of the policy is not necessarily the issue here. The cause for an inaccurate implementation of measures may be the incorrect interpretation of the security policy, or even no understanding of it at all. An evaluation of the policy itself can deliver certainty about whether the text transports the obligation, and it gives auditors—and governance officers—an insight into what measures are necessary to improve the *status quo*.

One must focus on policies' readability and comprehensibility. How can authors—and auditors evaluating policies under the aspect of effectiveness—determine whether a policy is appropriate for those employees who will have to implement and conduct it? Is it possible to tailor the text to a target audience? Are there metrics for this purpose?

TYPICAL METRICS FOR INFORMATION SECURITY POLICIES

What metrics help to evaluate the quality of an information security policy in the course of an audit or self-assessment? Typical metrics[2] that are used to assess and evaluate information security policies relate to the following issues, among others (**figure 1**):

- Dissemination of the policies in the company
- Application of policies in various divisions

Figure 1—Metrics for the Information Security Policy

Type of Metrics	Performance Indicators
Security policy dissemination	1. Percentage of organisational units for which security policies and procedures with respect to the standardisation of the management of security features are defined, implemented and executed 2. Percentage of organisational units that applies to the security policies and procedures in accordance with the systemic risk, the asset criticality and the sensitivity of the information 3. Proportion of employees (percentage) that has confirmed the knowledge of security policies, procedures and standards relevant to them
Application	4. Share of security measures (percentage) that tested in the current period and have proved to function properly under normal and abnormal conditions, e.g., the error distribution by type and weight for the current period and the three preceding periods 5. Share of security policies, procedures and standards that is in use in normal and abnormal situations
Awareness	6. Percentage of employees who have received the current, relevant-for-their-tasks security policies, procedures and standards, divided into organisational units such as internal staff, internal external staff (e.g., in-house consultants) and external internal staff (so-called "pseudo-outsiders," e.g., staff working outside the company as consultants) 7. Frequency of training staff regarding the security policies, procedures and standards available, by organisational units: • Date of last training • Percentage of employees who have received the necessary training within the previous six months • Number of comments or amendments from the training courses that have been considered in the past six months in the security policies
Adequacy and timeliness	8. Share of security policies, procedures and standards that: • Is up to date • Is sufficiently detailed to be implemented • Defines roles and responsibilities • Defines specific functions assigned • Is tailored for specific risk factors and criticality • Is associated with certain assets by organisational units
Grade of implementation	9. Proportion of the security policy requirements, procedures and standards that was implemented and put into operation by means of: • Technical controls • Manual or management controls • Combination of the two 10. Proportion of third parties for which compliance with the security policies has been contracted for external workers working within the organisation, internal workers employed outside the organisation, outsourcing partners and offshore partners

Sources: Adapted from Herrmann, D. S.; *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI,* Auerbach Publications, USA, 2007; and Brooks, P.; *Metrics for IT Service Management,* ITSMF International, 2006

• Awareness of the policies
• Exceptions to the policies
• Timeliness and update mode

Appropriate metrics from **figure 1** may be selected, by auditors assessing the evaluation of the adequacy and effectiveness of controls (not the security policy as such) according to the specific audit goals. These metrics are often derived using the goal question paradigm (GQP), a methodology that makes it possible to establish a link between the company's objectives and performance indicators (e.g., metrics).[3]

There are, however, some critics of these metrics. Companies should strive to reach a sound understanding of security policies in order to assure their effective implementation. Thus, the standard approach is security instruction once a year (e.g., formally documented in employees' signature lists) that is sometimes followed by a multiple-choice comprehension test. This measure has flaws. It addresses only the very basic knowledge needs of a general audience, i.e., staff, management, auditors. It does not, however, reflect the complexity of the internal regulatory framework.

What do people need to adopt the more complex content of security policies? One component is simply understanding the text. Is there a way to measurably improve?

READABILITY METRICS

Details on how the information security policies should be amended to improve their effectiveness can be derived from the metrics that relate to their inherent properties: the text, its readability and reading ease. The presumption is that if the policy is not understood or its content is difficult to read, the policy will either not be applied or will be applied poorly. Readability and reading-ease metrics make it possible to assess how easy it is to understand the document.

The readability metrics may be used to assess (lexical) reading ease of the information security policy. The readability index (or score) is measured by means of statistical text analysis consisting of several measurements, such as length of sentences, number of syllables, and number of words with three or more syllables. This metric says that the longer the text, the longer the sentence, or the more words with more than three syllables, the harder it is to understand the text. That is, the higher the reading-ease index, the easier it is to understand the document.

The most widely used reading-ease index is the Flesch Reading Ease Index,[4] which can be calculated according to the following formula:

FI = 206.835 - (1.015 x ASL) - (84.6 x ASW)
Where:
FI = Flesch Reading Ease readability score
ASL = Average sentence length in words (average number of words in a sentence, calculated by dividing the number of words by the number of sentences)
ASW = Average syllables per word (the number of syllables divided by the number of words)

The calculated score—the obtained Flesch Index—based on the statistical text analysis is mapped to the standardised values indicating the readability level. The index is typically a number between 0 and 100, but values may also occur beyond these limits (see **figure 2**).

Figure 2—Readability Level According to Flesch Index

Flesch Index	Readability Level
0 - 29	Very difficult
30 - 49	Difficult
50 - 59	Fairly difficult
60 - 69	Standard
70 - 79	Fairly easy
80 - 89	Easy
90 - 100	Very easy

Source: Adapted from Flesch, R.; *The Art of Readable Writing*, Harper & Row Publishers, USA, 1974

WHO UNDERSTANDS THE SECURITY POLICY

Evaluating the Flesch Index of the information security policy may help to assess how difficult it is to read and understand the document. Consequently, if the text is difficult to read, auditors may suggest formulating it in a less complex way (e.g., introducing shorter sentences, fewer long words), so that it is easier to read in general.

Reading ease is, however, only one aspect of security policy readability. Another aspect is the question of whether the reading ease of the policy meets the demands of the target group to which it is addressed. The readability level metrics may be used to answer this question.

The popular Flesch-Kincaid Grade Level Index may be utilised as a metrics of readability level. The test is based on a score created by Rudolf Flesch and later enhanced by John P. Kincaid. It maps the Flesch Index to US grade levels. It can also mean the number of years of education generally required to understand the text. It is used by the US Department of Defense as a standard test, required for all kinds of internal requirements and instructions.[5]

This score analyses and rates text on a US grade school level based on the average number of syllables per word and words per sentence (like the Flesch Index). For example, a score of 60.0 means that an average student in eighth grade would understand the text (**figure 3**).

Figure 3—Metrics for Information Security Policy

Flesch Index	Education
90.0 - 100.0	Easily understood by an average 11-year-old student
60.0 - 70.0	Easily understood by 13- to 15-year-old students
0.0 - 30.0	Best understood by university graduates

The education required to understand a document of a specific Flesch Index is different from country to country.

CLOSING REMARKS

If, for example, the calculated Flesch Index for the information security policy is below the value of 20, its reading ease would correspond with that of a professional essay or doctoral thesis. This is obviously inappropriate if the particular policy is aimed at the average employee whose areas of expertise do not include information security.

Furthermore, many executives and experts do not have the time for a thorough study of administrative matters, such as security policies. This group also benefits from the reading ease that comes with a high Flesch Index. "Time is money" is also true in the case of understanding security policies. It takes much less time to read and understand a document that is easy to read (e.g., has a higher reading-ease index) than to study a text with a reading-ease index indicating research essay qualities.

By appropriate linguistic revision of the text, the reading ease for these polices can be improved and, in turn, the level of security in an organisation is improved.

Metrics for information security policies can be used to assess the quality and effectiveness of the document, i.e., how easy it is to be understood and consequently the requirements to be followed. Additionally, metrics concerning the level of distribution, implementation, timeliness or awareness can be utilised for monitoring exceptions from security policies and the grade of compliance organisations achieve when implementing policies.

ENDNOTES

[1] Independent Oracle Users Group (IOUG), *Closing the Security Gap: 2012 IOUG Enterprise Data Security Survey*, *https://blogs.oracle.com/securityinsideout/*

[2] For examples of typical security metrics and maturity models, see: Chapin, A.; S Akridge; "How Can Security Be Measured?," *Information Systems Control Journal*, vol. 2, 2005, *www.isaca.org/archives*

[3] Sowa, A.; S. Fedtke; *Metriken—der Schlüssel zum erfolgreichen Security und Compliance Monitoring: Design, Implementierung und Validierung in der Praxis*, Vieweg Springer, 2011

[4] The test is based on a score created in the 1940s by Austrian-born American author Rudolf Flesch. The formula to compute the Flesch Index is one of the best known and most popular for readability indicators. However, the formulas differ for different languages. The formula provided here is true only for English documents.

[5] Hayden, L.: *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*, McGraw-Hill Professional, USA, 2010

DDoS Attacks—A Cyberthreat and Possible Solutions

Ajay Kumar, CISM, CCSK, ISO 27001 LA, is an information security manager who has been working for a decade in the information security and risk management domain and has expertise in infrastructure security, identity and access management, data protection and privacy, cloud security, and cybersecurity.

Distributed denial of service (DDoS) is one of the most diffused types of cyberattacks that represent a great concern for governments and institutions today. These attacks are an insidious foe to online service providers as their businesses depend on the availability of their web sites for critical business functions and productivity. This article is focused on the types of DDoS attacks, the trend and changing frequency, the business impact and countermeasures that organizations can take to prevent successful DDoS attacks, and building a strategic approach to defend from this growing cyberthreat.

Cyberattacks on various banks worldwide reflect a frightening new era in cyberwarfare. For example, since September 2012, US banks have been battling, with mixed success, DDoS attacks from a self-proclaimed hacktivist group called Izz ad-Din al-Qassam Cyberfighters.[1] Due to a shortage of experts skilled in building effective defenses, many corporations are not prepared to battle such attacks.

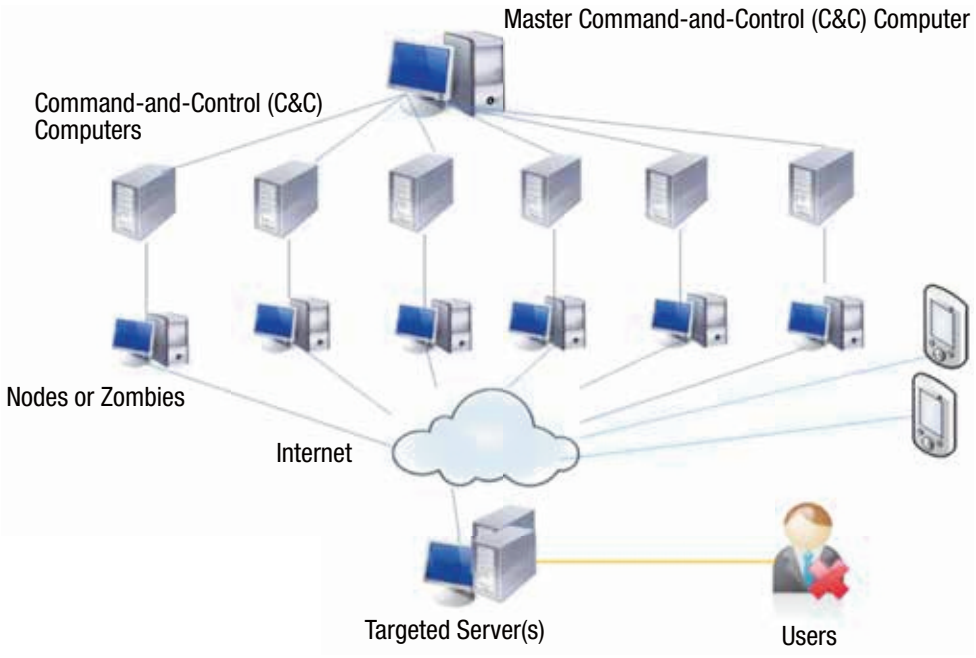
The growing concern of HTTPS-based attacks adds a new dimension to the security landscape. Though conventionally associated with security on the web, hackers have managed to weaponize the encryption layer, using it to launch application-level and SSL attacks that can escape detection and remain hidden until it is too late. This has become an especially troubling phenomenon for financial services and e-commerce web sites that rely heavily on HTTPS.[2]

DDOS AND HOW IT WORKS

Denial of service is a form of cybercrime in which attackers overload computing or network resources with so much traffic that legitimate users are prevented access to network resources. Attacks are called "distributed" when the attack traffic originates from multiple hosts.

Historically, DDoS attacks originate from Internet-connected PCs that are compromised by malware. These PCs are called "bots" and are typically under the control of a command-and-control (C&C) server operated by the attacker or "botmaster" (see **figure 1**).

Figure 1—DDoS Attack Conceptual Diagram



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:

BOTNETS

The word "bot"[3] (from robot) refers to automated software programs that perform specific tasks on a network of computers with some degree of autonomy. "Botnets" are a set of computers controlled by a C&C computer to execute commands as directed. Typically, computers become bots when attackers illicitly install malware that secretly connects the computer to a botnet; attackers then perform tasks such as sending spam, hosting or distributing malware, or attacking other computers. The C&C computer can issue commands directly, often through Internet Relay Chat (IRC) or by using a decentralized mechanism, such as peer-to-peer (P2P) networking. Computers in a botnet are often called nodes or zombies.

The DDoS attacks work in phases. In the first phase, the attacker compromises the weak machines in the network from around the world. In the second phase, a set of tools (also called malware) is installed on the compromised systems to attack the victims by controlling them from a C&C server.

TYPES OF DDOS ATTACKS

While there are hundreds of types, DDoS attacks can be broadly classified into the following three major categories:

- **Flood or volumetric attacks**—This type of attack seeks to consume all the available bandwidth of or to a data center or a network, such as User Datagram Protocol (UDP) floods, Internet Control Message Protocol (ICMP) floods and Domain Name System (DNS) reflection. As a result, the legitimate user is no longer able to connect or access the desired servers or applications.
- **Connection state attacks**—All network devices or systems (such as firewalls, webservers and application servers) have internal tables with some limited resource/capacity that are used to track the active connections or disconnected connections. With this type of attack, the table is filled with many connections, so the new user cannot make a connection. Sometimes these attacks cause device failures that result in all active users losing connection.
- **Application-layer attacks**—In these types of attacks, application servers are overloaded with so many requests for resources that all available resources are consumed. Examples of these types of attacks include memory, processors, malformed HTTP, HTTP get/post floods and DNS cache poisoning.

THE TRENDS IN DDOS ATTACKS

The volume, duration and frequency of DDoS attacks used to flood web sites and other systems with junk traffic have significantly increased over the years. According to a report released by a DDoS mitigation service provider security firm, an 88 percent increase in the total number of DDoS attacks was seen in the third quarter of 2012 compared to the same period in 2011. The packet-per-second (pps) rate in attacks has also increased apart from the increase in the bandwidth.[4] The size of a high-profile attack against a spam-fighting organization called Spamhaus was reported to have peaked at more than 300 Gbps, making it the largest in history.[5]

DDoS attacks are evolving in the following ways:

- The attack paradigm is rapidly shifting from the realm of network security into the application layer.
- Consumerization of IT is broadening the DDoS attack platform.
- DDoS attacks are increasing in frequency and impact.
- Inherent limitations in today's infrastructure make DDoS a very realizable risk.
- Complex and advanced DDoS attacks can be difficult to mitigate.

THE DDOS THREAT LANDSCAPE

The first step in defending against today's complex DDoS threat is to understand the threat landscape. According to recent attack data, DDoS attacks are being used in combination with other forms of cybercrime to facilitate information theft by degrading perimeter defenses with DDoS attackers and then gaining access to resources inside the network.[6] Sony estimated that US $170 million in losses were enabled by DDoS attacks.

In September 2012, the US Federal Bureau of Investigation issued a warning to financial institutions that some DDoS attacks are actually being used as a distraction.[7] These attacks are launched before or after cybercriminals engage in an unauthorized transaction and are an attempt to avoid discovery of the fraud and prevent attempts to stop it. In these scenarios, attackers target a company's web site with a DDoS attack. They may or may not bring the web site down, but that is not the main focus of the attack; the real goal is to divert the attention of the company's IT staff toward the DDoS attack. Meanwhile, the hackers attempt to break into the company's network using

any number of other methods that may go unnoticed as the DDoS attack continues in the background.

Furthermore, the availability of DDoS tool kits has turned DDoS attacks into a commodity that is readily available to anyone. It is safe to assume that DDoS tool kits will continue to evolve and offer new capabilities—forcing the defending or victim organizations to adjust their defense strategies. Furthermore, cloud computing, which has proven to be one of the most transformative changes in IT, has also been successfully applied by the cybercriminal in DDoS attacks.

MOTIVATION BEHIND DDOS ATTACKS

The number one motivation behind DDoS attacks is believed to be ideological hacktivism,[8] followed by other motivational factors such as financial fraud, extortion and competitive rivalry.

Hacktivists often utilize DDoS attacks to advance political and social objectives, disabling the legitimate usage of web sites and targeting IT resources to express a message of dislike or disapproval. Hacktivism is not a new concept, but recent advances in malicious software have made point-and-click malware tools available to anyone wanting to join a hacktivist's cause. These tools include the Low Orbit Ion Cannon (LOIC) or the slightly newer High Orbit Ion Cannon (HOIC), which can target up to 256 web address simultaneously.

BUSINESS IMPACT OF DDOS THREATS

The impact of a DDoS incident can be devastating to the organization from a financial and brand perspective. A few-hour network outage can cost millions of dollars and anger thousands of customers who rely on online services. Direct revenue losses can be high for organizations that rely heavily on public-facing services. DDoS attacks are even more impactful when they are used in conjunction with other types of offenses.

The consequences of a DDoS-related attack can include:

- Brand and reputation damage
- Breach of contract and violations of service level agreements
- Loss of shareholder confidence
- Service interruption leading to, for example, issuance of customer credits, nonrenewal of business and lost sales
- Marketing and advertising costs associated with damage control

In 2012, a large telecommunications organization experienced a DDoS attack that flooded its DNS servers, lasted about eight hours and took down its business web site. The intermittent disruptions affected Internet services for its business customers due to DNS outages resulting from the DDoS attack.[9]

THE CHALLENGES

Virtually any resource that is connected to the Internet is vulnerable to DDoS attacks, and contrary to popular belief, many existing controls do not protect against these attacks.

> "Virtually any resource that is connected to the Internet is vulnerable to DDoS attacks."

Typically DDoS attacks attempt to bring down the critical services by targeting the organization's web servers, application servers, routers or firewalls. In most enterprises and government organizations today, these resources either perform or provide access to business functions that are essential to the enterprise's operations, services delivery, productivity, revenue generation and other core activities.

Today, most enterprises rely on traditional perimeter security tools, such as firewalls, secure web gateway and Internet service providers (ISP) devices, to protect the networks. Although these essential devices serve as a first layer of defense and should remain part of a layered security defense, they are not designed to handle network availability or protection from advanced threats and can fail to actually protect from sophisticated attacks.

POSSIBLE SOLUTIONS TO DDOS ATTACKS

Given the extraordinary and rapid changes in DDoS attack techniques, traditional DDoS mitigation solutions (e.g., bandwidth provisioning, firewall, intrusion prevention systems) are no longer sufficient to detect and protect an organization's network or applications from sophisticated DDoS attacks.

External Solutions

The most cost-effective approach to mitigate DDoS attacks is to pay the ISP to detect and mitigate attacks before they reach the organization's Internet-facing resources (e.g., web servers, email servers). The key here lies with the ISP, in terms of its maturity of service offerings that address most forms of DDoS attacks.

In addition, there are many organizations that provide services for DDoS mitigation and play a middleman role. Their offerings include such things as DNS redirection to

Border Gateway Protocol (BGP) route changes in which inbound Internet traffic flows through them and they detect the attacks and perform scrubbing/filtering in their Internet data centers. As a result, their customers get filtered and clean Internet traffic.

Internal Solutions

Various security vendors provide appliance-based solutions to defend against DDoS attacks. They detect and provide protection from a broad array of DDoS attacks. Many vendors claim solutions with different appliance models and offer throughput ranging from 12 Mbps to enterprise-class solutions. Further, these appliances are integrated with the central management suite, giving users a single point of control and a full view of security events. As DDoS threats evolve every day, these specialized vendors are likely to respond faster with innovative solutions than vendors that offer basic DDoS protection embedded in the firewall and ISP offerings.

DDOS ATTACK MITIGATION GUIDELINES AND BEST PRACTICES

Successful DDoS attack mitigation involves having 24/7 continuous monitoring technology capabilities and capacity to identify and detect attacks while allowing legitimate traffic to reach its destination. Furthermore, to address issues appropriately in real time, a solid and tested incident response plan and procedures need to be in place. Key technologies, best practices and processes include:

- **Centralized data gathering and analysis**—Organizations need to build centralized monitoring dashboards that allow them to see the entire network, systems and traffic patterns in one place and have a team of experts keeping watch consistently and continually over them.
- **Layered defense approach**—The goal should be to allow only legitimate traffic to the network and exclude all unwanted traffic.
- **Scalable and flexible infrastructure**—To make sure systems function properly even under attack, organizations must have a highly scalable and flexible infrastructure in place with on-demand capacity.
- **Regularly addressing application and configuration issues**—DDoS attacks have evolved to be more sophisticated and difficult to detect at the application layer. One needs to know and understand what each application does, its uses and usage pattern, what a normal application request looks like, and the normal transaction level for each application component.

CONCLUSION

DDoS attacks have left their mark. As time goes by, these types of attacks against private organizations and governments for the purpose of distraction are expected to continue to unfold with even more complexity and sophistication. DDoS attacks are also largely adopted in cyberwarfare to hit a country's critical infrastructures. Enterprises must pay attention to this threat and properly assess their environment and monitoring capability to protect and defend against these aggressive attacks. As DDoS attacks continue to evolve, it is critical not to underestimate the threat.

ENDNOTES

[1] Gonsalves, Antone; "U.S. Bank Cyberattacks Reflect 'Frightening' New Era," *CSO*, 10 January 2013, *www.csoonline.com/article/726131/u.s.-bank-cyberattacks-reflect-frightening-new-era*

[2] Radware, "Server-based Botnets and HTTPS Layer Attacks Among the Tactics Leveraged by Hackers in Some of 2012's Most Notorious Attacks," 22 January 2013, *www.radware.com/newsevents/pressrelease.aspx?id=1630879*

[3] Microsoft, "What is a Botnet?" *www.microsoft.com/security/sir/story/default.aspx#!botnetsection*

[4] Prolexic Report, "Increasing Size of Individual DDoS Attacks Define Third Quarter," 16 October 2012, *www.prolexic.com/news-events-pr-increasing-size-of-individual-ddos-attacks-20-gbps-is-the-new-norm-2012-q3.html*

[5] Vijayan, Jaikumar; "Spamhaus Hit by Biggest-ever DDoS Attacks," *CIO*, 27 March 2013, *www.cio.com/article/730849/Spamhaus_Hit_by_Biggest_ever_DDoS_Attacks?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+cio%2Ffeed%2Fdrilldowntopic%2F3089+%28CIO.com+-+Security%2*

[6] Arbor Networks, "A Focus on Distributed Denial of Service," p. 3

[7] Symantec, "Internet Security Threat Report 2013: Volume 18," April 2013, *www.symantec.com/security_response/publications/threatreport.jsp*

[8] Arbor Special Report, Worldwide Infrastructure Security Report 2012 Volume VIII, "Motivation, Scale, Targeting and Frequency of DDoS Attacks," p. 18

[9] Ragan, Steve; "DDoS Attack Caused AT&T DNS Outage on Wednesday," *Security Week*, 17 August 2012, *www.securityweek.com/ddos-attack-caused-att-dns-outage-wednesday*

Leveraging and Securing the Bring Your Own Device and Technology Approach

Gaurav Priyadarshi, CISA, BS 25999 LI, ISO 27001 LA, ITIL V3, is a senior security consultant at TATA Consultancy Services, a leading IT service company with worldwide experience in the information security domain. Priyadarshi is a technology evangelist and a follower of trending security concepts. He can be reached at *gpriyadarshi@gmail.com*.

The IT infrastructure that was created at the beginning of the IT era remains a constant framework for the future. Just as everything in life evolves, the IT environment and its landscape transform. Today, IT must continue to grow.

The bring your own device (BYOD) trend of enabling and empowering employees to bring their own devices (e.g., laptop, smartphones, tablets) has expanded to bring your own technology (BYOT) including office applications (e.g., word processing), authorized software (e.g., data analytics tools), operating systems, and other proprietary or open-source IT tools (e.g., software development kits, public cloud, communication aids) to the workplace. This coupling has been coined as bring your own device and technology (BYODT). As BYODT becomes increasingly acceptable and popular, it is likely to be one of the biggest challenges for information security governance.

This article describes some of the pros and cons of BYODT and outlines the various security governance steps to be taken by enterprises that are considering adopting a BYODT approach.

PROS FOR IMPLEMENTING BYODT

Implementing BYODT can result in numerous benefits including:

- **Happy employees**—BYODT makes (most) employees happier and more satisfied as they prefer to use their own devices over the often budget-oriented and dull devices offered by the company. Employees may also prefer to reduce the number of devices they carry while traveling; before BYOD, traveling employees would carry their personal and company-provided devices (i.e., two mobile phones/smartphones, two laptops and so forth).
- **Cost savings**—Implementation of a BYODT program can also result in a substantial financial savings to IT budgets because employees can use devices and other IT components they already possess.[1] The savings include those made on the purchase of devices for workers, on the maintenance of these devices and on data plans (for voice and data services). These savings can then be utilized by the company to enhance its operating margins or to offer more employee benefits.
- **IT workload optimization**—The IT department can be freed from a myriad of tasks such as desktop support, trouble shooting and end-user hardware maintenance activities. This savings can then be leveraged by the IT department to optimize its budget and resources.
- **Faster adoption of new technology**—The BYODT trend is attributed, in part, to the fact that employees adopt technology well before their employers and subsequently bring these items to work. Thus, BYODT results in faster adoption of new technologies, which can also be an enabler for employees to be more productive or creative—one resulting area of competitive advantage for the business.
- **Increased employee efficiency**—Employees can use their own, familiar device to complete their tasks more efficiently as it gives them the flexibility to quickly customize their device or technology to run faster and per their requirements.[2] On the other hand, in the case of company-provided devices and technology, such customization is often time-consuming as the employees have to provide proper cost justifications and then seek authorization through change requests.

CONCERNS OF BYODT

As with all other evolutionary approaches, BYODT comes with its own set of concerns and objections:

- **Security governance and administration complexities**—By allowing employees to BYODT, companies are opening a new chapter for security managers and administrators. The security governance framework and corporate security policies will need to be redefined and a great deal of effort will be required to make each policy efficiently operational and streamlined.

- **Increased concerns with privacy and data protection (PDP)**—This could be perhaps the biggest challenge for BYODT. In some industries that deal with sensitive and confidential data, PDP concerns will hamper a rollout of BYODT. Such enterprises will have to tread cautiously with this trend.
- **Increased challenges with ownership of data and regulatory compliance**—By adopting BYODT, organizational control over data is blurred. Objections are also raised when business and private data exist on the same device. This could interfere with meeting the stringent controls mandated by certain regulatory compliance requirements.
- **Lack of uniformity and compatibility issues**—Applications and tools may not be uniform on all devices, which can result in incompatibility when trying to, for example, connect to the corporate network or access a Word file created by another employee who has purchased a newer version.
- **Reluctance by employees**—There may be a lack of consensus among employees; some may not be willing to use their personal devices or software for company work.

THE VERDICT

This discussion of pros and cons is displayed through the schematic diagram in **figure 1**.

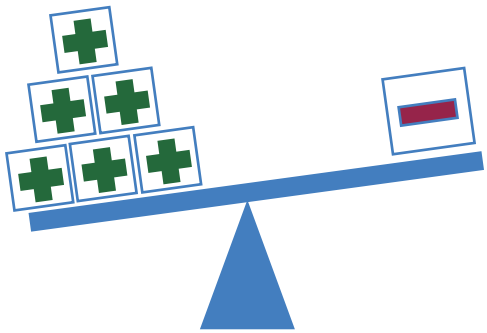
Clearly, the ongoing trend and the benefits realized from BYODT suggest that the concerns should be considered as challenges and companies should address BYODT implementation by leveraging these challenges.

LEVERAGING AND MITIGATING CHALLENGES AND OBJECTIONS OF BYODT

The following approach can assist in the successful implementation of a BYODT program that mitigates security challenges:

- **Establish a well-defined BYODT governance framework.** This can be done by soliciting input from various departments of the enterprise regarding how different areas use portable gadgets. This helps create a uniform governance strategy. Following are the essential steps for creating a BYODT governance framework:
  - **Network access control:**
    1. Determine which devices are allowed on the network.
    2. Determine the level of access (e.g., guest, limited, full) that can be granted to these devices.
    3. Define the who, what, where and when of network access.
    4. Determine which groups of employees are allowed to use these devices.
  - **Device management control:**
    1. Inventory authorized and unauthorized devices.
    2. Inventory authorized and unauthorized users.
    3. Ensure continual vulnerability assessment and remediation of the devices connected.
    4. Create mandatory and acceptable endpoint security components (e.g., updated and functional antivirus software, updated security patch, level of browser security settings) to be present on these devices.

Figure 1—Pros and Cons of BYODT



- Happy employees
- Savings for employers
- IT department workload optimization
- Faster adoption of new technologies
- Boost to employees' productivity

- Complex security governance
- Data privacy concerns
- Regulatory compliance
- Lack of uniformity and compatibility
- Reluctance by some employees

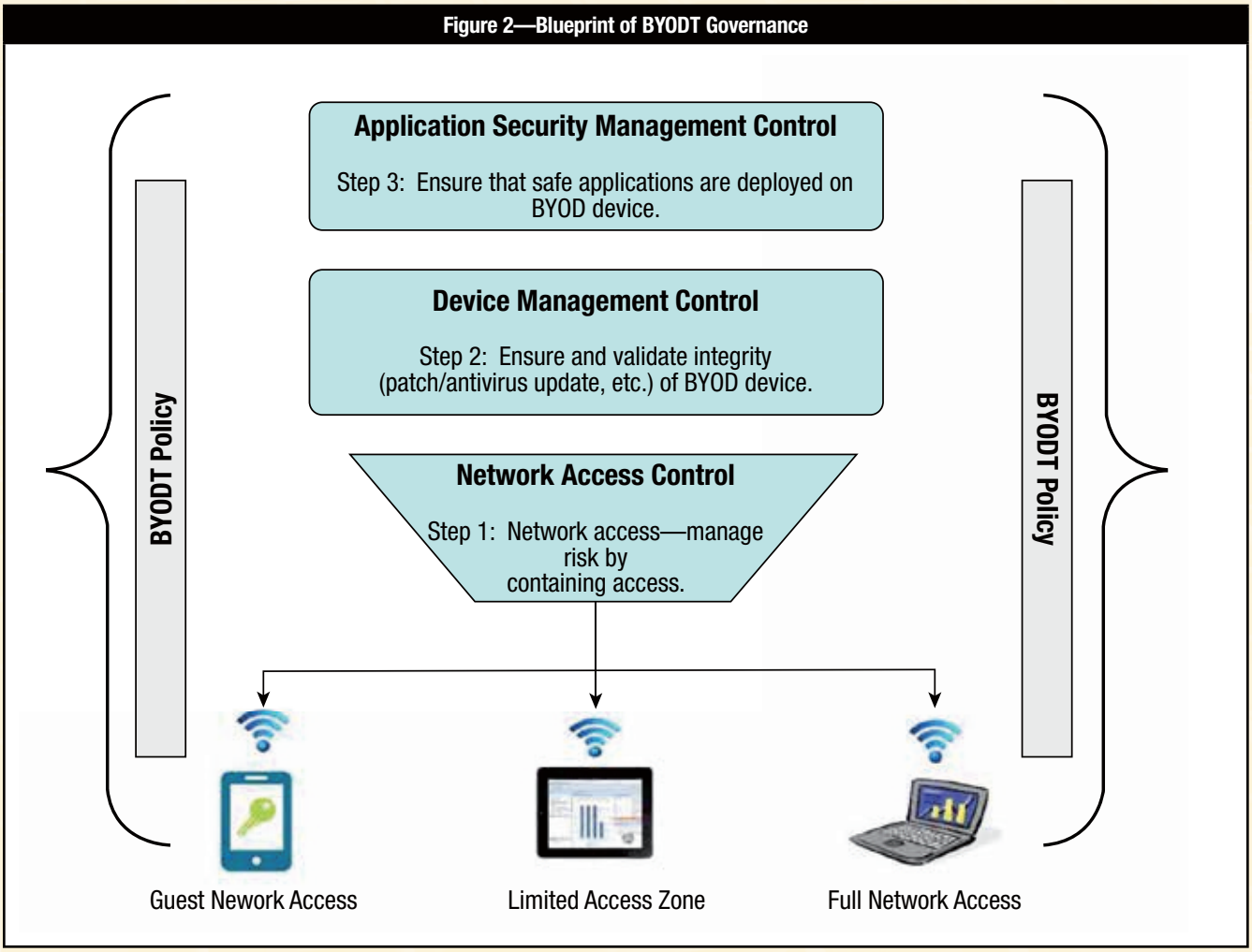
– **Application security management control:**
  1. Determine which operating systems and versions are allowed on the network.
  2. Determine which applications are mandatory (or prohibited) for each device.
  3. Control enterprise application access on a need-to-know basis.
  4. Educate employees about the BYODT policy.

Figure 2 schematically represents the steps to be taken to reach the maturity of BYODT governance in order to establish a BYODT program.

- **Create a BYODT policy.** Make sure there is a clearly defined policy for BYODT that outlines the rules of engagement and states the company's expectations. The policy should also state and define minimum security requirements and may even mandate company-sanctioned security tools as a condition for allowing personal devices to connect to company data and network resources.

BYODT security requirements should be addressed by having the IT staff provide detailed security requirements for each type of personal device that is used in the workplace and connected to the corporate network. For example, IT staff might require devices to be configured with passwords, to prohibit specific types of applications from being installed on the device, or require all data on the device to be encrypted. Other BYODT security policy initiatives might include limiting activities that employees are allowed to perform on these devices at work (e.g.,

Figure 2—Blueprint of BYODT Governance



limiting email usage to corporate email accounts only) and periodic IT audits to ensure the device is in compliance with the company's BYODT security policy.

Figure 3 provides a sample BYOD policy.

Figure 3—Sample BYOD Policy

Bring Your Own Device Policy

[Employer] would like to provide greater IT device choice to its employees and simultaneously reduce end-user IT device complexity…Thus, [Employer] is implementing a "Bring Your Own Device" (BYOD) program to permit [Employer] personnel to use personally owned smartphones and tablets for business purposes. This document applies to employees…

Current BYOD Approved for Use

1. Android smartphones and tablets (version 2.2 or higher)
2. …

Expectation of Privacy

[Employer] will respect the privacy of your personal device and will request access to the device by technicians only to implement security controls as outlined below…

Information Technology/Responsibilities

The information technology (IT) department is responsible for configuring and supporting the user's device to receive and access company email, calendar and contact data…

Employee Responsibility and Requirements for all BYODs Accessing [Employer] Network Services

1. User is responsible for using company email on his/her personal smartphone within the same constraints as on a company-owned device.
2. User agrees that he/she will password-protect the device via the device's operating system's available password-protection protocols.
3. User's device will be remote wiped if (i) you lose the device, (ii) your employment with [Employer] ends, or (iii) IT detects a data or policy breach or virus.

User Acknowledgment and Agreement

It is [Employer]'s right to restrict or rescind computing privileges or take other administrative or legal action due to failure to comply with the BYOD Policy. Violation of these rules may be grounds for disciplinary action up to and including termination.

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of [Employer] service.

Employee Name: _____
BYOD Device(s): _____
Employee Signature _____ **Date:** _____

- **Use virtualization as a solution.** Windows 8, Windows Server 2012 and the Microsoft Desktop Optimization Pack (MDOP) provide virtualization solutions that can be used to enable BYODT. Windows Server 2012 enables the user to easily create a virtual desktop infrastructure (VDI).

  VDI is an alternative desktop delivery model that can help enable BYODT. It gives users secure access to centrally managed desktops running in the data center. With employees using their personal devices, they can access the hosted desktop for work while keeping their work and personal environments separate.

  VDI removes the limitations of maintaining a stringent acceptable client list for an organization (e.g., Dell Latitude 5400S and Mac Books only) and allows end users to use their preferred devices that ultimately connect back into a managed VDI. As long as the devices have a support view client, they should be permissible for use within the company.
- **Use the sandbox approach.** Organizations planning to allow storage of corporate data on mobile devices must assess the risk and classification of the data on those devices. Implementing a BYODT strategy should include considerations of data classification and different access methods for different types of data in the IT environment. One approach is sandboxed applications. This approach boxes corporate data into a separate container that can be secured with passwords and other authentication mechanisms; nonbusiness data are kept separate and users can continue to use their devices for personal use.

  Should the device be lost or the employee leave the company, corporate data can be wiped from the device while leaving personal data intact. The downside to this approach is that this method often limits the use of the phone for email and calendaring, often considered one of the greatest advantages of having an integrated device.
- **Separate personal and corporate data.** Some employers make connecting with an employee-owned device contingent on signing an agreement allowing the company to monitor compliance with acceptable-use policies and otherwise act to protect corporate data. In some cases, the agreement may include remote wiping of all data on the device—potentially including personal data—which can be a source of contention between IT and users if not properly managed.

- **Maintain secure access to the corporate network.** Device choice does not mean sacrificing security. IT must establish the minimum security baseline that any device must meet to be used on the corporate network, including Wi-Fi security, virtual private network (VPN) access and, perhaps, add-on software to protect against malware. In addition, due to the wide range of devices, it is critical to be able to identify each device connected to the network and authenticate both the device and the person using the device.

CONCLUSION

BYODT provides numerous benefits to the business, the key ones being reducing the IT budget and the IT department's workload, faster adaptation to newer technology, and making employees happier by giving them flexibility to use and customize their devices to enhance efficiency at work. Of course, various challenges come along with BYODT: increased security measures, more stringent controls for privacy and data protection, and other regulatory compliance.

These challenges provide a fundamentally new opportunity for innovation, redefining the governance structure and adoption of underlying technology. Clearly, the way forward for organizations is to mitigate the challenges of BYODT, align it with their future IT strategy and put it on the IT road map so that they can move ahead in the evolutionary cycle and thereby bring benefits and flexibility to one of their most important stakeholders—their employees.

REFERENCES

Bradford Networks, "Fallout of the iPod Holiday: The 10 Steps to a Secure BYOD Strategy," 20 December 2011, *http://www.slideshare.net/BradfordNetworks/the-10-steps-to-a-secure-byod-strategy*

Cisco, "Cisco Bring Your Own Device (BYOD) Smart Solution Design Guide," 20 December 2011, *http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html*

Honeycutt, Jerry; *Introducing Windows® 8: An Overview for IT Professionals*, Microsoft Press, USA, 2012

Hyman, Jonathan; *The Employer Bill of Rights: A Manager's Guide to Workplace Law*, Apress, USA, 2012

Mann, Andi; George Watt; Peter Matthews; *The Innovative CIO: How IT Leaders Can Drive Business Transformation*, Apress, USA, 2012

Meyler, Kerrie; Byron Holt; Marcus Oh; Jason Sandys; Greg Ramsey; *System Center 2012 Configuration Manager Unleashed*, Pearson Education Inc., USA, 2012

Moore, Connie; "Bring Your Own Technology: The Lines Between Work and Personal Technology are Blurring," Forrester, 26 November 2012, *http://blogs.forrester.com/connie_moore/12-11-26-bring_your_own_technology_the_lines_between_work_and_personal_technology_are_blurring,*

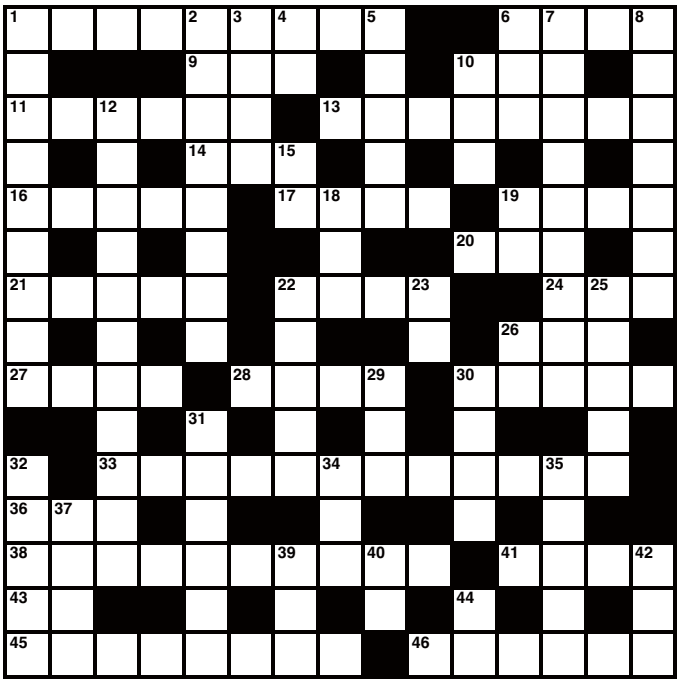
ENDNOTES

[1] Forrester, *Key Strategies to Capture and Measure the Value of Consumerization of IT*, May 2012, *www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf*

[2] *Ibid*.

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. One type of access control in relation to privacy (2 words)
6. Malware attacks effective against online banking systems, abbr.
9. Remain
10. Criticize harshly
11. Protected from danger
13. Emphasizing the organic or functional relation between parts and the whole
14. Limit
16. Inception
17. The R in IRMS
19. Advantages
20. Web site address ending of some sites
21. Search for
22. Information risk level
24. Company offering Internet service
26. Agent (abbr.)
27. ____door, undocumented means of computer entry
28. Unit of storage measurement
30. Authority
33. Subject relating to who is authorized to see what information, an important field for an IT auditor to check into (2 words)
36. Appropriate
38. Another type of access control in relation to privacy (2 words)
41. A.k.a. zombies
43. The in Spanish
45. Make a new evaluation of
46. ____ Reading Ease readability score

DOWN

1. Vulnerability management needs to be supplemented with a _____ approach to security (2 words)
2. Statistical display medium (2 words)
3. Zone
4. Compass direction
5. Falls
6. Spanish for more
7. One method for an auditor to obtain information for an IT audit
8. Makes another copy of, for security purposes
10. Banking access code
12. Back up with evidence and make certain of correctness
15. Reputation
18. Third in a family
19. Purchase order, abbr.
22. ISACA's incoming president, Tony _____
23. Type of TV
25. Detailed proposals
26. Read only, abbr.
29. Miscalculate
30. Google founder
31. Its second revision introduced the concept of risk correlation associated with prioritization of remediation actions
32. More secure
34. Help request
35. Means for implementation
37. Stack
39. Access points, for short
40. Former partner
42. "Quiet!"
44. Soft metal symbol

(Answers on page 54)

CPE Quiz

Prepared by Sally Chan, CGEIT, CMA, ACIS

Take the quiz online:

QUIZ #149

Based on Volume 2, 2013—Legal and Regulatory Challenges

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

TRUE OR FALSE

GATEWOOD ARTICLE

1. Many unknowns still surround cloud computing decisions. These unknowns lie in the gap between what cloud promises and what is delivered. The unknowns include the ability of users to overcome pressure points—areas of conflict between how cloud services are designed and delivered and how the enterprise integrates these services into business activities.
2. The 2011 Cloud Market Maturity Study indicated that cloud was just approaching the growth level of maturity. Among the different service models—Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) —IaaS was the most advanced, just entering the growth stage of maturity.
3. Not having a full appreciation of how cloud differs from traditional outsourcing restricts the ability of the board to govern and the ability of executives to define and manage cloud solutions. To change perceptions, cloud computing should be on the board's agenda to ensure that the board understands the benefits and risk factors associated with cloud service models.
4. Cloud has the potential for adding to existing business risk or for introducing risk that is outside of the organization's current risk profile. Because of the operational importance of cloud computing, cloud risk needs to be considered from the perspective of operational risk management.

JOSEPH ARTICLE

5. One of the principles of The Code of Fair Information Practices states that there must be a way for a person to find out what information about the person is in a record and how it is used.
6. An example of information security threats in the form of social engineering can be found in the exchange of personal data, along with photo and video tagging on social networking sites (such as Facebook, LinkedIn and Twitter).

KONING AND BIKKER ARTICLE

7. The Dutch Central Bank's IT Supervision Department learned from experience that it is important to translate legislation and regulation into practical measures to create effective supervision of compliance with legal and regulatory requirements.
8. One of the supervision-related advantages of using standards/frameworks is that assessment frameworks are viewed as rule-based rather than principle-based. Compliance with an assessment framework becomes a goal in itself.
9. Signing off on a completed assessment framework by a board member responsible for IT increases involvement and prevents a lack of engagement.

PIERRE-LOUIS, SANCHEZ AND SHEK ARTICLE

10. The Unified Control Matrix has been used to develop high-level information security policies for end users, information security guidelines to be inserted into requests for proposal, and requests for information to set expectations for information security with potential vendors, among other uses.
11. The security risk self-assessment consists of an application profile and data content, regulatory requirements, gating based on data classification, a criticality assessment with an applied scoring system, a vulnerability self-scan, and an overall scheduled remediation action plan.
12. The future plan of Unified Control Matrix is to incorporate updates to regulations, new regulations, policies, risk assessment questionnaires, security guidelines and checklists.

SESHADRI ARTICLE

13. SOC 1 reports are certifications, and these reports can be generally distributed to potential customers and used as a marketing tool.
14. IAASB/AICPA guidelines specify that the SOC 1 report is applicable only to internal controls over financial reporting. In cases where organizations want to include other areas such as privacy or confidentiality, for example, they should adopt SOC 2/SOC 3 reports.
15. Work done by an internal auditor can be used for work related to SSAE 16, and whether to do so is the judgment of the service auditor.

DUBEY ARTICLE

16. Top management must effectively balance its time, resources and strategic portfolios to meet today's demanding, intrinsically woven business and security needs. To fulfill these obligations from a security perspective, top management needs to understand the business risk, current state of existing security controls, gaps within those controls, and how the changing threats over time may require alignment of existing security initiatives and demand new ones.
17. The ability to attain top management's commitment toward information security programs should be based on the degree quantitative understanding has on how an information security product/tool or activity performs in the specific environment without negatively impacting the business.
18. The degree of customization/change required in the technical landscape to implement the security product/tool/activity is not a parameter impacting management commitment and success of information security programs.

ISACA Journal

CPE Quiz

Based on Volume 2, 2013—Legal and Regulatory Challenges

Quiz #149 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC # _____

Quiz #149

True or False

GATEWOOD ARTICLE

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

JOSEPH ARTICLE

5. _____
6. _____

KONING AND BIKKER ARTICLE

7. _____
8. _____
9. _____

PIERRE-LOUIS, SANCHEZ AND SHEK ARTICLE

10. _____
11. _____
12. _____

SESHADRI ARTICLE

13. _____
14. _____
15. _____

DUBEY ARTICLE

16. _____
17. _____
18. _____

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

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

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

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

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

Answers—Crossword by Myles Mellor

See page 52 for the puzzle.

1 R	O	L	E	2 B	3 A	4 S	E	5 D	■	■	6 M	7 I	T	8 B
I	■	■	■	9 A	R	E	■	R	■	10 P	A	N	■	A
11 S	E	12 C	U	R	E	■	13 H	O	L	I	S	T	I	C
K	■	O	■	14 C	A	15 P	■	P	■	N	■	E	■	K
16 B	I	R	T	H	■	17 R	18 I	S	K	■	19 P	R	O	S
A	■	R	■	A	■	■	I	■	■	20 G	O	V	■	U
21 S	C	O	U	R	■	22 H	I	G	23 H	■	■	24 I	25 S	P
E	■	B	■	T	■	A	■	■	D	■	26 R	E	P	■
27 D	O	O	R	■	28 B	Y	T	29 E	■	30 P	O	W	E	R
■	■	R	■	31 P	■	E	■	R	■	A	■	■	C	■
32 S	■	33 A	C	C	E	S	34 S	R	I	G	H	35 T	S	■
36 A	37 P	T	■	I	■	■	O	■	■	E	■	O	■	■
38 F	I	E	L	D	B	39 A	S	40 E	D	■	41 B	O	T	42 S
43 E	L	■	■	S	■	P	■	X	■	44 A	■	L	■	H
45 R	E	A	S	S	E	S	S	■	46 F	L	E	S	C	H

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 and reporting 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:

- **Standards**, divided into three categories:
  - General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
  - Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care
  - Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated
- **Guidelines**, supporting the standards and also divided into three categories:
  - General guidelines (2000 series)
  - Performance guidelines (2200 series)
  - Reporting guidelines (2400 series)
- **Tools and techniques**, providing additional guidance for IS audit and assurance professionals, e.g., white papers, IS audit/assurance programmes, the COBIT® 5 family of products

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

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

The ISACA Professional Standards and Career Management Committee (PSCMC) is committed to wide consultation in the preparation of standards and guidance. 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 guidance are posted at *www.isaca.org/standards*. Please note that the guidelines are being updated for integration into ITAF. An exposure draft of the revised guidelines is scheduled to be posted for comment on the ISACA web site in the fourth quarter of 2013. The titles of issued standards documents are listed as follows.

IS Audit and Assurance Standards (effective 1 September)

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 development)

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)

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

Advertisers/Web Sites

Leaders and Supporters

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

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

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

ISSN 1944-1967


When you're ready to
further develop your top talent
When you're ready to
invest in your organization's future
You are ready for
American Public University
American Public University is ready to help your team succeed. We're a nationally recognized university with bachelor's and master's degrees for business, retail, and IT professionals — completely online. So your employees can take classes on their own time. And people are taking notice. 99% of employers surveyed would hire one of our graduates again.*
When you're ready,
visit StudyatAPU.com/ISACA
*APUS Alumni Employer Survey, January 2011-December 2011
We want you to make an informed decision about the university that's right for you. For more about the graduation rate and median debt of students who completed each program, as well as other important information—visit www.APUS.edu/disclosure.
APU American Public University
Ready when you are. ™

Complex World. Real Solutions. Securing Success.

INFORMATION SECURITY AND RISK MANAGEMENT CONFERENCE

MARK YOUR CALENDARS! 6-8 November 2013 | The Cosmopolitan Hotel, Las Vegas, NV

This premier conference on Information Security, Governance, and Risk Management is a true investment in your future! Here are just a few of the career-enhancing benefits you can expect to receive from attending ISACA's North America ISRM:

Networking—Surround yourself with a community of like-minded IT professionals with whom you will build valuable relationships.

Thought-provoking seminars—Learn first-hand from leading professionals when you attend workshops such as:

- COBIT 5 for Security
- Innovation in Cybersecurity
- Managing Risk for Enterprise using COBIT 5
- Practical Approach to Network Vulnerabilty
- Securing Mobile Technologies
- Data Privacy Risks
- Tools and Tech of Digital Forensics

Earn up to 39 hours of CPE credit—Earn the hours you need to stay certified as you gain access to the latest issues facing your profession.

Don't wait—reserve your spot today to join Eddie Schwartz and other industry experts as they share their insights on today's most relevant information security and risk topics. **Visit *isaca.org/NAISRM2013* today!**

Eddie Schwartz
CISO, RSA

Robert Bigman,
Former CISO
for the CIA

Exclusive Keynote Speakers
will share their insights on cybersecurity and risk management in this changing world.

ISACA®
Trust in, and value from, information systems

ISACA®
Trust in, and value from, information systems

BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

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

New Books...

www.isaca.org/newbooks

IT Governance and Business Management

Robust Control System Networks: How to Achieve Reliable Control After Stuxnet
206 pages, 2013—**2MPRC**
Member $88.00 | Nonmember $98.00

Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets
263 pages—**98WSC**
Member $75.00 | Nonmember $85.00

Internet and Related Security Topics

Responding to Targeted Cyberattacks
Print Format—90 pages, 2013—**RTC**
Member $35.00 | Nonmember $59.00
Ebook—**WRTC**
Member FREE | Nonmember $59.00

Transforming Cybersecurity: Using COBIT®5
Print Format—190 Pages, 2013—**CB5TC**
Member TBD | Nonmember TBD
Ebook—**WCB5TC**
Member FREE | Nonmember TBD

The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, Second Edition
784 pages, 2013—**4JBSS**
Member $74.00 | Nonmember $84.00

Vendor Management: Using COBIT® 5
Print Format—196 Pages, 2013—**CB5VM**
Member TBD | Nonmember TBD
Ebook—**WC35VM**
Member TBD | Nonmember TBD

The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition
912 pages—**97WWAH**
Member $50.00 | Nonmember $60.00

Featured...

www.isaca.org/featuredbooks

Illustrating PRINCE2®: Project Management in Real Terms
226 pages, 2012—**15-ITIP**
Member $30.00 | Nonmember $40.00

Information Security Governance Simplified: From the Boardroom to the Keyboard
431 pages, 2011—**54-CRC**
Member $80.00 | Nonmember $90.00

Introduction to Healthcare Information Technology, 1st Edition
320 pages, 2013—**16-IT**
Member $73.00 | Nonmember $83.00

IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud
WITCOCI Italian, Ebook—PDF Format
(purchase online only)
Member FREE | Nonmember $50.00

Once MoreUnto the Breach: Managing Information Security in an Uncertain World
246 pages, 2012—**14-ITOM**
Member $40.00 | Nonmember $50.00

Wireless Network Security A Beginner's Guide
368 pages, 2012—**30-MWNS**
Member $40.00 | Nonmember $50.00

* Published by ISACA and ITGI

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

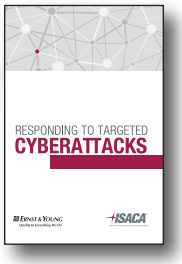
All prices are listed in US Dollars and are subject to change

SUPPLEMENT

NEW/FEATURED BOOKS www.isaca.org/newbooks

Responding to Targeted Cyberattacks

NEW



By ISACA

The threat environment had radically changed over the last decade. Most enterprises have not kept pace and lack the necessary fundamentals required to prepare and plan against cyberattacks.
To successfully expel attackers, the enterprise must be able to:
- Conduct an investigation
- Feed threat intelligence into a detailed remediation/eradication plan
- Execute the remediation/eradication plan

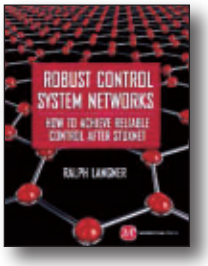
This publication covers a few of the basic concepts that will help answer the key questions posed by a new outlook that a breach WILL eventually occur. *Responding to Targeted Cyberattacks* is available for purchase in ebook and as print format. ISACA members have complimentary download access to the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

Print Format—90 pages, 2013—**RTC.** Member $35.00 Nonmember $59.00

Ebook—**WRTC.** Member FREE Nonmember $59.00

Robust Control System Networks: How to Achieve Reliable Control After Stuxnet

NEW



By: Ralph Langner

"This is the first great, 5-star ICS security book." *Dale Peterson, Digital Bond*
"Read *Robust Control System Networks* — it's brief, concise, well-written, full of compelling anecdotes, and groundbreaking" *Richard Bejtlich, TaoSecurity*

He was the researcher who was one of the first to identify and analyze the infamous industrial control system malware "Stuxnet," and has now written a book that takes a new, radical approach to making Industrial control systems safe from such cyber attacks: design the controls systems themselves to be "robust."

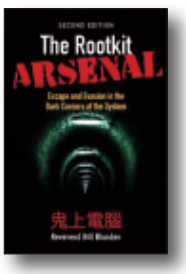
Other security experts advocate risk management, implementing more firewalls and carefully managing passwords and access. Not so this book: those measures, while necessary, can still be circumvented. Instead, this book shows in clear, concise detail how a system that has been set up with an eye toward quality design in the first place is much more likely to remain secure and less vulnerable to hacking, sabotage or malicious control.

It blends several well-established concepts and methods from control theory, systems theory, cybernetics and quality engineering to create the ideal protected system. The book's maxim is taken from the famous quality engineer William Edwards Deming, "If I had to reduce my message to management to just a few words, I'd say it all has to do with reducing variation." Highlights include:—An overview of the problem of "cyber fragility" in industrial control systems - How to make an industrial control system "robust," including principal design objectives and overall strategic planning—Why using the methods of quality engineering like the Taguchi method, SOP and UML will help to design more "armored" industrial control systems.

206 pages, 2013—**2MPRC.** Member $88.00 Nonmember $98.00

The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, Second Edition

NEW



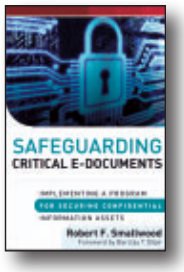
By: Bill Blunden

While forensic analysis has proven to be a valuable investigative tool in the field of computer security, utilizing anti-forensic technology makes it possible to maintain a covert operational foothold for extended periods, even in a high-security environment. Adopting an approach that favors full disclosure, the updated *Second Edition of The Rootkit Arsenal* presents the most accessible, timely, and complete coverage of forensic countermeasures. This book covers more topics, in greater depth, than any other currently available. In doing so the author forges through the murky back alleys of the Internet, shedding light on material that has traditionally been poorly documented, partially documented, or intentionally undocumented.
The range of topics presented includes how to:
- Evade post-mortem analysis
- Frustrate attempts to reverse engineer your command & control modules
- Defeat live incident response
- Undermine the process of memory analysis
- Modify subsystem internals to feed misinformation to the outside
- Entrench your code in fortified regions of execution
- Design and implement covert channels
- Unearth new avenues of attack

Features & Benefits
- Offers exhaustive background material on the Intel platform and Windows Internals
- Covers stratagems and tactics that have been used by botnets to harvest sensitive data
- Includes working proof-of-concept examples, implemented in the C programming language
- Heavily annotated with references to original sources

784 pages, 2013—**4JBSS.** Member $74.00 Nonmember $84.00

Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets



NEW

By: Robert F. Smallwood, Barclay T. Blair

Practical, step-by-step guidance for corporations, universities and government agencies to protect and secure confidential documents and business records.

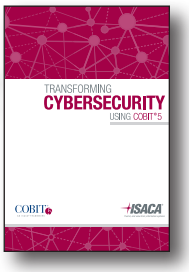
Managers and public officials are looking for technology and information governance solutions to "information leakage" in an understandable, concise format. *Safeguarding Critical E-Documents* provides a road map for corporations, governments, financial services firms, hospitals, law firms, universities and other organizations to safeguard their internal electronic documents and private communications.

- Provides practical, step-by-step guidance on protecting sensitive and confidential documents—even if they leave the organization electronically or on portable devices
- Presents a blueprint for corporations, governments, financial services firms, hospitals, law firms, universities and other organizations to safeguard internal electronic documents and private communications
- Offers a concise format for securing your organizations from information leakage

In light of the recent WikiLeaks revelations, governments and businesses have heightened awareness of the vulnerability of confidential internal documents and communications. Timely and relevant, Safeguarding Critical E-Documents shows how to keep internal documents from getting into the wrong hands and weakening your competitive position, or possible damaging your organization's reputation and leading to costly investigations.

263 pages, 2013—**98WSC** Member $75.00 Nonmember $85.00

Transforming Cybersecurity: Using COBIT 5



NEW

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.** Member TBD Nonmember TBD Ebook—**WCBTC.** Member FREE Nonmember TBD

The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition

NEW

By: Dafydd Stuttard, Marcus Pinto

The highly successful security book returns with a new edition, completely updated .Web applications are the front door to most organizations, exposing them to attacks that may disclose personal information, execute fraudulent transactions, or compromise ordinary users. This practical book has been completely updated and revised to discuss the latest step-by-step techniques for attacking and defending the range of ever-evolving web applications. You'll explore the various new technologies employed in web applications that have appeared since the first edition and review the new attack techniques that have been developed, particularly in relation to the client side.

- Reveals how to overcome the new technologies and techniques aimed at defending web applications against attacks that have appeared since the previous edition
- Discusses new remoting frameworks, HTML5, cross-domain integration techniques, UI redress, framebusting, HTTP parameter pollution, hybrid file attacks, and more
- Features a companion web site hosted by the authors that allows readers to try out the attacks described, gives answers to the questions that are posed at the end of each chapter, and provides a summarized methodology and checklist of tasks

Focusing on the areas of web application security where things have changed in recent years, this book is the most current resource on the critical topic of discovering, exploiting, and preventing web application security flaws.

912 pages—**97WWAH**. Member $50.00 Nonmember $60.00

Vendor Management: Using COBIT 5

COMING SOON

By ISACA

Vendors constitute an important part of an enterprise's external environment. As the scope, scale and complexity of vendor relationships and services increase, the risk related to them and the importance of effective vendor management increase proportionately. These relationships can have significant impact on the success of strategic projects and may generate substantive financial implications and should be a key competency for every enterprise. This practical guidance was developed to educate all stakeholders involved in the vendor management process. The guidance explores the vendor management process, supporting activities and outlines the most common threats, risk and mitigation actions.

Print Format—196 pages, 2013—**CB5VM.** Member TBD Nonmember TBD Ebook—**WCB5UM.** Member FREE Nonmember TBD

* 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

2013 CISA® EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CISA exam, order ◆
www.isaca.org/cisabooks


CISA Review Manual 2013*


CISA Review Questions, Answers & Explanations Manual 2013*


CISA Review Questions, Answers & Explanations Manual 2013 Supplement*


CISA Practice Question Database v13*

2013 CISM® EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CISM exam, order ◆
www.isaca.org/cismbooks


CISM Review Manual 2013*


CISM Review Questions, Answers & Explanations Manual 2013 Supplement*


CISM Practice Question Database v13*

2013 CGEIT EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CGEIT exam, order ◆
www.isaca.org/cgeitbooks


CGEIT Review Manual 2013*


CGEIT Review Questions, Answers & Explanations Manual 2013*


CGEIT Review Questions, Answers & Explanations Manual 2013 Supplement*

2013 CRISC EXAM REFERENCE MATERIALS

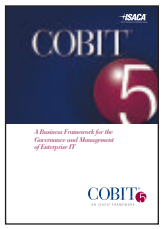
◆ To prepare for the June 2013 CRISC exam, order ◆
www.isaca.org/criscbooks


CRISC Review Manual 2013*


CRISC Review Questions, Answers & Explanations Manual 2013*

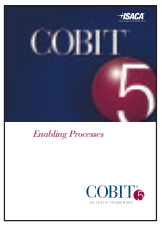

CRISC Review Questions, Answers & Explanations Manual 2013 Supplement*

COBIT 5 PUBLICATIONS
www.isaca.org/featuredbooks



COBIT 5
CB5

Member $35.00
Nonmember $50.00



COBIT 5: Enabling Processes
CB5EP

Member $35.00
Nonmember $135.00

WCB5EP—EBOOK PDF FORMAT

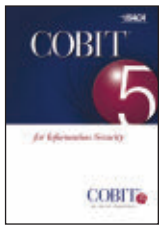
Member FREE
Nonmember $135.00

COBIT 5 Implementation
CB5IG

Member $35.00
Nonmember $150.00

WCB5IG, EBOOK PDF FORMAT

Member FREE
Nonmember $150.00

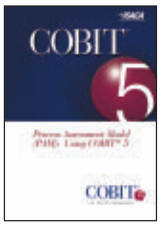


COBIT 5 for Information Security
CB5IS

Member $35.00
Nonmember $175.00

WCB5IS—EBOOK PDF FORMAT

Member $35.00
Nonmember $175.00

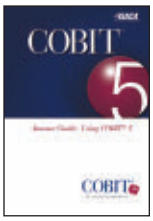


COBIT Process Assessment Model (PAM): Using COBIT 5
CPAM5

Member $30.00
Nonmember $50.00

WCPAMS—EBOOK PDF FORMAT

Member FREE
Nonmember $40.00



COBIT Assessor Guide: Using COBIT 5
CAG5

Member $30.00
Nonmember $50.00

WCAG5—EBOOK PDF FORMAT

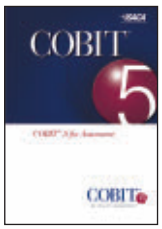
Member $30.00
Nonmember $80.00

COBIT Self-assessment Guide: Using COBIT 5
CSAG5

Member $30.00
Nonmember $50.00

WCSAG5—EBOOK PDF FORMAT

Member $30.00
Nonmember FREE



COBIT 5 for Assurance
CB5A

Member $35.00
Nonmember $175.00

WCB5A—EBOOK PDF FORMAT

Member $35.00
Nonmember $175.00

* 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

2013 CISA® EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CISA exam, order ◆

Code	Title		Nonmember	Member
CISA Review Manual 2013*				
CRM-13	English Edition		$135.00	$105.00
CRM-13C	Chinese Simplified Edition		135.00	105.00
CRM-13F	French Edition		135.00	105.00
CRM-13I	Italian Edition		135.00	105.00
CRM-13J	Japanese Edition		135.00	105.00
CRM-13S	Spanish Edition		135.00	105.00
CISA Review Questions, Answers & Explanations Manual 2013*				
QAE-13	English Edition	(950 Questions)	130.00	100.00
QAE-13C	Chinese Simplified Edition	(950 Questions)	130.00	100.00
QAE-13I	Italian Edition	(950 Questions)	130.00	100.00
QAE-13J	Japanese Edition	(950 Questions)	130.00	100.00
QAE-13S	Spanish Edition	(950 Questions)	130.00	100.00
CISA Review Questions, Answers & Explanations Manual 2013 Supplement*				
QAE-13ES	English Edition	(100 Questions)	60.00	40.00
QAE-13CS	Chinese Simplified Edition	(100 Questions)	60.00	40.00
QAE-13FS	French Edition	(100 Questions)	60.00	40.00
QAE-13IS	Italian Edition	(100 Questions)	60.00	40.00
QAE-13JS	Japanese Edition	(100 Questions)	60.00	40.00
QAE-13SS	Spanish Edition	(100 Questions)	60.00	40.00
CISA Review Questions, Answers & Explanations Manual 2011*				
QAE-11G	German Edition	(900 Questions)	130.00	100.00
CISA Practice Question Database v13 (1,050 Questions)*				
CDB-13	CD-ROM—English Edition		225.00	185.00
CDB-13W	Download—English Edition (no shipping charges apply to download)		225.00	185.00
CDB-13S	CD-ROM—Spanish Edition		225.00	185.00
CDB-13SW	Download—Spanish Edition (no shipping charges apply to download)		225.00	185.00
CAN*	Candidate's Guide to the CISA Exam and Certification (No charge to paid CISA exam registrants)		15.00	5.00

2013 CISM® EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CISM exam, order ◆

Code	Title		Nonmember	Member
CISM Review Manual 2012*				
CM-12J	Japanese Edition		115.00	85.00
CISM Review Manual 2013*				
CM-13	English Edition		115.00	85.00
CM-13S	Spanish Edition		115.00	85.00
CISM Review Questions, Answers & Explanations Manual 2012*				
CQA-12	English Edition	(700 Questions)	90.00	70.00
CQA-12S	Spanish Edition	(700 Questions)	90.00	70.00
CISM Review Questions, Answers & Explanations Manual 2012 Supplement*				
CQA-12ES	English Edition	(100 Questions)	60.00	40.00
CQA-12JS	Japanese Edition	(100 Questions)	60.00	40.00
CQA-12SS	Spanish Edition	(100 Questions)	60.00	40.00
CISM Review Questions, Answers & Explanations Manual 2013 Supplement*				
CQA-13ES	English Edition	(100 Questions)	60.00	40.00
CQA-13JS	Japanese Edition	(100 Questions)	60.00	40.00
CQA-13SS	Spanish Edition	(100 Questions)	60.00	40.00
CISM Practice Question Database v13 (900 Questions)*				
MDB-13	CD-ROM – English Edition		160.00	120.00
MDB-13W	Download – English Edition (no shipping charges apply to download)		160.00	120.00
CGC*	Candidate's Guide to the CISM Exam and Certification (No charge to paid CISM exam registrants)		15.00	5.00

2013 CGEIT EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CGEIT exam, order ◆

Code	Title	Nonmember	Member
CGM-13*	CGEIT Review Manual 2013	115.00	85.00
CGQ-13*	CGEIT Review Questions, Answers & Explanations Manual 2013 (60 Questions)	60.00	40.00
CGQ-13ES*	CGEIT Review Questions, Answers & Explanations Manual 2013 Supplement (60 Questions)	60.00	40.00
CACG*	Candidate's Guide to the CGEIT Exam and Certification (No charge to paid CGEIT exam registrants)	15.00	5.00

2013 CRISC EXAM REFERENCE MATERIALS

◆ To prepare for the June or December 2013 CRISC exam, order ◆

Code	Title	Nonmember	Member
CRR-13*	CRISC Review Manual 2013	115.00	85.00
CRQ-13*	CRISC Review Questions, Answers & Explanations Manual 2013 (200 Questions)	60.00	40.00
CRQ-13ES*	CRISC Review Questions, Answers & Explanations Manual 2013 Supplement (100 Questions)	60.00	40.00
XMXCR13-6M*	CRISC Exam Self-Study Subscription–6 Months	225.00	185.00
CACR*	Candidate's Guide to the CRISC Exam and Certification (No charge to paid CRISC exam registrants)	15.00	5.00

COBIT®

Code	Title	Nonmember	Member
COBIT 5			
CB5*	English	50.00	35.00
CB5C*	Chinese Simplified	50.00	35.00
CB5G*	German	50.00	35.00
CB5J*	Japanese	50.00	35.00
CB5SS*	Spanish	50.00	35.00
COBIT 5: Enabling Processes			
WCB5EP*	English, Ebook—PDF format (purchase online only)	135.00	FREE
CB5EP*	English, Print Format	135.00	35.00
WCB5EPG*	German, Ebook—PDF format (purchase online only)	135.00	FREE
CB5EPG*	German, Print Format	135.00	35.00
WCB5EPJ	Japanese, Ebook—PDF format (purchase online only)	135.00	FREE
CB5EPJ	Japanese, Print Format	135.00	35.00
WCB5EPS	Spanish, Ebook—PDF format (purchase online only)	135.00	FREE
CB5EPS	Spanish, Print Format	135.00	35.00
COBIT 5 Implementation			
WCB5IG*	English, Ebook—PDF format (purchase online only)	150.00	FREE
CB5IG*	English, Print Format	150.00	35.00
WCB5IGS	Spanish, Ebook—PDF format (purchase online only)	135.00	FREE
CB5IGS	Spanish, Print Format	135.00	35.00
COBIT 5 for Assurance			
WCB5A	Ebook—PDF format (purchase online only)	175.00	35.00
CB5A	Print Format	175.00	35.00
COBIT 5 for Information Security			
WCB5IS*	Ebook—PDF format (purchase online only)	175.00	35.00
CB5IS*	Print format	175.00	35.00
COBIT Process Assessment Model (PAM): Using COBIT 5			
CPAM5*	COBIT® Process Assessment Model (PAM): Using COBIT® 5	50.00	30.00
WCPAMS*	Ebook—PDF format (purchase online only)	40.00	FREE
COBIT Assessor Guide: Using COBIT 5			
CAG5*	COBIT® Assessor Guide: Using COBIT® 5	50.00	30.00
WCAG5*	Ebook—PDF format (purchase online only)	80.00	30.00
COBIT Self-assessment Guide: Using COBIT 5			
CSAG5*	COBIT® Self-assessment Guide: Using COBIT® 5	50.00	30.00
WCSAG5*	Ebook—PDF format (purchase online only) (does not include the Tool Kit)	30.00	FREE
Securing Mobile Devices Using COBIT 5 for Information Security			
WCB5SMD*	Ebook—PDF format (purchase online only)	75.00	FREE
CB5SMD*	Print format	75.00	35.00
CB4.1*	COBIT 4.1	190.00	75.00
COBIT and Application Controls: A Management Guide			
WCAC*	Ebook—PDF format (purchase online only)	55.00	FREE
CAC*	Print format	75.00	35.00
CBX*	COBIT 4.1 Excerpt	5.00	5.00
CPS2*	COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition	110.00	55.00
CBQ2*	COBIT Quickstart, 2nd Edition	110.00	55.00
COBIT Assessor Guide: Using COBIT 4.1			
WCAG*	Ebook—PDF format (purchase online only)	80.00	30.00
CAG*	Print format	100.00	50.00
COBIT Process Assessment Model (PAM): Using COBIT 4.1			
WCPAM*	Ebook—PDF format (purchase online only)	40.00	FREE
CPAM*	Print format	50.00	30.00
COBIT Self-assessment Guide: Using COBIT 4.1			
WCSAG*	Ebook—PDF format (purchase online only)	30.00	FREE
CSAG*	Print format	40.00	25.00
CBSB2*	COBIT Security Baseline, 2nd Edition	40.00	20.00
	Additional Set (5 each) Reference Cards		
	HRC2 Home Users	3.00	2.00
	PRC2 Professional Users	3.00	2.00
	MRC2 Managers	3.00	2.00
	ERC2 Executives	3.00	2.00
	SRC2 Senior Executives	3.00	2.00
	BRC2 Board of Directors/Trustees	3.00	2.00
COBIT User Guide for Service Managers			
WCUG*	Ebook—PDF format (purchase online only)	35.00	FREE
CUG*	Print format	50.00	20.00
CB4A*	IT Assurance Guide: Using COBIT	165.00	55.00
ITG9*	Implementing and Continually Improving IT Governance	115.00	55.00
SDG*	SharePoint Deployment and Governance Using COBIT 4.1: A Practical Approach	70.00	30.00
COBIT Online 4.1			
COLB*	Annual Full Subscription + Benchmarking (purchase online at *www.isaca.org/cobitonline*) ISACA members SAVE 75%	400.00	200.00 50.00

Meycor COBIT Suite

Comprehensive software for implementing COBIT 4.1 as an IT governance, security or assurance tool. (see *www.isaca.org/cobit* for descriptions and pricing)

See **NON-ENGLISH RESOURCES** for additional COBIT material.

For COBIT 4 and COBIT 4.1 Mapping please Visit *www.isaca.org/cobitmappings*.

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

VAL IT™/RISK IT

Code	Title	Nonmember	Member
Enterprise Value: Governance of IT Investments			
VITM*	Getting Started With Value Management	40.00	25.00
VITF2*	The Val IT Framework 2.0	90.00	45.00
VITB2*	The Business Case Guide—Using Val IT 2.0	40.00	25.00
VITAG*	Value Management Guidance for Assurance Professionals—Using Val IT 2.0	40.00	25.00
VITS2*	Complete Set	185.00	105.00
39-CRC	The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results	90.00	80.00
5-RO	A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance	105.00	95.00
RITF*	The Risk IT Framework	95.00	45.00
RITPG*	The Risk IT Practitioner Guide	115.00	55.00

RISK RELATED TOPICS

78-WRM	The Failure of Risk Management: Why It's Broken and How to Fix It	60.00	50.00
70-WFR	Fraud Risk Assessment: Building a Fraud Audit Program	84.00	74.00
11-CRC8	How to Complete a Risk Assessment in 5 Days or Less	98.00	88.00
84-WRM	Information Technology Risk Management in Enterprise Environments	110.00	100.00
2-HBS	IT Risk: Turning Business Threats Into Competitive Advantage	45.00	35.00
1-HHOP	The Operational Risk Handbook for Financial Companies	63.00	53.00
5-PL	Risk Management & Risk Assessment	105.00	95.00

AUDIT, CONTROL AND SECURITY—ESSENTIALS

48-CRC	Access Control, Security, and Trust: A Logical Approach	105.00	95.00
1-IT9	Accounting Information Systems, 9th Edition	324.00	314.00
93-WAAS	Auditing and Assurance Services: Understanding the Integrated Audit	235.00	225.00
6-PL	Auditing IT Infrastructures	105.00	95.00
53WAG2	Auditor's Guide for IT Auditing + Software Demo, 2nd Edition	105.00	95.00
76-WSL	Build Your Own Security Lab: A Field Guide for Network Testing	60.00	50.00
43-CRC	Building an Effective Information Security Policy Architecture	94.00	84.00
31-CRC	Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI	140.00	130.00
79-WCAF	Computer Aided Fraud Prevention and Detection: A Step by Step Guide	74.00	64.00
51-CRC	Data Protection: Governance, Risk Management, and Compliance	86.00	76.00
13-ITCAT	The Definite Guide to the C&A Transformation	80.00	70.00
50-WPM6	Effective Project Management: Traditional, Agile, Extreme, 6th Edition	70.00	60.00
1-ABES	Enterprise Security for the Executive: Setting the Tone from the Top	45.00	35.00
92-WIA	The Essential Guide to Internal Auditing, 2nd Edition	65.00	55.00
71-WCF	Essentials of Corporate Fraud	58.00	48.00
82-WACL	Fraud Analysis Techniques Using ACL	221.00	211.00
7-ART	Implementing the ISO/IEC 27001 Information Security Management System Standard	105.00	95.00
2-ABA	Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists	130.00	120.00
4-CRC4	Information Technology Control and Audit, 4th Edition	100.00	90.00
95-WISA	Interpretation and Application of International Standards on Auditing	115.00	105.00
8-PL	IT Auditing: The Process	105.00	95.00
90-WACS	IT Audit, Control, and Security	100.00	90.00
IT Control Objectives for Basel II			
WITCOB*	Ebook—PDF Format (purchase online only)	35.00	FREE
ITCOB*	Print Format	50.00	20.00
IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud			
WITCOC*	English Ebook – PDF Format (purchase online only)	50.00	FREE
WITCOCI*	Italian Ebook – PDF Format (purchase online only)	50.00	FREE
ITCOC*	English Print Format	60.00	35.00
WITAF*	ITAF: A Professional Practices Framework for IT Assurance ebook—PDF (purchase online only)	45.00	FREE
15-MIT2	IT Auditing Using Controls to Protect Information Assets, 2nd Edition	80.00	70.00
PSOX*	IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition	7.00	7.00
STDPK*	IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals	20.00	15.00
22-MSM	IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data	60.00	50.00
6-ITSOC	IT Strategic and Operational Controls	70.00	60.00
1-IIA	A New Auditor's Guide to Planning, Performing, and Presenting IT Audits	80.00	70.00
14-ITOM	Once More unto the Breach: Managing Information Security in an Uncertain World	50.00	40.00
7-SYN10	PCI Compliance, Third Edition	70.00	60.00
1-RIA	Practical IT Auditing with current Supplement	470.00	460.00
12-IT	Principles of Information Security, 4th Edition	166.00	156.00
2-SAPP	SAP Security and Risk Management, 2nd Edition	80.00	70.00
28-MSM	Security Metrics: A Beginner's Guide	50.00	40.00

AUDIT, CONTROL AND SECURITY—ESSENTIALS *(cont.)*

SOC 2: A User Guide			
WSOC*	Ebook—PDF format (purchase online only)	75.00	FREE
SOC*	Print Format	75.00	35.00
2-BAY*	Stepping Through the InfoSec Program	45.00	35.00

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

18-MAO	Applied Oracle Security: Developing Secure Database and Middleware Environments	70.00	60.00
4-DC	Audit Guidelines for DB2	80.00	70.00
10-ART	Identity Management: Concepts, Technologies, and Systems	119.00	109.00
16-IT	Introduction to Healthcare Information Technology, 1st Edition	83.00	73.00
Linux: Security, Audit and Control Features			
WLIN*	Ebook—PDF Format (purchase online only)	30.00	15.00
PLIN*	Print Format	50.00	35.00
Managing Risk in Wireless Environment: Security, Audit and Control Issues			
WW*	Ebook—PDF Format (purchase online only)	40.00	20.00
PW*	Print Format	50.00	35.00
29-ST4	A Practical Guide to IBM i and i5/OS Security and Compliance	89.00	79.00
1-MPPI	Protecting Industrial Control Systems from Electronic Threats	100.00	90.00
ODB9*	Security, Audit and Control Features Oracle® Database, 3rd Edition	55.00	40.00
ISOA3*	Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition	75.00	60.00
ISPS3*	Security, Audit and Control Features Oracle® PeopleSoft®, 3rd Edition	80.00	65.00
ISAP3*	Security, Audit and Control Features SAP® ERP, 3rd Edition	75.00	60.00
3-JBSS	Security Strategies in Windows Platforms and Applications	106.00	96.00
30-MWNS	Wireless Network Security A Beginner's Guide	50.00	40.00

NON-ENGLISH RESOURCES

3-TCA	Administración de la Seguridad de Información, 2nd Edition	55.00	45.00
1-AOCF	Computación Forense: Descubriendo los Rastros Informáticos	50.00	40.00
1-TCA2	Principios de auditoría y control de sistemas de información	60.00	50.00

CISA Examination Reference Material

Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the June 2013 CISA exam—see page S5

CISM Examination Reference Material

Study aids available in Japanese and Spanish for the June 2013 CISM exam—see page S1

COBIT 5			
CB5C*	Chinese Simplified	50.00	35.00
CB5G*	German	50.00	35.00
CB5J*	Japanese	50.00	35.00
CB5SS*	Spanish	50.00	35.00
COBIT 5: Enabling Processes			
WCB5EPG	German, Ebook—PDF format (purchase online only)	135.00	FREE
CB5EPG	German, Print Format	135.00	35.00
WCB5EPJ	Japanese, Ebook—PDF format (purchase online only)	135.00	FREE
CB5EPJ	Japanese, Print Format	135.00	35.00
WCB5EPS	Spanish, Ebook—PDF format (purchase online only)	135.00	FREE
CB5EPS	Spanish, Print Format	135.00	35.00
COBIT 5: Implementation			
WCB5IGS	Spanish, Ebook—PDF format (purchase online only)	135.00	FREE
CB5IGS	Spanish, Print Format	135.00	35.00

COBIT 3rd Edition, available at the following web site
Korean Edition—*www.isaca.or.kr*
COBIT 4.0 Edition, available at the following web sites
German Edition—*www.isaca.ch*
COBIT 4.1 Edition, available at the following web site
Chinese Simplified Edition - *www.isaca.org/getcobit*
French Edition—*www.afai.fr*
Hebrew Edition - *www.isaca.org.il*
Hungarian Edition—*www.isaca.org/getcobit*
Russian Edition—*www.isaca-russia.ru*
Spanish Edition—*www.isaca.org/getcobit*
Italian Edition - *www.aiea.it*
Japanese Edition—*www.isaca.org/getcobit*
Portuguese Edition—*www.isaca.org/getcobit*

IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud			
WITCOCI*	Ebook – PDF Format (purchase online only)—Italian	50.00	FREE

Meycor COBIT Suite

Meycor COBIT es un software completo e integrado para la implementación de COBIT como una herramienta para el Buen Gobierno de la TI, Seguridad de la TI o Aseguramiento de la TI según COBIT 4.1. (see *www.isaca.org/nonenglishbooks* para descripción y precios)

INTERNET AND RELATED SECURITY TOPICS

45-CRC	Cloud Computing: Implementation, Management, and Security	90.00	80.00
11-EL	Cyber Attacks: Protecting National Infrastructure	70.00	60.00
1-CAP3	Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 3rd Edition	48.00	38.00
10-IT	Cybersecurity: The Essential Body of Knowledge	107.00	97.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

Code	Title	Nonmember	Member
INTERNET AND RELATED SECURITY TOPICS			
95-WCSP	Cyber Security Policy Guidebook	90.00	100.00
4-MGH3	Gray Hat Hacking: The Ethical Hakers Handbook, 3rd Edition	70.00	60.00
23-MHE	Hacking Exposed Web Applications, 3rd Edition	60.00	50.00
2-MCG7	Hacking Exposed 7: Network Security Secrets & Solutions, 7th Edition	60.00	50.00
17-MHE2	Hacking Exposed Wireless: Wireless Security Secrets & Solutions, 2nd Edition	60.00	50.00
49-CRC	Honeypots: A New Paradigm to Information Security	150.00	140.00
54-CRC	Information Security Governance Simplified: From the Boardroom to the Keyboard	90.00	80.00
29ST-3	The Little Black Book of Computer Security, 2nd Edition	35.00	25.00
21-MMS	Mobile Application Security	60.00	50.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00
10-MOC2	Network Security: The Complete Reference, 2nd Edition	80.00	70.00
1-WCNR	No Root for You: A Series of Tutorials, Rants and Raves, and Other Random Nuances Therein	33.00	23.00
15-IT	Official Certified Ethical Hacker Review Guide:For Version 7.1, 1st Ed	50.00	40.00
Responding to Targeted Cyberattacks			
WRTC	Ebook—PDF Format (purchase online only)	59.00	FREE
RTC	Print Format	59.00	35.00
4JBSS	The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, Second Edition	84.00	74.00
Security Considerations for Cloud Computing			
WSCC	Ebook—PDF Format (purchase online only)	75.00	FREE
SCC*	Print Format	75.00	35.00
24-MSIEM	Security Information and Event Management (SIEM) Implementation	75.00	65.00
27-MSC	Securing the Clicks: Network Security in the Age of Social Media	50.00	40.00
2-JBSF	System Forensics, Investigation, and Response	106.00	96.00
29-MWAS	Web Application Security: A Beginner's Guide	50.00	40.00
97WWAH	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition	80.00	50.00
Transforming Cybersecurity: Using COBIT® 5			
WCB5TC	Ebook—PDF Format (purchase online only)	TBD	FREE
CB5TC	Print Format	TBD	TBD
Vendor Management: Using COBIT® 5			
WCB5VM	Ebook—PDF Format (purchase online only)	TBD	FREE
CB5VM	Print Format	TBD	TBD
IT GOVERNANCE AND BUSINESS MANAGEMENT			
94-WIFRS	An Executive Guide to IFRS: Content, Costs and Benefits to Business	50.00	40.00
3-PAGE	7 Steps to Better Written Policies and Procedures	30.00	20.00
4-PAGE	Best Practices in Policies and Procedures	36.00	26.00
1-ITG*	Board Briefing on IT Governance, 2nd Edition	7.00	7.00
6-SYN	Business Continuity and Disaster Recovery Planning for IT Professionals	70.00	60.00
BMIS*	The Business Model for Information Security	60.00	45.00
54-WCIO2	CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition	80.00	70.00
WCCS*	Creating a Culture of Security (ebook)	50.00	FREE
11-ITDG	The Data Governance Imperative	50.00	40.00
89-WEG	Empowering Green Initiatives with IT: A Strategy and Implementation Guide	60.00	50.00
13-IT	Ethics in Information Technology, 4th Edition	110.00	100.00
3-VH	Frameworks for IT Management	65.00	55.00
85-WF101	Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition	65.00	55.00
64-WGRC	Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices	173.00	163.00
20-MHE	Hacking Exposed Malware and Rootkits: Malware & Rootkits Secrets & Solutions	60.00	50.00

Code	Title	Nonmember	Member
IT GOVERNANCE AND BUSINESS MANAGEMENT *(cont.)*			
67-WHF	Human Factors in Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation	62.00	52.00
WGOALS*	Identifying and Aligning Business Goals and IT Goals (Ebook—PDF purchase online only)	35.00	20.00
15-ITIP	Illustrating PRINCE2®: Project Management in Real Terms	40.00	30.00
4-ID	Implementing Information Technology Governance: Models, Practices and Cases	110.00	100.00
46-CRC	Implementing the Project Management Balanced Scorecard	94.00	84.00
11-ITISQ	Implementing Service Quality based on ISO/IEC 20000, 3rd Edition	35.00	25.00
2-ITG*	Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition	7.00	7.00
Information Security Governance: Guidance for Information Security Managers			
W3ITG*	Ebook—PDF Format (purchase online only)	45.00	FREE
3-ITG*	Print Format	50.00	25.00
WSH*	Information Security Harmonisation: Classification of Global Guidance (Ebook—PDF format purchase online only)	40.00	FREE
50-CRC	Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement	90.00	80.00
1-BS12	Information Security Policies Made Easy, Version 12	805.00	795.00
2-PS3	Information Security Roles & Responsibilities Made Easy, Version V3	505.00	495.00
3-IGI	Information Technology Governance and Service Management: Frameworks and Adaptations	205.00	195.00
80-WITM8	Information Technology for Management: Improving Strategic and Operational Performance, 8th Edition	217.00	207.00
81-WIC	Internal Controls Policies and Procedures	90.00	80.00
4-ITIG	IT Governance: A Pocket Guide	25.00	15.00
5-AS13	IT Governance: Policies & Procedures, 2013 Edition	285.00	275.00
WGPM*	IT Governance and Process Maturity (Ebook—purchase online only)	30.00	FREE
8-ITHP	IT Governance to Drive High Performance: Lessons from Accenture	25.00	15.00
5-ITOC	IT Outsourcing Contracts: A Legal and Practical Guide	40.00	30.00
11-VH	IT Outsourcing: Part 1 Contracting the Partner	41.00	31.00
12-ITPM	IT Project Management: 30 Steps to Success	30.00	20.00
25-MIPM	IT Project Management: On Track from Start to Finish, 3rd Edition	60.00	50.00
91-WKPI	Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs, 2nd Edition	60.00	50.00
26-MDM	Master Data Management and Data Governance, 2nd Edition	70.00	60.00
9-VH	MOF—Microsoft Operations Framework V4.0: A Pocket Guide	32.00	22.00
MIC*	Monitoring Internal Control Systems and IT	70.00	55.00
2-ITO	Outsourcing IT: A Governance Guide	60.00	50.00
3-JR	A Practical Guide to Reducing IT Costs	55.00	45.00
6-RO	Principles and Practice of Business Continuity: Tools and Techniques	85.00	75.00
1-IS	The Privacy Management Toolkit	505.00	495.00
98WSC	Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets	85.00	75.00
2MPRC	Robust Control System Networks: How to Achieve Reliable Control After Stuxnet	98.00	88.00
Security Awareness: Best Practices to Secure Your Enterprise			
WSA*	Ebook—PDF Format (purchase online only)	35.00	20.00
PSA*	Print Format	50.00	35.00
13-VH	The Service Catalog	65.00	55.00
9-ITSIA	Swanson on Internal Auditing: Raising the Bar	60.00	50.00
77-WTS	Technology Scorecards: Aligning IT Investments with With Business Performance	60.00	50.00
4-ITG*	Unlocking Value: An Executive Primer on the Critical Role of IT Governance	7.00	7.00
2-ITPI	Visible OPS Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps	32.00	22.00
87-WWC	World Class IT: Why Businesses Succeed When IT Triumphs	48.00	38.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

FOUR EASY WAYS TO PLACE AN ORDER:

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

Mail completed form with payment:
ISACA/ITGI
1055 Paysphere Circle
Chicago, IL 60674-1055 USA

Fax completed order form with credit card number and expiration date to +1.847.253.1443

Phone: +1.847.660.5650
Monday-Friday, 8:00 am-5:00 pm Central Time (Chicago, Illinois, USA) Personal service—please have credit card number available. We will confirm availability and expected delivery date.

Send electronic payments in US dollars to: Bank of America, ABA #0260-0959-3
ISACA Account #22-71578
S.W.I.F.T code BOFAUS3N

RETURN POLICY

All purchases are final. No refunds or exchanges.

PUBLICATION QUANTITY DISCOUNTS

Academic and bulk discounts are available on books published by the ISACA and IT Governance Institute. Please call +1.847.660.5501 or +1.847.660.5578 for pricing information.

DELIVERY

Orders normally ship within 2-3 business days upon receipt of payment. Once shipped, delivery time can vary between 2-7 business days.

CUSTOMS

Customers are responsible for any custom duties/taxes/VAT charges levied by the country of destination. See *www.isaca.org/shipping* for further information.

SUPPLEMENT

ISACA®
Trust in, and value from, information systems

Customer Order Form

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

OFFICE USE ONLY

Vol. 4-13

U.S. Federal I.D. No. 23-7067291

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

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*

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

Name _____
FIRST MIDDLE LAST/FAMILY

ISACA Member: ☐ No ☐ Yes Member Number _____

Company Name _____

Address: ☐ Home ☐ Company

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

Fax Number ( ) _____

E-mail Address _____

Shipping Information (If different from customer information)

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

Name _____
FIRST MIDDLE LAST/FAMILY

Company Name _____
(IF PART OF SHIPPING ADDRESS)

Address: _____

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

E-mail Address _____

Code	Title/Item	Quantity	Unit Price	Total

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

Subtotal	
Sales Tax: Add sales tax if shipping to: Louisiana (LA), 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.	
TOTAL	

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 ☐ MasterCard ☐ Discover ☐ American Express ☐ Diners Club

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.

For Orders Totaling	Outside US	Within US
Up to US $30.00	US $10.00	US $5.00
US $30.01 to US $50.00	US $15.00	US $7.00
US $50.01 to US $80.00	US $20.00	US $8.00
US $80.01 to US $150.00	US $26.00	US $10.00
Over US $150.00	17% of Total	10% of Total

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.**