VOLUME 5, 2013

ISACA® Journal

Integrated Business Solutions

Featured articles:

Understanding the Core Concepts in COBIT 5

In-memory Computing—Evolution, Opportunity and Risk

How to Measure Security From a Governance Perspective

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

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

TeamMate® CM

Controls Management System

DOES IT SEEM LIKE SOMETHING'S BEEN MISSING?

WHEN IT COMES TO YOUR CONTROLS MANAGEMENT NEEDS, TRUST A PROVEN LEADER

TeamMate, the proven leader in Audit Management, has recently released TeamMate CM, a breakthrough in Compliance Management Software. Finally, the tool you have been waiting for to address SOX, A-123, and other financial reporting and IT compliance standards, brought to you by a Proven Leader.

Learn More at: TeamMateSolutions.com/CM

PRINCIPAL PARTNER

Wolters Kluwer
Audit, Risk & Compliance

VOLUME 5, 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.

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.

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 October 2013.

Auditorías Integradas—Un Modelo Práctico
Davis A. Porras Rodríguez, CISA, CISM

Does Your Cloud Have a Secure Lining?
Shah H. Sheikh, CISA, CISM, CRISC, CISSP, CCSK

Embed With SFIA—Secrets From the Missing Framework
Simon Roller, CISA, CISSP, DPSM, FBCS CITP

Recognizing Transference of Issues From a Vendor
Samuel P. Kuntz, CGEIT, ITIL V3F

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

Emo, Ergo Sum

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.*

With apologies to René Descartes, I suggest that in the 21st century, we must change his famous conclusion that he knew he existed from "I think, therefore I am" to "I buy, therefore I am." It is not so much that we live in a materialistic age. Since the dawn of civilization the quest for material wealth has been a major—some would say *the* major—motivator of human activity. With overwhelming oversimplification, it is possible to say that most of the positive growth in human endeavor has come from the creation of marketplaces and that the negative forces in our history have proceeded to undermine those markets through violence and theft.

THE INFORMATION SECURITY MARKETPLACE

We can certainly see this in the information security field. In a period of less than 50 years, we have seen the market for safeguards grow from practically nothing at all to a reported US $68.3 billion.[1] Let us be clear how that happened: enterprising technologists and business people saw a need and created valuable security products. These met with a positive response from other business people who paid to obtain a level of security consistent with their appreciation of their needs. To a very real extent, information security exists because people bought things.

The conditions of information security have changed over time, with new technologies spawning new threats. External attacks on information systems have metastasized from random exploits of individual hackers to targeted attacks by governments, terrorist groups and organized criminals. The ability of the information security community, vendors and buyers alike, to keep up with a changed security environment is under great stress. In a previous article, I discussed a report that antivirus products are no longer effective in preventing infection of computer systems and their software and data.[2]

This is a solvable problem; I am unwilling to say that the war is over and that the barbarians have won. What is unresolved in my mind is how much investment the community of buyers is willing to make in achieving victory, no matter how temporary that may be. The buyers who will move the market for security are company and governmental executives, as influenced by security professionals. These organizational leaders will determine the investment that must be made in new products.

THE NATURE OF THE THREAT

The information security market is unusual because the threats are cumulative. Old threats have not disappeared just because new ones have arisen. Information security is often compared with insurance, but that is an inexact analogy. Insurance implies the acceptance of some cost (i.e., the premiums) in order to mitigate the impact of negative events in the future. If the negative event does not occur in that policy period, one can buy more insurance and pay more premiums, implicitly spreading the cost of losses out over time. With security products, the threats remain year after year while also increasing over time. Therefore, information security costs are cumulative—the threats only disappear with the removal of the underlying technology. (For example, there is no need for a mainframe access control system once an organization has retired its last mainframe computer.) Until the technology is removed, the existing threats remain and new ones are continually added.

COMPLIANCE AND COST

The enemies of secure information are clearly gathering force. Will the marketplace respond? Will the buyers of security systems continue to pay the cumulative cost? I have exchanged some correspondence with Nigel Hedges of Melbourne, Victoria, Australia. Hedges has been employed by some of the world's most renowned information security companies and brings a skeptical viewpoint to the subject of the elasticity of the security market.

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:

He writes:

> *You would appreciate a certain level of FUD (fear, uncertainty and doubt) occurs within the anti-virus industry as a marketing vehicle to improve revenue, and this to some degree does not help customers in recognizing the real dangers that do exist…There is a degradation of senior management support and operational consistency of antimalware/security systems/[disaster recovery] (DR) because it is not new and does not win brownie points at the C-level where strategy is about the cloud with its proposed cost savings and business enablement. Being on the vendor side of the fence for most of my career, I have participated in, created and responded to many antimalware tenders, and if I look back on it, most of the time commercial considerations end up being the primary driver for selection. Price is certainly very important to help organizations show they are deriving value for money, ROI and all that lovely stuff…but I think at some point antimalware (for example) becomes a set-and-forget commodity product in the eyes of management and administration. I think this is dangerously close to complacency.*

Hedges articulates two of the factors that worry me at this time: complacency and cost. If others in the information security community share my concern about the growing power of cyberattackers—and I believe that my fears are broadly shared—have we done enough to convince those who have control over finances to pay sharply steeper costs to combat a burgeoning crisis? Historically, the expenditures for security have paralleled the increases in attacks, if slightly behind the level of the threat at any given time. The need for security has grown gradually, with certain leaps when a version of a widely used software product was released with significant vulnerabilities. It seems to me that the growth of risk to information security has reached crisis proportions, that the curve has turned exponentially upward. I wish that I could say that executives around the world were aware of this situation. As things stand, many are being asked, in essence, to finance information security companies as they develop products that will provide effective protection in changed circumstances. It is a difficult position for executives to be in. They must pay in advance for security they will (might?) receive in the future, while continuing to absorb risk today.

ADVOCACY FOR CHANGE

It may take a catastrophic information security event to wake up the buyers of information security products. That catastrophe may have already happened. The head of the US Cyber Command and director of the National Security Agency, General Keith B. Alexander—certainly someone who is in a position to know—has said attacks have resulted in the "greatest transfer of wealth in history."[3]

To a certain extent, we information security professionals are like the dog that actually caught the garbage truck; what do we do now? Some of us have been proclaiming imminent doom for so long that now that the circumstances really are direr, it is hard to regain credibility. If executives are complacent, it is in part because they have heard from us that "Civilization as We Know It Is Coming to an End" for far too long. Nonetheless, it behooves the world's information security professionals to be advocates for change.

There are enough well-documented stories in the general-interest media concerning cyberattacks that appeals to sensationalism are unnecessary, nor is there a need to endorse any particular product or vendor. Rather, security professionals should be leading efforts, along with auditors, risk managers, compliance and privacy officers, and other security stakeholders, to document the risk landscape in the times ahead and to estimate the magnitude of the investment needed to manage efforts to undermine information security. This research will give executives the wherewithal to make informed judgments on the necessary and acceptable price for security in the near future.

ENDNOTES

[1] PR Newswire, "Global Cyber Security Market to Be Worth $68.34 Bn in 2013—New Market Study on ASDReports," 10 January 2013, *www.prnewswire.com/news-releases/global-cyber-security-market-to-be-worth-6834bn-in-2013---new-market-study-on-asdreports-186335242.html*. Note that other observers put the figure higher. Such estimates can be challenged, but all agree that the market is huge.

[2] Ross, Steven J.; "Barbarians at the Ramparts," *ISACA Journal*, vol. 3, 2013. The report was in Perlroth, Nicole; "Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt," *New York Times*, 31 December 2012.

[3] Sanger, David E.; Mark Landler; "U.S. and China Agree to Hold Regular Talks on Hacking," *New York Times*, 1 June 2013

Managing Data With a Streamlined Solution

Paul Selway is president and cofounder of Redpath Consulting Group, a Minneapolis, Minnesota, USA-based cloud solutions consulting firm. Selway creates weekly blogs on cloud solutions and enjoys educating those who are not familiar with the cloud about what it can do for their business.

John Schulte is vice president of finance and technology at BestPrep, a Minnesota, USA-based nonprofit providing innovative education programs to students and teachers throughout the US.

BestPrep is a Minnesota-based nonprofit organization that offers six unique educational programs to students and teachers in the US to prepare them with business, career and financial literacy skills through experiences that inspire success in work and life. These programs provide individuals with the chance to gain real-world knowledge through fun, hands-on experiences, such as mock interviews, workplace tours, mentorships, money-management courses and technology-integration workshops. With the help of more than 2,500 volunteers per year, BestPrep reaches more than 60,000 students and educators.

CHALLENGE

Known for teaching the latest educational technology and how it can be used in the classroom to effectively engage students in learning, BestPrep's back-end systems needed to reflect the same technological savvy.

However, BestPrep was utilizing multiple data systems to manage thousands of program participants and volunteers, as well as events, sponsorships and donations. This led to multiple silos of data, limited cross-program visibility, time-consuming and manual reporting processes, and data-quality issues. BestPrep needed an integrated solution that could consolidate and centralize data, streamline reporting, and provide staff members with a cross-functional, efficient tool to assist them in their mission.

PROCESS

BestPrep began its search for an integration partner that could handle a nonprofit's specific program needs. The team started by exploring Salesforce-approved partners and interviewing a few select firms. Ultimately, BestPrep chose Redpath Consulting Group, a Minneapolis, Minnesota, USA-based cloud strategy integration firm that specializes in not only cloud strategy creation, but also Salesforce consultation and implementation.

SOLUTION

BestPrep is a unique organization with specialized needs and, thus, required a system that could cater to its business model. After evaluating a number of options, BestPrep decided on a Salesforce cloud solution featuring customer resource management (CRM), form assembly, email marketing and online registration applications—all to improve efficiencies of its daily operations and the effectiveness of its internal and external communications.

Why? For one, Redpath was able to customize Salesforce to meet the specific needs of BestPrep. Every organization operates differently and needs its own applications that enhance, not change, how it does business. Second, Salesforce does not require additional hardware expenses, instead making use of existing technology investments with minimal start-up cost and predictable ongoing expenses. Third, Salesforce automatically provides a disaster recovery solution in the event one of BestPrep's servers fails or a BestPrep employee's computer is lost or stolen. All data are backed up securely and automatically in the cloud without additional steps or expense. Finally, Salesforce inherently enhances staff productivity, as team members can access the most up-to-date data at any time, from any computer with an Internet connection.

The pay-as-you-go model also works well for the nonprofit organization, saving it from paying for more than it needs or uses. In the end, the Salesforce cloud was the only solution that provided BestPrep with the ability to streamline data from five databases to one, utilize applications such as iContact for newsletters and email marketing, assemble forms easily and accurately, and automate processes for an easy and simple transition from the old, inefficient methods. The Salesforce cloud empowered BestPrep to leverage enterprise-class technology as a smaller nonprofit organization.

With a high level of concentration on customer service and the project's objectives,

BestPrep spent three months in a phased rollout of a custom, integrated Salesforce strategy. There were a few programs based around the school year, so those programs were prioritized and launched in the first month, leveraging the speed and ease at which cloud solutions can be deployed, as compared to their hardware and software counterparts. These programs took BestPrep's existing five databases and streamlined them into one, giving staff members an enhanced global view of data, including, for example, information on which individuals were volunteering for what programs and which students enrolled in and paid for the different classes.

RESULTS

By consolidating five disparate databases into one centralized cloud-based system, BestPrep is now a collaborative organization in which the most accurate data are visible to all staff members as needed and/or permitted. BestPrep employees are also now able to pull reports accurately and on demand in 15 minutes, instead of the two days the forms used to require. BestPrep is also seeing improved insights into the services provided, as well as the number of volunteers and students being utilized across all programs.

In addition to the increased administration efficiencies, the Salesforce cloud has alleviated manual tasks for BestPrep employees, such as reformatting every donor or student list into one common format before moving forward with uploading it into a system. Perhaps one of the best benefits has been the online registration capability that allows students and teachers to register for programs from any device with an Internet connection. This has not only proved convenient for BestPrep participants, but it has also improved the perception of BestPrep as a leading technology education organization.

> "Organizations should evaluate the time and expense they are currently exhausting trying to access or create information."

As for advice for other organizations, BestPrep encourages every organization to consolidate its databases, whether or not they reside in the cloud. Organizations should evaluate the time and expense they are currently exhausting trying to access or create information, when it could—and should—be right at their fingertips.

Today, BestPrep is enjoying automated processes, reduced manual labor, more consistent outcomes, and a significantly enhanced global view of the organization and its performance.

Enjoying this article?

- Check out ISACA's cloud guidance.
  www.isaca.org/cloud
- Discuss and collaborate on big data and service management in the Knowledge Center.
  www.isaca.org/knowledgecenter

Where the Rubber Meets the Road

Vasant Raval, DBA, CISA, ACMA, is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interests include information security and corporate governance. Opinions expressed in this column are his own and not those of Creighton University. He can be reached at *vraval@creighton.edu*.

Ethics is a practical social activity, not a utopian concept to be contemplated in the abstract.[1] In this column, we take a hard look at the realities of information ethics programs and ponder over the question: Can such a thing be effective and, if it can be, under what conditions? Theories and paradigms help us get ready to take action, but practical ways to detect, manage and attempt to prevent ethical lapses are important to the real world. Despite their pervasiveness, we know little about how to manage and even survive the aftermath of ethical failures.[2]

If there is one lesson from history that provides an important beginning, it is this: Unethical behavior happens; what is undetermined is *when* and by *whom*, not *if*. And this is despite good intentions on most everyone's part, including the one who is seen as the violator of our trust who believes that he has done no wrong.

Just recently, a sudden media surge focused on Edward Snowden, who leaked documents from US National Security Agency (NSA) programs to make the point that US citizens' privacy is being encroached upon by their government and that their democratic rights are at risk. He is convinced he did nothing wrong, while the US Department of Justice claims that he performed a criminal act by leaking secret documents, breaking a condition of his employment. Many themes emerge from this story: privacy, national security risk and monitoring such risk factors, freedom of speech, inner conviction of what is right and what is wrong, whistleblowers perceived as heroes or criminals, and breaking the law. How do you sort all this out if you are the head of the NSA?

A first realization to be considered is that it is impractical to divide the world into good people and bad people and use it to develop tactics to generate appropriate behavior. At times, ordinary, decent individuals exercise indiscretion, and those who habitually violate ethical precepts may surprise us with remarkably humane deeds. Just about anyone could end up in an indiscretion; to minimize ethical misconduct, groups—formal and informal—could do more to lay out the rules that, when obeyed, will result in trust in others. Forceful behaviors emerge from strong ties with an organization (e.g., neighborhoods, communities, societies, businesses). Therefore, we focus on those drivers that help people embrace and adopt group norms.

Another way to look at this is from the perspective of self-interest of a member of the community or an employee. Self-interest can often be a strong motivation for individuals to get ahead and materially prosper quickly and at any cost. When people focus on self-interest at the cost of group interest, lapses occur that harm the well-being of the group. In practice, group norms of governance invariably focus on helping members of the group to be aware of, and control, their self-interests.

Remember the story of the programmer, Sergey Aleynikov, who quit a US $1.2 million-a-year job at Goldman Sachs for greater riches in 2009? Before he left Goldman, he uploaded the firm's high-frequency trading code—the secret sauce—to a server overseas and then downloaded it on to a pen drive with a view to replicate it at his new employer.[3] Temptations resulting from self-interest could cause havoc in the IT space; Goldman's intellectual property and substantial future revenues from it were at risk—all because of one person's self-interest.

ETHICAL LEADERSHIP

Beyond any doubt, the environment of the entity (i.e., workplace, family) takes the color and spirit of the leader. No code of ethics will work unless the environment—the tone at the top—supports it unconditionally. People learn vicariously and do what you do, not what you say. Since the culture of the entity overlaps with the character of its leader, it is hard to separate the two, for the tone at the top is just a derivative of the leader's moral cognition. If the followers do not see integrity in their leader, it is likely that they will not take the written word seriously. A self-sacrificing leader

has a better chance of making the environment drive ethical behavior than a self-interested leader.[4]

Honesty and integrity are pillars of the ethical climate. Without honesty, stakeholders doubt that they are engaging with the leadership in an open discussion—that there is transparency in communication. To reinforce honesty, leader behavior consistent with communication is key to creating an effective ethical climate. Managers not acting according to the code either introduce noise into the communication process or provide direct information that a convention does not really exist.[5]

When the tone at the top reinforces the code and related rules by force of day-to-day behavior, these become a convention, a custom or common law of the organization. Stakeholders follow the code because it is customary, expected and well-known to those who are responsible to abide by it. To make the code and related rules a strong custom, their nature and importance, including the consequences of failure to act accordingly, must be routinely and clearly communicated. A convention formed in this way can be quite effective in motivating people to follow the set norms.

CONVENTION

How a convention takes root can be seen by examining the elements of convention. These elements include the utility of justice, conditional motives, the usual force of passions, intelligibility, moral approbation and language.[6] The utility of justice emphasizes the influence of how others are acting. Others' behavior reinforces expected behavior and, thus, in a collective sense, creates the environment of predictability and trust. Of course, any single individual's act is not enough; the assumption is that everyone exhibits desired behaviors, i.e., cooperates for the good of the collective. In cooperating with others, there is the force of self-interest—in the sense that you and your possessions are protected from violators. No harm is normally expected because the convention draws all actors to respect others' rights—their duties—to hold the society in a predictable balance. Intelligibility has to do with the recognition of what others are doing, much like creating a brand reputation that implicitly declares the traits of the brand. Once intelligible, the force of convention influences the collective and makes everyone want to be part of the convention. When a (summary) rule becomes a practice rule, members of the society are informed to not violate the rule when working on their self-interest. Moral approbation imposes consequences of indiscretion on violators of rules.

Finally, for the transition from paradigms to practice, the convention should become part of the common language of the entity. Without this transition, the convention remains opaque and may be subject to misinterpretation.

MORAL AWARENESS

When good people behave in pathological ways that are alien to their nature, they are suffering from ethical blindness.[7] Ethical blindness suggests the temporary inability of a decision maker to see the ethical dimension of a decision at stake. It is assumed here that people deviate from their own values and principles. Ethical blindness is context-bound and, thus, a temporary state. Ethical blindness is unconscious; the person suffering such blindness cannot access or does not use those values when making a decision.[8] Doing the right thing begins with an awareness that an ethical question exists and this presupposes that the person is not ethically blind at the time.

> Doing the right thing begins with an awareness that an ethical question exists.

Awareness of an ethical dilemma is the initial stage in which the questions of right and wrong first emerge. If you are not aware, you cannot recognize the problem and, therefore, you cannot address the problem. However, just because you are aware of the dilemma, it does not automatically mean that you will arrive at the right behavior. Moral awareness is a rational process that allows the person facing the dilemma to interpret it in a conscious manner. Unfortunately, people suffer from bounded rationality (bounded ethicality). Individuals do not see the moral components of an ethical decision, not because they are morally uneducated, but because people are cognitively limited and cannot make perfect and accurate decisions.[9] A person facing an ethical dilemma should have the commitment to ethical conduct and should be able and willing to wade through the process of doing the right thing. This is where the leadership of the organization and the tone at the top come into play. Moral commitment should be motivated by strong ethical leadership, include constant communication of the convention and relevant examples related to the convention, and comprise leadership's willingness to provide help—all these aspects clearly play a part in generating the right behavior by members of the organization.

RESTORING TRUST

As the NSA story suggests, restoring trust after an ethical lapse can be a nightmare. Not doing anything is not an option; immediate and swift actions are necessary to restore trust, reinforce the convention and communicate consequences of the violation. People learn from concrete examples of what happened and how the leadership dealt with the wrongdoing. Compliance, if not enforced, will marginalize the convention and make people interpret the code according to their beliefs. Although compliance is often no more than a corrective action and cannot be taken without detecting the wrong in the first place, it still serves the important role of laying down consequences and confirming the rules of behavior.

> "Immediate and swift actions are necessary to restore trust."

SELF-REGULATION

Technological changes bring new risk and reward. For example, bring your own device (BYOD) was not a significant question 10 years ago; today, it is an opportunity that comes with myriad risk factors. Nanotechnology, big data and virtual currencies are streaming in a whole host of questions, both technology- and business-related. Business models are changing at an unprecedented pace.

Change implies progress in tandem with new uncertainties. For this to result in a net positive, uncertainties need to be identified and harnessed while leveraging the obvious benefits of the change. Because of its proximity to the change, the entity that experiments with a new technology is morally responsible to lead the search for guidance on desired behavior. For example, enterprises such as Google and Facebook should set the tone as exemplars on the issues of privacy, IBM and Amazon should help develop benchmarks for cloud services, and Apple and Samsung should show the way to right conduct in the deployment of mobile devices. If those at the frontier who are fortunate to experience the new environment will not lead, regulators will likely step in.[10] Since regulators may know little about the change and its consequences, the rules of compliance may end up as counterproductive in large measure.

Some technological changes can be monitored and evaluated by a group of firms instead of a single corporation. The problems evident in the use of virtual currency (e.g., the case of Liberty Reserve) can be avoided if the players in the world of virtual currency unite and at least initially agree to self-regulate. Firms in the financial services industry know about programmed, fast trading and should lead a search for moral guidance. Nanotechnology start-ups should be responsible to develop guidelines for their industry for they know more about their products, processes and the impact on norms of behavior for the common good.

CONCLUSION

Regardless of the locus of responsibility and leadership in the search for answers, two considerations are important. First, the entire value chain—from product research to after-market—should be carefully examined to ensure reasonable completeness of solutions proposed. Second, for a systematic search, even in the case of mature technologies, new deployments of existing technologies, or technologies not previously explored, frameworks such as COBIT® 5 can prove useful for relatively stable and fruitful solutions.

ENDNOTES

1 Bird, F.B.; *The Muted Conscience: Moral Silence and the Practice of Ethics in Business*, Greenwood Publishing, 2002

2 De Cremer, D.; A.E. Tenbrunsel; M. van Dijke; "Regulating Ethical Failures: Insights From Psychology," *Journal of Business Ethics*, 95:1-6, 2010

3 Albergotti, R.; "Questions Linger in Goldman Code Case," *Wall Street Journal*, 14 June 2013, p. C1

4 Mulder, Laetitia B.; Rob M. A. Nelissen; "When Rules Really Make a Difference: The Effect of Cooperation Rules and Self-sacrificing Leadership on Moral Norms in Social Dilemmas," *Journal of Business Ethics*, 95:57-72, September 2010

5 Kline, William; "Hume's Theory of Business Ethics Revisited," *Journal of Business Ethics*, 105:163-174, 2012

6 *Ibid*. Derived from Humean ethical precepts, Kline discusses these elements in depth.

7 Zimbardo, P.; *The Lucifer Effect—Understanding How Good People Turn Evil*, Random House, USA, 2007

8 Palazzo, G.; F. Krings; U. Hoffrage; "Ethical Blindness," *Journal of Business Ethics*, 109: 323-338, 2012

9 De Cremer, D.; A.E. Tenbrunsel; M. van Dijke; "Regulating Ethical Failures: Insights From Psychology," *Journal of Business Ethics*, 95:1-6, 2010

10 Linton J. D.; S. D. Walsh; "Introduction to the Field of Nanotechnology Ethics and Policy," *Journal of Business Ethics*, 109:547-549, 2012

EARN CREDIT FOR YOUR IT KNOWLEDGE

Save time and money at Capella University

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

Online degrees in key IT fields

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

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

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

Accredited ABET Computing Accreditation Commission

Global Accreditation Center for Project Management — Accredited Program

National Security Agency — United States of America

U.S. Department of Homeland Security

Put your IT certifications to work:

capella.edu/ISACA or **1.866.670.8737**

Capella University

Washington residents may receive credit through Capella's prior learning assessment only in the bachelor's and MBA programs.

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

CAPELLA UNIVERSITY: Capella Tower, 225 South Sixth Street, Ninth Floor, Minneapolis, MN 55402, 1.888.CAPELLA (227.3552), capella.edu.

What Every IT Auditor Should Know About Transforming Data for CAATs

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.

For several decades now, advances in computers and information technology have led to the ubiquitous employment of computers in the business community, whether the entity is small or large. That growth led to a concomitant increase in the amount of data entities have and keep, due to the significant decline in the cost of storage. Today, the outcome is referred to as "big data." Considered a hot topic in IT, big data is also the result of collecting nonfinancial data along with financial data. Everything from network logs to industry and economic data is being collected. These facts drive the need for experts in using computer assisted audit tools/techniques (CAATs).

Another consideration is the number of paperless transactions that occur. These days, many transactions do not necessarily have any paper at the point of sale (e.g., e-commerce sales). How can the primary source document (i.e., data) for such a transaction be evaluated without a CAAT?

None of this is new to the average business person, but there is something many may not realize. Big data is going to get bigger—much bigger—and faster. According to the Berkeley School of Management, more data have been created in the three years 2009-2011 than in the whole of human history.[1, 2] According to one expert, in 2005, there were 130 exabytes of data in the digital universe. By 2010, it was 1,227 exabytes—a 10-fold increase. By 2015, it is predicted that the digital universe will contain 7,910 exabytes.[3] In addition, from 2011 to 2020, data being managed by IT professionals are expected to increase 50 times, with the number of IT professionals only increasing 1.5 times.[4]

Combining these facts, there is an inescapable conclusion about auditing or analyzing data, whether financial or operational objectives: Expertise in CAAT-like techniques and tools is needed to examine big data. More than ever, entities are in need of IT auditors who can properly extract and analyze mounds of data and turn them into useful information. That requires an effective methodology and an effectual set of tools.

The data warehouse segment of IT has developed a sound methodology to do just that by using extract-transform-load (ETL) techniques and tools to get various source data sets into a single warehouse, where business analytics tools are used to analyze the huge amounts of data amassed in the warehouse. This methodology should be equally beneficial to IT auditors using CAATs and big data.

USING ETL METHODOLOGY FOR CAATS AND DATA MINING

The ETL approach can be applied to CAATs and data. Most experts agree that the most difficult part of using CAATs is the data extraction phase. In *ISACA Journal*, volume 6, 2010, this column addressed the issues of extract. In summary, the primary issue was getting data from operational computers, generally online transaction processing systems, into a form and format that are compatible with the CAAT. Often, data are exported into a format that is not immediately suitable for use in the CAAT. The ideal format was presented in the previous article: a flat file with column headings. Various potential extraction formats were discussed in that article, as were preferences based on suitability of the resulting format. The need to verify the data integrity of the extracted data, compared to the original data, was also discussed.

There are three major types of issues that cause extracted data to need to be corrected or cleaned after they are extracted:

1. Formatting issues related to the way data are formatted in a particular extraction approach. For example, the export could be in a report format (e.g., a digital PDF report) and have a lot of extraneous lines of data (e.g., headings, subtotals). In addition, some reports take a single transaction and list the information on two lines.
2. The various idiosyncrasies in the way that specific data values are presented and/or formatted. For example, a negative number could have a negative sign in front of or behind the figure, or negative numbers could be put in

parentheses. Sometimes data have leading zeros or spaces or trailing zeros or spaces.

3. When data are not optimal for CAAT commands and procedures. Almost all CAATs have procedures (commands) that are dependent on certain columns being defined as numeric, character or date data. An improperly defined column results in an inability to run certain procedures from certain CAATs. There are other constraints about data mining that require the data to be a certain way.

Figure 1 provides a list of the second type, "messy data" scenarios, and **figure 2** illustrates situations of the third type.

Figure 1—Examples of Messy Data
Leading or trailing spaces
Leading or trailing zeros
Inconsistencies in the way data values are keyed
Hanging parentheses
Nonprinting characters

Figure 2—Examples of Optimizing Data
Changing case of character data to something consistent
Filling empty cells with something (e.g., "N.A." for character data)
Separating dates into four columns for day, month, year and day of week
Splitting a column into two columns or splitting off part of the data value to a separate column
Converting a column defined as character to numeric, or *vice versa*
Removing hyperlinks
Converting formulas to values

These situations create a need to clean the data—similar to cleaning data going into a data warehouse. This article refers to this intermediate process as transforming, using the same terminology as the data warehouse ETL methodology.

TOOLS FOR TRANSFORMING

The key to the transform process is understanding what needs to be transformed and having a suitable tool to perform a specific transform procedure. Whether it be formatting, cleaning messy data or optimizing data for CAAT procedures, the IT auditor needs a tool that makes the transform process as easy as possible.

Some CAATs provide specific commands related to the problems described in **figures 1** and **2**. In fact, a tool that is good at transforming data could be cost-effective even if a different CAAT is being used to perform the procedures after the data are transformed and loaded into the CAAT. Microsoft Excel can do most of these transforming procedures, and using macros, it is likely that all of them can be done in Excel. However, CAATs exist for most, if not all, of these transform needs, and are much easier and more reliable than using macros in Excel.

CONCLUSION

Efficiency and effectiveness in data mining and data analytics are highly dependent on reliable, clean data provided to the CAAT. A useful approach is the data warehouse ETL process. An earlier article addressed the process of extracting data (volume 6, 2010). This article addresses the transform process. In a data warehouse, the transform process is usually considered the most time-consuming; the same is true in using CAATs. The good news is once the extract and transform steps are properly performed, the load part, to get the data into the CAAT, is usually a simple process.

The first major point regarding transform is that, for it to be effective, the IT auditor needs to understand the procedures and commands of the CAAT in order to determine what needs to be addressed or changed in the data for those commands to execute properly. The second point is to understand the need for a sound methodology or approach to the transform process. Finally, the IT auditor needs an effectual tool that can perform most, if not all, of the three types of transform issues discussed.

ENDNOTES

[1] LightBound, *www.iquest.net/data-center/scale-computing-sannas.aspx*

[2] Industry Perspectives, "Three V's of Big Data: Volume, Velocity, Variety," 8 March 2012, *www.datacenterknowledge.com/archives/2012/03/08/three-vs-of-big-data-volume-velocity-variety/*

[3] Gantz, John; David Reinsel; "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East," IDC, December 2012, *http://idcdocserv.com/1414*

[4] EMC2, "Extracting Value From Chaos," *www.emc.com/leadership/programs/digital-universe.htm*

Member Get a Member 2013

Get Members. Get Rewarded.

Reach out and help friends, colleagues and other professionals become ISACA® members. They get the benefits of ISACA Membership. You Get Rewarded.

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

Get recruiting today. It's easy.
Learn more at *isaca.org/GetMembers*

ISACA®
Trust in, and value from, information systems

The More Members You Recruit, the Better the Rewards.

- Win an Apple® iPad mini®—get one entry into a monthly prize drawing for every new member you recruit*
- Get an Apple® iPod touch® for recruiting 5-9 new members*
- Get an Apple® iPad 2® for recruiting 10+ new members*

*Rules and restrictions apply and can be found at *www.isaca.org/getamember-rules*. Please be sure to read and understand these rules. If your friends or colleagues do not reference your ISACA member ID at the time they become ISACA members, you will not receive credit for recruiting them. Please remember to have them enter your ISACA member ID on the application form at the time they sign up.

Understanding the Core Concepts in COBIT 5

Steven De Haes, Ph.D., is associate professor at the University of Antwerp and the Antwerp Management School (Belgium) and academic director of the IT Alignment and Governance (ITAG) Research Institute and the Executive Masters in IT Governance & Assurance and Enterprise IT Architecture.
He can be contacted at *steven.dehaes@ua.ac.be.*

Roger Debreceny, Ph.D., is the distinguished professor of accounting in the Shidler College of Business, University of Hawaii at Manoa (USA).
He can be reached at *rogersd@hawaii.edu.*

Wim Van Grembergen, Ph.D., is a professor at the University of Antwerp (Belgium), executive professor at the University of Antwerp Management School and academic director of the ITAG Research Institute.
He can be contacted at *wim.vangrembergen@ua.ac.be.*

The COBIT® 5 good-practice framework for governance and management of enterprise IT (GEIT) incorporates many widely accepted concepts and theories from general management and academic IT literature. Exploring how the core principles of the framework are derived from insights from theory and literature,[1] this article provides guidance to practitioners as they apply COBIT 5 in their organizations.

GOVERNANCE OF ENTERPRISE IT AND COBIT 5

Information and related technology have become increasingly crucial in the sustainability, growth and management of value and risk in most enterprises. As a result, IT has moved from a support role to a central position within enterprises. The enhanced role of IT for enterprise value creation and risk management has been accompanied by an increased emphasis on GEIT. Enterprise stakeholders and the governing board wish to ensure that IT fulfills the goals of the enterprise.[2, 3] GEIT is an integral part of overall corporate governance. GEIT addresses the definition and implementation of processes, structures and relational mechanisms within the enterprise that enable business and IT staff to execute their responsibilities in support of creating or sustaining business value.[4] GEIT is complex and multifaceted. Members of the governing board and senior management typically need assistance in implementing GEIT. Over the years, good-practice frameworks have been developed and promoted to assist in this process.[5]

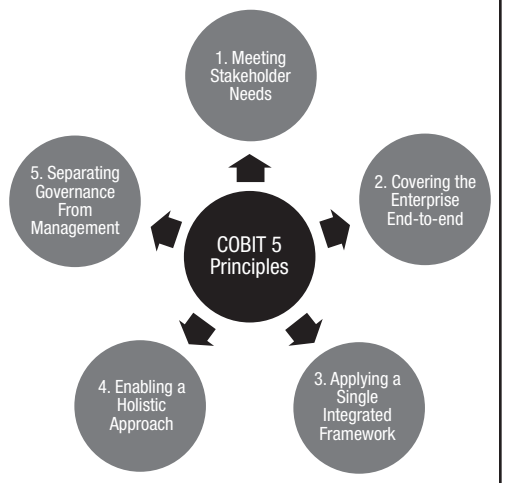
Released in 2012, COBIT 5[6] builds on and integrates 20 years of development in this field. From its foundation in the IT audit community, COBIT has become a broader and comprehensive IT governance and management framework and continues to establish itself as a generally accepted framework for IT governance.

COBIT 5 was further complemented with alignment of Val IT and Risk IT. Before COBIT 5, Val IT addressed IT-related business processes and responsibilities in enterprise value creation and Risk IT provided a holistic business view on risk management. Now, incorporated into COBIT 5, the single comprehensive framework guides managers as they implement GEIT in their enterprise.

SUBSTANTIATING THE COBIT 5 PRINCIPLES

The COBIT 5 framework is built around five core principles, illustrated in **figure 1**. Each principle is discussed in this section and relates to concepts and insights from professional and academic literature. The following subsections address the COBIT 5 principles and the concepts that are appropriate for the given principle.

Figure 1—COBIT 5 Principles



Source: ISACA, COBIT 5, 2012, *www.isaca.org/cobit*

Meeting Stakeholder Needs—Strategic Business/IT Alignment

Principle one (meeting stakeholder needs) implies that COBIT 5 provides all the required processes and other enablers to support business value creation through the use of IT. This principle closely aligns with the long-standing concept of strategic alignment. The belief that a core component of IT governance is to achieve strategic alignment between IT and the rest of the organization is a core element of COBIT. However, a continuing challenge for organizations is how to achieve alignment. To

assist organizations with enhancing strategic alignment, the COBIT 5 development team undertook research to provide guidance in understanding how enterprise goals drive IT-related goals and *vice versa*. This research was based on in-depth interviews in different sectors and expert (Delphi Method) assessments. A generic list of enterprise goals, IT-related goals and their interrelationships was established (see **figure 2**). This cascade constitutes the core entry point for COBIT 5. It suggests that organizations should start with analyzing their business/IT strategic alignment through defining and linking enterprise goals and IT-related goals.[7, 8]

COBIT 5 uses the term "enterprise goals" (as opposed to "business goals" in COBIT 4) to signal explicitly that the framework includes profit-oriented, not-for-profit and governmental enterprises. Further, COBIT 5 talks about IT-related goals (as opposed to "IT goals" in COBIT 4); this is addressed in the next subsection.

Figure 2 shows that the enterprise goal of "external compliance with laws and regulation" requires a primary focus (P) on the IT-related goals of "IT compliance and support for business compliance with external laws and regulations" and "security of information and processing infrastructure." In COBIT 5, the weighted importance of IT-related goals leads in turn to a primary focus on the subset of COBIT 5 enablers, such as management and governance processes. In this example, the subset of processes includes manage risk, manage security and manage changes.

Meeting Stakeholder Needs—The Balanced Scorecard

To verify whether stakeholder needs are indeed being met, a sound measurement process should be established. Traditional performance methods such as return on investment (ROI) capture the financial worth of IT projects and systems, but reflect only a limited (tangible) part of the value that can be delivered by IT.[9]

To facilitate a broader measurement process, the developers of COBIT 5 have built on the balanced scorecard concepts.[10, 11] As shown in **figure 2**, all enterprise goals and IT-related goals are grouped in the balanced scorecard perspectives. COBIT also provides samples of outcome metrics to measure each of those goals and to build a scorecard for IT-related activities. **Figure 3** provides examples of metrics for the customer perspective of the enterprise and IT-related goals.

Moreover, COBIT 5 provides outcome measures at the level of the 37 detailed COBIT 5 processes. An example providing specific process goals and related metrics is shown in **figure 4** for the process of *Manage security*. Of course, these process goals and metrics cannot merely be reported to stakeholders—including senior operational management and the governing board—because the stakeholders would be overwhelmed with information. Rather, the process goals and metrics must be consolidated and aggregated in a way that facilitates a usable and comprehensive balanced scorecard for the entire IT-related environment. The balanced scorecard allows the organization to determine if stakeholder needs are being met.

Covering the Enterprise End-to-end—IT Savvy

The principle of covering the enterprise end-to-end articulates that COBIT 5 covers all functions and processes within the enterprise. COBIT 5 does not focus only on the IT function, but treats information and related technologies as assets that need to be dealt with just like any other asset within the enterprise.[12] Business managers should take on responsibility for managing their IT-related assets just as they do for other assets, such as physical plant and financial and human resource assets, within their own organizational units and functions. The business must take ownership of, and be accountable for, governing the use of IT in creating value from IT-enabled business investments.[13]

A focus on covering the enterprise end-to-end implies a crucial shift in the minds of business and IT management; it comprises a move from managing IT as a cost to managing IT as an asset. This shift is an essential element of business value creation. "If senior managers do not accept accountability for IT, the company will inevitably throw its IT money to multiple tactical initiatives with no clear impact on the organizational capabilities. IT becomes a liability instead of a strategic asset."[14]

COBIT 5, then, covers both IT and IT-related business responsibilities. As a demonstration of this, COBIT 5 provides Responsible, Accountable, Consulted and Informed (RACI) charts for its processes, in which business and IT roles are included. To illustrate this, an example RACI chart for the process *Manage service agreements* is shown in **figure 5**. This RACI chart indicates that for the service level agreement (SLA) process, both business and IT functions have accountabilities and responsibilities.

Figure 2—Enterprise Goals and IT-related Goals

			Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimization of service delivery costs	Optimization of business process functionality	Optimization of business process costs	Managed business change programs	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
	IT-related Goal		**Financial**					**Customer**					**Internal**					**Learning and Growth**	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realized benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimization of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13	Delivery of programs delivering benefits on time and on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Figure 3—Example Balanced Scorecard Metrics for Enterprise and IT-related Goals

BSC Dimension	Enterprise Goal	Metric
Customer	6. Customer-oriented service culture	• Number of customer service disruptions due to IT service-related incidents (reliability) • Percent of business stakeholders satisfied that customer service delivery meets agreed-upon levels • Number of customer complaints • Trend of customer satisfaction survey results
	7. Business service continuity and availability	• Number of customer service interruptions causing significant incidents • Business cost of incidents • Number of business processing hours lost due to unplanned service interruptions • Percent of complaints as a function of committed service availability targets
	8. Agile responses to a changing business environment	• Level of board satisfaction with enterprise responsiveness to new requirements • Number of critical products and services supported by up-to-date business processes • Average time to turn strategic enterprise objectives into an agreed-upon and approved initiative
	9. Information-based strategic decision making	• Degree of board and executive management satisfaction with decision making • Number of incidents caused by incorrect business decisions based on inaccurate information • Time to provide supporting information to enable effective business decisions
	10. Optimization of service delivery costs	• Frequency of service delivery cost optimization assessments • Trend of cost assessment vs. service level results • Satisfaction levels of board and executive management with service delivery costs
	IT-related Goal	**Metric**
	07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-upon service levels • Percent of users satisfied with the quality of IT service delivery
	08 Adequate use of applications, information and technology solutions	• Percent of business process owners satisfied with supporting IT products and services • Level of business-user understanding of how technology solutions support their processes • Satisfaction level of business-users with training and user manuals • Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions

Figure 4—Example Balanced Scorecard Metrics for the Security Process

Process Goal	Related Metrics
1. A system is in place that considers and effectively addresses enterprise information security requirements.	• Number of key security roles clearly defined • Number of security-related incidents
2. A security plan has been established, accepted and communicated throughout the enterprise.	• Level of stakeholder satisfaction with the security plan throughout the enterprise • Number of security solutions deviating from the plan • Number of security solutions deviating from the enterprise architecture
3. Information security solutions are implemented and operated consistently throughout the enterprise.	• Number of services with confirmed alignment to the security plan • Number of security incidents caused by nonadherence to the security plan • Number of solutions developed with confirmed alignment to the security plan

Figure 5—End-to-end Responsibility in Managing Service Agreements

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programs/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP009.01 Identify IT services.		C		R	R	R	C		I							I	I	R	I	C	C	C	A	I	I	
AP009.02 Catalog IT-enabled services.					I	I			I							I	I	R	I	C	C	C	A	I	I	
AP009.03 Define and prepare service agreements.					R	C			C		C					C	C	R		C	R	R	A	C	C	
AP009.04 Monitor and report service levels.		I		I	I	R					C							I		I	I	I	A			
AP009.05 Review service agreements and contracts.					A	C			C		C					C	C	R		C	R	R	R	C	C	I

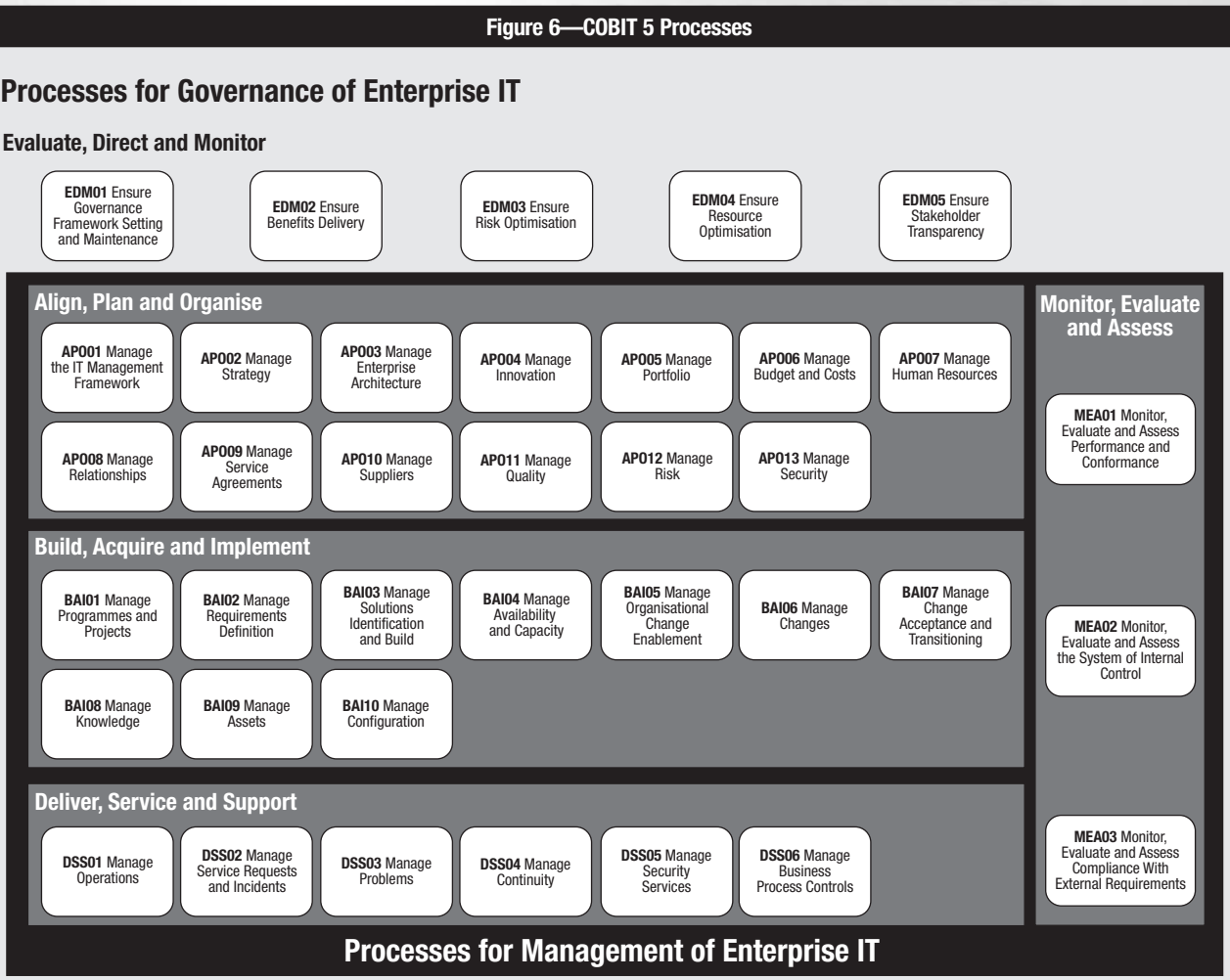
Applying a Single, Integrated Framework—COBIT/Risk IT/Val IT and Other Frameworks

Principle three (applying a single, integrated framework) explains that COBIT 5 aligns with other relevant standards and frameworks at a high level and thus can serve as the overarching framework for GEIT. ISACA® has made a major investment over the years in aligning COBIT with other frameworks including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control–Integrated Framework*, IT Infrastructure Library (ITIL), the Project Management Body of Knowledge (PMBOK), The Open Group Architecture Framework (TOGAF), and Projects in Controlled Environments, Version 2 (PRINCE 2). Many of the processes in COBIT 5 are inspired by the guidance in these frameworks. As such, many of the processes and practices in COBIT 5 relate to and align with one or more detailed frameworks in the field. To work effectively with COBIT 5 and other frameworks, a high level mapping of COBIT 5 to each is included at the process level in *COBIT 5: Enabling Processes*. Considering that COBIT 5 also integrates Risk IT and Val IT, COBIT 5 is a one-stop shop that includes in its scope previous guidance from ISACA and guidance from other standards and frameworks in the field.[15]

In its overarching approach, COBIT 5 identifies a set of governance and management enablers that includes 37 processes (see **figure 6**). At the governance layer, there are five processes in the Evaluate, Direct and Monitor (EDM) domain. These processes set out the board's responsibilities for evaluating, directing and monitoring the use of IT assets to create value for the enterprise. The EDM domain covers setting the governance framework, establishing responsibilities in terms of value (e.g., investment criteria), risk factors (e.g., risk appetite) and resources (e.g., resource optimization), and maintaining transparency on IT to stakeholders.

There are four domains defined at the management layer: Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA). The APO domain

Figure 6—COBIT 5 Processes



Source: ISACA, COBIT 5, 2012, *www.isaca.org/cobit*

concerns the identification of how IT can best contribute to the achievement of the business objectives. Specific processes within the APO domain relate to IT strategy and tactics, enterprise architecture, innovation and portfolio management. Other important processes address the management of budgets and costs, human resources, relationships, service agreements, suppliers, quality, risk, and security. The BAI domain makes IT strategy concrete by identifying the requirements for IT and managing the IT investment program and projects within that program. This domain also addresses the management of capacity; organizational change; IT change management; acceptance and transitioning; and knowledge, asset and configuration management. The DSS domain refers to the actual delivery of the IT services required to meet strategic and tactical plans. The DSS domain includes processes to manage operations, service requests and incidents, as well as the management of problems, continuity, security services and business process controls. The fourth management domain, MEA, includes processes that are responsible for the assessment of process performance and conformance, evaluation of internal control adequacy, and monitoring of regulatory compliance.[16]

Applying a Single Integrated Framework—IT Savviness

Compared to its previous versions, COBIT 5 includes a more thorough and complete involvement of business management in governing and managing IT. For example, three newly inserted processes that address specific business roles are APO3 *Manage enterprise architecture*, APO4 *Manage*

innovation and BAI05 *Manage organizational change*. Also, in line with this change, there are fewer processes in the Deliver, Service and Support (DSS) domain (six) compared to the number of processes in the Deliver and Support domain of COBIT 4.1 (13). Some of these processes were moved to a higher domain within the framework. A typical example is the shift of the *Manage service agreements* process to the APO domain, recognizing the evolution in IT operations with an increasing importance in outsourcing and cloud computing.

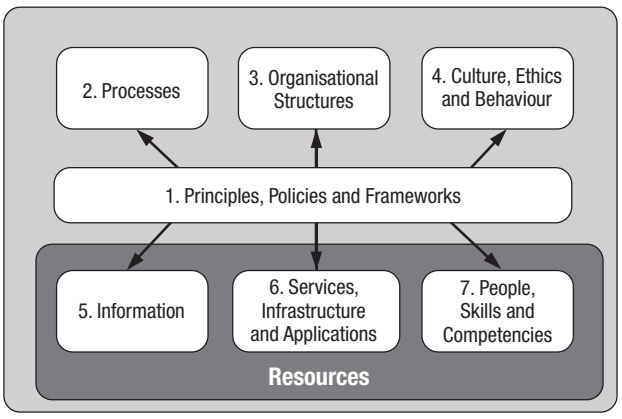
Enabling a Holistic Approach—Organizational Systems

The fourth principle (enabling a holistic approach) explains that efficient and effective implementation of GEIT requires a holistic approach, taking into account several interacting components—processes, structures and people. This implementation challenge is related to what is described in strategic management literature as the need for an organizational system, i.e., the way a firm gets its people to work together to carry out the business.[17] Such organizational systems require the definition and application, in a holistic manner, of structures (e.g., organizational units and functions) and processes (to ensure that tasks are coordinated and integrated), as well as attention to people and relational aspects (e.g., culture, values, joint beliefs).

In applying this organizational system theory to GEIT, organizations are deploying it using a holistic mixture of structures, processes and relational mechanisms.[18, 19] GEIT structures include organizational units and roles responsible for making IT-related decisions and for enabling contacts between business and IT management decision-making functions (e.g., IT steering committee). This can be seen as a form of blueprint for how the governance framework should be structurally organized. GEIT processes refer to the formalization and institutionalization of strategic IT decision making and IT monitoring procedures to ensure that daily behaviors are consistent with policies and provide input back to decision makers (e.g., IT balanced scorecard). The relational mechanisms are ultimately about the active participation of, and collaborative relationship among, corporate executives, IT management and business management, and include mechanisms such as announcements, advocates and education efforts.

COBIT 5 builds on these insights. A key change in COBIT 5 is the concept of enablers. "Enablers" are defined as factors that individually and collectively influence whether something will work—in this case, governance and management over enterprise IT. The COBIT 5 framework describes seven categories of enablers (see **figure 7**)—of which processes; organizational structures; and culture, ethics and behavior are closely related to the organizational systems concept. COBIT 5 then complements these organizational systems insights with other important enablers including principles, policies and frameworks; information; service, infrastructure and applications; and people, skills and competencies.

Figure 7—Organizational Systems of Enablers



Source: ISACA, COBIT 5, 2012, *www.isaca.org/cobit*

Separating Governance From Management—ISO/IEC 38500 (2008)

Finally, principle 5 (separating governance from management) is about the distinction COBIT 5 makes between governance and management. As discussed previously, this distinction aligns with the guidance in ISO/IEC 38500.[20] In COBIT 5, ISACA states for the first time that IT governance and IT management processes encompass different types of activities. The governance processes are organized following the EDM model, as proposed by ISO/IEC 38500. IT governance processes ensure that enterprise objectives are achieved by evaluating

stakeholder needs; setting direction through prioritization and decision-making; and monitoring performance, compliance and progress against plans. In enterprises, IT governance should be the accountability of the board of directors or equivalent. Based on these governance activities, business and IT management plans, builds, runs and monitors activities (a COBIT translation of Deming's Plan, Do, Check, Act [PDCA] cycle) in alignment with the direction set by the governance body to achieve the enterprise objectives.

CONCLUSION

In summary, GEIT is the board's accountability and responsibility and the execution of the set direction is management's accountability and responsibility.[21] COBIT 5 is primarily a framework made by and for practitioners and includes insights from IT and general management literature, including concepts and models such as strategic alignment, balanced scorecard, IT savviness and organizational systems. By clearly indicating how the core elements of COBIT 5 are built on these IT and general management insights, this article provides guidance to practitioners in their endeavors to apply COBIT 5 in their organizations.

ENDNOTES

[1] For additional details on this topic, read: De Haes, Steven; Roger Debreceny; Wim Van Grembergen, "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities," *Journal of Information Systems*, USA, 2013.

[2] De Haes, S., W. Van Grembergen; "An Exploratory Study Into the Design of an IT Governance Minimum Baseline Through Delphi Research," *Communications of AIS*, USA, 2008

[3] Thorp, J.; *The Information Paradox*, McGraw-Hill, USA, 2003

[4] Van Grembergen, W.; S. De Haes; *Enterprise Governance of IT: Achieving Strategic Alignment and Value*, Springer, USA, 2009

[5] *Ibid*.

[6] ISACA; COBIT 5, 2012, *www.isaca.org/cobit*

[7] De Haes, S., W. Van Grembergen; "Prioritizing and Linking Business Goals and IT Goals in the Financial Sector," *International Journal of IT/Business Alignment and Governance*, USA, 2010

[8] Van Grembergen, W., S. De Haes; H. Van Brempt: *Understanding How Business Goals Drive IT Goals*, 2008, *www.isaca.org*

[9] *Op cit*, Van Grembergen and De Haes, Springer, 2009

[10] Kaplan, R., D. Norton; "The Balanced Scorecard—Measures That Drive Performance," *Harvard Business Review*, USA, 1992

[11] Van Grembergen, W.; R. Saul; S. De Haes; "Linking the IT Balanced Scorecard to the Business Objectives at a Major Canadian Financial Group," *Journal for Information Technology Cases and Applications*, USA, 2003

[12] Weill, P.; J. Ross; *IT Savvy: What Top Executives Must Know to Go From Pain to Gain*, Harvard Business Press, USA, 2009

[13] *Ibid*.

[14] *Ibid*.

[15] ISACA, COBIT 4.1, USA, 2007, *www.isaca.org/cobit*

[16] *Op cit*, ISACA 2012

[17] De Wit, B.; R. Meyer; *Strategy Synthesis: Revolving Strategy Paradoxes to Create Competitive Advantage*, Cengage Learning EMEA, USA, 2005

[18] Peterson, R.; "Crafting Information Technology Governance," *Information Systems Management*, USA, 2004

[19] De Haes, S.; W. Van Grembergen; "An Exploratory Study Into IT Governance Implementations and Its Impact on Business/IT Alignment," *Information Systems Management*, USA, 2009

[20] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 38500:2008, *Corporate governance of information technology*, 2008, *http://www.iso.org*

[21] *Op cit*, Van Grembergen and De Haes, Springer, 2009

Using COBIT 5 for Data Breach Prevention

Mathew Nicho, Ph.D., CEH, SAP-SA, RWSP, is the director of the Master of Science program at the College of Information Technology at the University of Dubai (Dubai, UAE). He trains students/professionals on ethical hacking and preventive measures; teaches IT governance, audit and control; and has published papers in several international journals and conference proceedings.

Hussein Fakhry, Ph.D., is the dean of the College of Information Technology at the University of Dubai (Dubai, UAE). Fakhry's research in information systems research using systems dynamics, information systems security, e-commerce and e-business, decision support systems, applications of artificial intelligence, and assessment of academic programs has appeared in numerous international journals and international conferences.

High-profile information security breaches have become a steady feature, creating increased pressure on firms to harden their networks and take a more aggressive security posture. However, it is often not clear which security initiatives can offer firms the greatest improvements.[1] Security and privacy remain in the top 10 of key issues for information security executives, as they have been since 2003.[2] In this respect, information security has become a critical issue for information systems (IS) executives[3] and crucial to the continuous well-being of modern organizations,[4] with the result that organizations need to protect information assets against cybercrime, denial-of-service attacks, web hackers, data breaches, identity and credit card theft, fraud, and other forms of internal threats.[5] A firm's information-related assets are now among its most valuable assets[6] so the ever-increasing mobility of the workforce and the convenience of working with company information inside and outside the organization through different portable and online media have amplified any threat to a critical level. Information is a fundamental asset within any organization, thus its protection through the process of information security is of high importance.[7] The application of existing technical IS security frameworks and IS controls has been effective in preventing attacks from external entities into the organizational networks, but the mobility of the organizational staff and the IT assets along the extended networks have posed serious risk to organizational data. This is substantiated by the fact that six out of 10 employees between the ages of 18 and 35 use a personal device at work and that the average corporate worker sends and receives 112 emails per day.[8]

A careful analysis and review of the trends and statistics in data breaches in the last three years (2010 to 2012) reported in CSI computer crime surveys and Identity Theft Resource Center (ITRC) studies point out that hackers circumvent the organizational network defenses by targeting the data and the media that are at rest, in use, and in motion inside and over the extended network. Moreover, errors, mistakes and accidents on the part of the employees using data have worsened the situation such that conventional technical and sociotechnical controls are not adequate preventions. In this respect, it is imperative for organizations to categorize and protect data that are at rest, in motion and in use.

COBIT® 5 enablers and management practices can be used to prevent malicious activities and data breaches within organizations and extended networks. The detailed identification and analysis of 10 high-profile data breaches and intrusions in 2012, sourced from the ITRC database, identifed, analyzed and highlighted the vulnerabilities and missing controls that led to the breaches. The analysis revealed that 70 percent of the breaches occurred due to missing or overlooked nontechnical IT controls; that is, 30 percent of the breaches could have been prevented using technical mechanisms.

For the identified vulnerabilities, corresponding IT management practices of COBIT 5 have been selected and mapped to demonstrate not only how the identified breaches could have been prevented using COBIT management practices, but also how to effectively monitor these practices using three COBIT monitoring management processes. This article recommends a security framework based on a set of essential COBIT 5 management practices and industry-specific relevant frameworks that are required to adequately protect organizations from external and internal intrusions.

TOP 10 DATA BREACHES IN 2012

The top 10 data breaches in 2012, according to the ITRC database, were analyzed to determine the nature of the attacks and evaluate the role of technical and nontechnical IT mechanisms in these breaches.[9] These data are presented in **figure 1** with the identifying methodology and the nature of attacks for each case.

Figure 1—Top 10 Data Breaches in 2012

#	Organization	Nature of Data Breach	Methodology	Nature of Attack
1	Nationwide Mutual Insurance—Allied Insurance (Columbus, Ohio, USA)	A database on the company's computer system was compromised. The breach included names, Social Security numbers and other identifying information, such as driver's license numbers and dates of birth and, in some cases, marital status, sex, occupation, and names and addresses of employers. No credit card information was disclosed as part of the breach.	Attacked by external hackers; investigation in progress	Not identified/ assumed to be the work of skilled hackers
2	Global Payments (Atlanta, Georgia, USA)	Payment card details of 1.5 million North American customers was stolen from the company servers that housed personal information collected from merchants who applied for Global Payments' processing services, costing the company US $93.9 million in fees and fines.	Attacked by external hackers; investigation in progress	Not identified/ assumed to be the work of skilled hackers
3	New York State Electric & Gas (NYSEG) (USA)	The breach involved 1.8 million records containing Social Security numbers, dates of birth and, for some customers, bank account numbers.	A subcontractor's employee who obtained unauthorized access to customer information	Nontechnical
4	University of Nebraska (Lincoln, Nebraska, USA)	The incident involved hacking into the university database that contained personal information on more than 650,000 student, parent and employee records. It exposed the Social Security numbers, names, addresses, course grades, financial aid and other information on students who have attended the university since 1985.	Skilled attack by an undergraduate student using a known vulnerability	Not identified/ assumed to be the work of skilled hackers
5	University of North Carolina—Charlotte (North Carolina, USA)	Confidential data, including bank account and Social Security numbers for some 350,000 University of North Carolina—Charlotte students, staff and faculty, were accidentally exposed.	A system misconfiguration and incorrect access settings that made electronic data publicly available	Nontechnical
6	South Carolina Department of Revenue (USA)	Usernames and passwords were stolen by attackers to access internal systems and other resources via remote services.	A targeted phishing attack against employees; inappropriate control procedure. The system was vulnerable as it did not require dual verification to access tax returns, Social Security numbers were unencrypted, software was antiquated and IT controls were outdated.	Nontechnical
7	California Department of Social Services (USA)	Personal information for more than 700,000 home care providers and recipients was lost in the mail; part of its shipment of payroll data for home care providers was missing.	Accidental error during shipment	Nontechnical
8	California Department of Child Support Services (USA)	Personal information of approximately 800,000 people in California's child support system was lost in transit.	Four backup tapes discovered missing after being transported from an IBM facility in Colorado to California following a routine disaster recovery exercise	Nontechnical

Figure 1—Top 10 Data Breaches in 2012 *(cont.)*				
#	**Organization**	**Nature of Data Breach**	**Methodology**	**Nature of attack**
9	Emory Healthcare, Inc. (Atlanta, Georgia, USA)	Ten disks that held data on surgical patients treated between September 1990 and April 2007 went missing.	Taken from a storage location at Emory University Hospital	Nontechnical
10	Utah Department of Technology Services (USA)	The breach involved Medicaid patients and recipients of Children's Health Insurance Plan, which provides insurance coverage for children without other health insurance and who meet income guidelines. Some 780,000 records were believed to be affected and the information breached included Social Security numbers, names, dates of birth, addresses and children's health plan data.	Weak password	Nontechnical
Adapted from: Shalal-Esa, A.; "Scores of US Firms Keep Quiet About Cyber Attacks," 2013 March, *www.reuters.com/article/2012/06/13/net-us-media-tech-summit-cyber-disclosur-idUSBRE85C1E320120613*				

ANALYSIS AND DISCUSSION

While it is impossible to totally secure information systems, systems risk can be substantially reduced through effective management practices.[10] Computer security technologies have had a difficult time keeping pace with advances in computing such that the growing emphasis on user friendliness has, to some extent, adversely affected the deployment of some control mechanisms, which often leads to compromises in security design and causes problems for systems controllers and auditors.[11]

In 70 percent of the aforementioned cases, the attack happened due to the lack of effective controls rather than weak security layers.

It has been stated that information security is primarily a people problem in which technology is designed and managed by people, leaving opportunities for human error.[12] In these cases, the identification of IT access control policies is required to direct best-practice approaches within the IT security program of an organization.[13] Thus, the cases prove that while hardening the technical layers is important to prevent data breaches, the involvement of humans in information security is equally important and many examples exist where human activity can be linked to security issues.[14]

ROLE OF IT CONTROLS

The shift from technical to nontechnical methods employed by hackers has led organizations to aim for an optimal mix of technical and nontechnical aspects of IS as well as the incorporation of best practices for comprehensive generic IS governance controls. Thus, in order for information security measures to become effective, security should not be built only like a staircase of combined measures; the measures should be mutually dependent on each other.[15]

Appropriate controls are necessary to protect organizations from legal suits against negligent duty and compliance to computer misuse and data protection legislation.[16] Internal control is broadly defined as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.[17] In this respect, the COBIT 5 framework helps enterprises implement sound governance enablers in which processes are one of the seven enabler categories for governance and management of enterprise IT (GEIT).[18] Currently, implementations of IS control frameworks are on the rise worldwide due to compliance and regulatory requirements to various regulations and standards.[19]

The key guiding principle for any control implementation is to decide on the appropriate level of security since organizations are not in a position to ensure maximum security. In this respect, the amount spent should be in proportion to the criticality of the system, cost of the control and probability of the occurrence of an event, as appropriate controls are also necessary to protect organizations from lawsuits against negligent duty and compliance to computer misuse and data protection legislation.[20] Organizations frequently view information security as compliance with laws

and regulations, which is not surprising as liability is a chief concern of executives.[21] However, this is a narrow, short-sighted view of information security, as laws and regulations are geared toward protecting external stakeholders of the organization, such as customers and investors.[22]

In a survey of security professionals, the Enterprise Strategy Group (ESG) found that 72 percent of North American organizations with 1,000 or more employees have implemented one or more formal IT best-practice control and process models.[23] Further, the study found that the most widely used commercial IT control frameworks are ITIL, ISO 27002 and COBIT, which provide optimal security management. ISO/IEC 27002, COBIT, ISO 20000 and ITIL are also the most applicable and widely used frameworks to manage and maintain IT services, as IT control implementers use ITIL to define strategies, plans and processes; COBIT for metrics, benchmarks and audits; and ISO/IEC 27002 to address security issues to mitigate risk.[24]

Information security is often not addressed in a holistic and comprehensive way. When all its dimensions are taken into account, real risk exists to prevent a really secure environment. In response, 12 dimensions of IS security are proposed, focusing on the governance, audit, legal, technical, human and measurement areas that need to work together to create a secure environment.[25] Mapping these 12 dimensions into the IT control frameworks as detailed in **figure 2** reveals the comprehensive nature of technical and nontechnical IT controls.

Figure 2 illustrates that COBIT encompasses most of the dimensions of IS security, taking into account the technical and nontechnical aspects. Next, the relevant processes of COBIT (also referred to as IT controls) are analyzed to see how applying these processes can prevent breaches like the 10 described previously.

Figure 2—Dimensions of IS Security Mapped With Related IS Control Frameworks/Standards

Dimensions	Available Frameworks
Strategic/corporate governance	The high-level focus of COBIT
Governance/organizational	Evident in the four domains of COBIT
Policy	IS security policy endorsed in COBIT, ISO 27002, National Institute of Standards and Technology (NIST), IT Infrastructure Library (ITIL)
Best practice	33 IT governance best practices, ITIL best practices, COBIT
Ethical	Extended Information Systems Secure Interconnection (ISSI) model, which addresses the ethical aspect of IS security
Certification	COBIT, ITIL and ISO certifications
Legal	Regulations such as US Federal Information Security Management Act (FISMA), US Health Insurance Portability and Accountability Act (HIPAA), and the US Sarbanes-Oxley Act
Insurance	(Relevant only for insurance companies)
Personnel/human resource	COBIT, ITIL, ISO 27002 controls
Awareness	Information Security Culture Framework
Technical	Payment Card Industry Data Security Standard (PCI DSS) 2.0 and ITIL
Measurement/metrics	Guidelines given in COBIT, ISO 27004 and ITIL
Audit	COBIT

Adapted from: IT Governance Institute (ITGI), *Global Status Report on the Governance of Enterprise IT (GEIT)*, USA, 2011

PROPOSED USE OF COBIT 5

COBIT 5 consolidates and integrates these previously released ISACA frameworks: COBIT 4.1, Val IT 2.0, Risk IT and the Business Model for Information Security (BMIS). It aligns with other frameworks and standards such as ITIL, International Organization for Standardization (ISO) standards, Project Management Body of Knowledge (PMBOK), PRINCE2 and The Open Group Architecture Framework (TOGAF).

Many of the detailed COBIT 5 processes map directly to information security. All the data breach cases presented earlier are mapped to COBIT 5. **Figure 3** demonstrates how each of the COBIT 5 management practices, if implemented, could have prevented the breach. While the mapped management practices correspond to COBIT 5's plan (APO) and run (DSS) domains, the six management practices—APO01.02, 01.06, 03.02, 09.03, BAI09.01 and DSS06.06—provide inputs for the activities.

Figure 3—Data Breach Case Vulnerabilities Mapped With IS Security-related COBIT Practices

Case Studied	COBIT 5 Management Practices		Inputs	Description	Outputs	To
1, 2, 4	**APO13.01 Establish and maintain an information security management system (ISMS).** *(Deliver through supporting activities)*	RACI	Outside COBIT (enterprise security approach)		• ISMS policy • ISMS scope statement	APO01.02 DSS06.03
	DSS05.01 Protect against malware. *(Deliver through supporting activities)*			• Malicious software prevention policy • Evaluations of potential threats		APO01.04 APO12.02 APO12.03
	DSS05.02 Manage network and connectivity security. *(Deliver through supporting activities)*		APO01.06 APO09.03		• Connectivity security policy • Results of penetration tests	APO01.04 MEA02.08
	DSS05.03 Manage endpoint security. *(Deliver through supporting activities)*		APO03.02 APO09.03 BAI09.01 DSS06.06	• Information architecture • Model, OLAs, SLAs • Results of physical inventory checks • Reports of violations	• Security policies for endpoint devices	APO01.04
	DSS05.04 Manage user identity and logical access. *(Deliver through supporting activities)*		APO01.02 APO03.02	• Definition of IT-related roles and responsibilities • Information architecture model	• Approved user access rights • Results of reviews of user accounts and privileges	Internal
	DSS05.05 Manage physical access to IT assets. *(Deliver through supporting activities)*			• Approved access requests • Access logs		Internal DSS06.03
	DSS05.06 Manage sensitive documents and output devices. *(Deliver through supporting activities)*		APO03.02	• Security event logs • Security incident characteristics • Security incident tickets		Internal
3	**APO10.05 Monitor supplier performance and compliance.** *(Deliver through supporting activities)*			• Supplier compliance monitoring criteria • Supplier compliance monitoring review results		
	DSS05.04 (see above)					

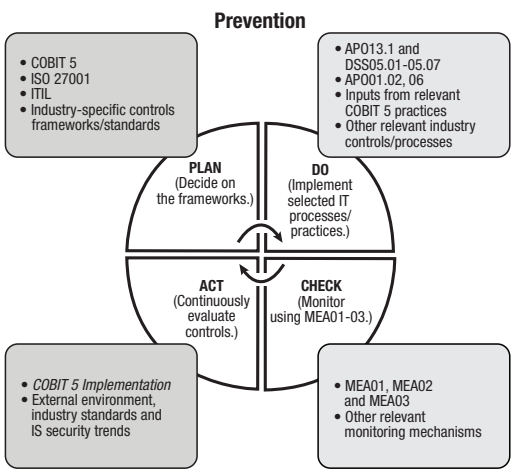
Figure 3—Data Breach Case Vulnerabilities Mapped With IS Security-related COBIT Practices *(cont.)*						
Case Studied	**COBIT 5 Management Practices**		**Inputs**	**Description**	**Outputs**	**To**
5, 10	**APO13.01; DSS05.02; DSS05.04** (see above for inputs and outputs)	**RACI**				
6	**APO13.01; DSS05.02; DSS05.04** (see above for inputs and outputs)					
7, 8, 9	**APO13.01; DSS05.03; DSS05.06** (see above for inputs and outputs)					

COBIT 5 management practices are generic and can be mapped to multiple vulnerabilities. In the 10 cases, seven management practices and six inputs are found to be essential to prevent the identified breaches. These management practices are APO13.01, DSS5.01, DSS5.02, DSS5.03, DSS5.04, DSS5.05 and DSS5.06, with APO01.02, APO01.06, APO03.02, APO09.03, BAI09.01 and DSS06.06 providing the inputs. The process enablers coming under the Monitor, Assess and Evaluate domain—MEA01, MEA02 and MEA03—ensure effective monitoring mechanisms for the selected management practices. Implementation of DSS05.07 along with the practices ensures the monitoring of security incidents, logs and tickets.

One of the advantages of COBIT 5 is its generic nature, which allows for greater freedom in customizing the enabling processes, corresponding practices and activities. This helps not only to achieve specific objectives and produce a set of outputs in support of achieving overall IT-related goals, but also suits the dynamic IS security threat environment. Looking at the highly dynamic nature of IS security threats translates into the continuous improvement of COBIT enablers to overcome current and emerging IS security threats. *COBIT 5 Implementation* provides guidelines to implement a continuous improvement process and maintain the momentum. The technical and nontechnical nature of threats prove that it is neither possible nor a good practice to separate business and IT-related activities.

Figure 4 illustrates an implementation framework that provides guidance on how to develop an implementation strategy for data breach prevention. However, frameworks, best practices and standards are useful only if they are adopted and adapted to the organization's situation. Looking from a holistic perspective, the implementation process of IS security controls takes into account selecting, customizing and mapping relevant IT controls and standards, depending on the IS security environment, industry and mandatory regulations

Figure 4—Proposed COBIT 5-based Implementation Framework for Data Breach Prevention



on a continual basis. The assessment of information is an ongoing continuous process where security assessment is an iterative process to review current functions with/against specific standards.[26] This follows Deming's Plan-Do-Check-Act (PDCA) cycle, which is used in ISO 27001.

The first stage involves deciding on relevant frameworks/standards based on a holistic IS security perspective or focusing only on COBIT 5. The next step involves selecting and implementing COBIT 5 management practices related to IS security (namely APO13.01 and DSS5.01–5.07), with the option of selecting and mapping the relevant security processes and controls for data breach prevention with COBIT 5. The use of the COBIT 5 enabler process of the MEA domain closes the feedback loop. The incorporation of the feedback loop to generated refinements and adjustments based on MEA01–MEA03 is a mechanism to monitor and ensure compliance. In this phase, the organization also has the option to select/map industry-specific or essential controls from relevant

standards/frameworks. The Act phase is very relevant to information security due to the highly dynamic nature of the vulnerabilities and methods of data breaches in which continuous review and customization of COBIT processes and relevant IT controls are done to reach the planning stage.

CONCLUSION

Despite advances in IS security technologies and the availability of relevant frameworks, standards and IT control mechanisms, statistical trends in data breaches reveal an increasing threat to organizations. Taking a sample of the top 10 high-profile cases, this article identifies the vulnerable areas and the remedial actions to counter them, thus proving that the majority of data breaches occurred due to missing or overlooked nontechnical IT controls and highlighting the emphasis that managers should place on nontechnical controls in IS security. From a practitioner's perspective, the mapping of COBIT 5 processes and management practices to the identified vulnerability provides a road map for implementation and for data breach prevention and monitoring.

ENDNOTES

[1] Johnson, E.; E. Goetz; "Embedding Information Security Risk Management Into the Extended Enterprise," *IEEE Security and Privacy*, vol. 5, 2007, p. 16-24

[2] Luftman, J.; T. Ben-Zvi; "Key Issues for IT Executives 2011: Cautious Optimism in Uncertain Economic Times," *MIS Quarterly Executive*, vol. 10, 2011, p. 203-212

[3] Culnan M. J.; E. R. Foxman; A. W. Ray; "Why IT Executives Should Help Employees Secure Their Home Computers," *MIS Quarterly Executive*, vol. 7, 2008, p. 49-56

[4] Kruger, H. A.; W. D. Kearney; "Consensus Ranking—An ICT Security Awareness Case Study," *Computers & Security*, vol. 27, 2008, p. 254-259

[5] Smith, S.; D. Winchester; D. Bunker; "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization," *MIS Quarterly Executive*, vol. 34, 2010, p. 463-486

[6] Gordon, L. A.; M. P. Loeb; T. Sohail; "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly Executive*, vol. 34, 2010, p. 567-594

[7] Thomson, K. L.; R. V. Solms; "Information Security Obedience: A Definition," *Computers and Security*, vol. 24, 2005

[8] ISACA, *COBIT® 5 for Information Security*, 2012, *www.isaca.org/cobit*

[9] While the findings in this study provide an understanding of data breaches from both technical and nontechnical perspectives, a number of caveats need to be noted. First, a small sample of 10 cases in one country does not represent the population and, hence, this study needs to be extended with a larger sample from different countries in order to generalize findings. Second, the cases are all taken from secondary sources, which may not always reveal the true cause or the events leading to the breach. Finally, while COBIT 5 is taken as the framework to demonstrate the mitigation of the identified vulnerabilities, further research can identify and map relevant IT controls/processes from related industry frameworks/standards and result in a common set of IT controls/processes for a set of commonly identified vulnerabilities.

[10] Adams, D. A.; S. Y. Chang; "An Investigation of Keypad Interface Security," *Information & Management*, vol. 24, 1993, p. 53-59

[11] Schultz, E.; "The Human Factor in Security," *Computer & Security*, vol. 24, 2005, p. 425-426

[12] Hagen, J. M.; E. Albrechtsen; J. Hovden; "Implementation and Effectiveness of Organizational Information Security Measures," *Information Management & Computer Security*, vol. 16, 2008, p. 377-397

[13] Ward and Smith; "The Development of Access Control Policies for Information Technology Systems," *Computers & Security*, vol. 21, 2002, p. 356-371

[14] *Op cit*, Kruger and Kearney

[15] Dhillon, G.; S. Moores; "Computer Crimes: Theorizing About the Enemy Within," *Computers & Security*, vol. 20, 2001, p. 715-723

[16] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, 22 May 2012, *http://coso.org/documents/Internal%20Control-Integrated%20Framework.pdf*

[17] ISACA, *COBIT 5: Enabling Processes*, 2012, *www.isaca.org/cobit*

[18] Dutta, A.; K. McCrohan; "Management's Role in Information Security in a Cyber Economy," *California Management Review*, vol. 45, 2002, p. 67-87

[19] *Op cit*, Smith, Winchester and Bunker

[20] *Op cit*, COSO

[21] Turner, M. J.; J. Oltsik; J. McKnigh; "ISO, ITIL, & COBIT Together Foster Optimal Security Investment," 2009, *www.thecomplianceauthority.com/iso-itil-a-cobit.php*

[22] Nicho, M.; "An Information Governance Model for Information Security Management," in Mellado, D.; L. E. Sánchez; E. Fernández-Medina; M. Piattini, Eds.; *IT Security Governance Innovations: Theory and Research*, IGI Global, 2012

[23] Sahibudin, S.; M. Sharifi; M. Ayat; "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," Second Asia International Conference on Modeling & Simulation, Malaysia, 2008

[24] Solms, B. V.; "Information Security—A Multidimensional Discipline," *Computers & Security*, vol. 20, 2001, p. 504-508

[25] *Op cit*, Nicho

[26] Yadav, S. B.; "A Six-view Perspective Framework for System Security: Issues, Risks, and Requirements," *International Journal of Information Security and Privacy*, vol. 4, 2010, p. 61-92

A COBIT Approach to Regulatory Compliance and Defensible Disposal

Lorrie Luellig, J.D., of Ryley Carlock & Applewhite, is the founding member and practice leader of Information Governance (RCA-IG) PC, faculty member of the Compliance, Governance and Oversight Council (CGOC), and leader of the Electronic Discovery Reference Model (EDRM) IGRM Corporations Subgroup and CGOC RIM WorkGroup. Luellig advises global clients from Fortune 100 to small privately held companies headquartered in Europe and the US.

Jake Frazier, J.D., is the information life cycle governance expert for IBM and is the executive director of the CGOC. Frazier provides assistance to corporate legal departments and law firms in identifying, evaluating and implementing in-house e-discovery and information governance solutions.

The successful IT governance plan demands a modern and transparent approach to data retention and routine disposal. Today's chief information officers (CIOs) face an unprecedented array of challenges:

- **Big data:** The volume of information that IT collects and manages continues to swell, constantly testing the processes and tools used to collect, analyze, store, process and archive data.
- **Globalization:** It is almost impossible today to find a large corporation operating in just one area of the world. Thousands of miles may separate an organization's headquarters from research and development and manufacturing, while customers, partners, suppliers and satellite offices may be located around the globe. As a result, IT must support information stored in multiple locations across a diverse infrastructure of networks, servers, desktops, laptops and mobile devices.
- **Complex, evolving regulations:** More than 100,000 international laws and regulations are potentially relevant to the information collected by Forbes Global 1000 companies. This information encompasses financial records, marketing data, emails, texts, social media posts, tweets, phone records, log data and more. Even more challenging, many of these regulations, including financial disclosure requirements and standards for data retention and privacy, are continually evolving and often vary or even contradict each other across borders and jurisdictions.
- **Tight budgets:** Despite all these challenges—and the disastrous consequences of failing to successfully manage all the data and comply with regulations on a global scale—IT is under constant pressure to reduce spending.

IT can meet all of these challenges with a comprehensive, globally aware information governance program that reduces information volumes, centralizes the management of data across all jurisdictions and ensures regulatory compliance—all while reducing costs. Many CIOs already use the COBIT® framework to support business objectives, reduce corporate risk and optimize resource use. Yet, when it comes to information governance practices related to regulatory issues, legal compliance, records retention and disposal policies, COBIT principles are often not being leveraged as broadly and as effectively as possible. However, COBIT may be the key to a successful governance program.

Also available in Brazilian Portuguese
www.isaca.org/currentissue

VALUELESS CORPORATE DATA

A lack of insight into what information needs to be kept has led many organizations to accumulate mountains of electronically generated debris in the form of excess applications, servers, storage and backup tapes that no longer have any utility.

A recent a survey of corporate CIOs and general counsels conducted at a Compliance, Governance and Oversight Council (CGOC)[1] summit found that typically only 1 percent of corporate information is on litigation hold, only 5 percent is in a records retention category and a mere 25 percent has any current business value.[2] This means that approximately 69 percent of all the data collected and maintained by most organizations have no business, legal or regulatory value at all.

A key step in creating a successful information governance program is developing the ability to identify and protect any information that has business, legal or regulatory value in order to support the legally defensible disposal of everything else. Effective defensible disposal—the ability to regularly and automatically eliminate information that has no regulatory, legal or business value—can have a dramatic

impact on information economics. Less IT budget spent on storage, servers and backup means that more can go to strategic investments. Less information to sift through means that the legal and regulatory response can be handled in a streamlined and efficient fashion while minimizing the risk associated with keeping too much or too little data, including retaining information that evolving privacy regulations require be eliminated and unnecessarily providing opposing counsel with broader discovery access than required. Less wasteful information management ultimately allows corporations to return more profit to shareholders.

> "Less wasteful information management ultimately allows corporations to return more profit to shareholders."

Historically, retention schedules have included only records—whether paper or electronic—that are distinct from the rest of the information in the organization. To achieve defensible disposal, IT stakeholders must be able to collaborate closely and transparently with the records and information management (RIM), legal and business units to create modern executable retention schedules—schedules that go beyond the scope of setting retention periods. What is deemed a "record" should include all information in the organization and incorporate retention criteria related to legal holds and business value.

RETENTION SCHEDULES IN A DIGITIZED WORLD

A retention schedule provides the legal foundation for records management and legal departments to organize corporate records and information and then detail the length of time that such records must be retained for compliance and business needs. The problem is that the retention schedules used by many organizations today were devised when paper records were the norm. Thus, they simply do not work in today's enterprises because a large amount of the information that needs to be retained or deleted is electronically generated and includes information not historically defined as a record, e.g., social media posts and tweets. This creates a critical disconnect because the information is now under the domain of IT and the company's compliance obligations will need to be linked to the thousands of applications, databases and other repositories IT manages.

Meanwhile, legal and RIM professionals possess the knowledge to set retention schedules and disposal policies according to relevant laws and regulations, but they may not have a holistic view of the IT infrastructure or any understanding of the business value of existing information. Relevant data should be identified and there should be a mechanism for disposing of information.

This disconnect is highlighted in the CGOC survey, which reported that:[3]

- Seventy-seven percent of respondents said their retention schedules were not actionable for business and IT staff
- Fifty percent said their IT departments did not use the retention schedule
- Seventy-five percent cited an inability to defensibly dispose of data as one of their greatest challenges, and many highlighted massive volumes of legacy data as financial drags on the business and compliance hazards

The goal of creating a modern, transparent and executable retention schedule is to overcome these challenges by facilitating the identification of valueless information and automating its disposal in a legally defensible manner.

BUILDING A BETTER RETENTION SCHEDULE WITH COBIT

Because a modern, executable retention schedule recognizes the dynamic nature of electronic data and the shared responsibility for information management and disposal, COBIT principles provide a solid foundation for creating one.

COBIT® 5 is based on five key principles for the governance and management of enterprise IT:

1. Meet stakeholder needs.
2. Cover the enterprise end-to-end.
3. Apply a single, integrated framework.
4. Enable a holistic approach.
5. Separate governance from management.

All of these principles are directly applicable to the creation of a modern and executable retention schedule that supports a legal framework for defensible disposal of unneeded data and takes into account the needs and roles of legal, RIM, business and IT stakeholders by:

- Understanding the flow of information through the enterprise—from creation to disposal—and enabling a holistic approach to information management

- Recognizing the multidimensional nature of data retention and disposal, and supporting interdependencies and collaboration among key stakeholders to meet all legal, regulatory and business requirements
- Having integrated governance policies and processes in place to meet the varied and diverse stakeholder needs, achieve global compliance, and enable regular updates to stay abreast of changes in the law and the business
- Making day-to-day management of information more efficient and compliant with transparent and clearly defined governance policies and processes

In such an environment, users would have the knowledge and tools they need to classify information, and IT would have the legal and records support it needs to implement a workable retention schedule and appropriately dispose of valueless information at the right time.

The following are the key elements that must be incorporated into a retention schedule for it to work in the modern information age:

1. **Apply retention schedules to all information, not just records.** The retention schedule should reflect the ongoing convergence of records management and data management and apply to all data in an organization's possession. Classify all information—including structured and unstructured data sources—as either having legal, regulatory or business value or as debris.
2. **Connect specific legal, privacy and regulatory retention obligations directly to relevant information.** The retention schedule must be supported by a transparent global framework that clearly defines how legal and regulatory obligations apply to all types of information and business users, including what is covered, who is obliged to comply, and how retention and disposal are triggered. This framework must also include evolving privacy obligations. Technology solutions, such as those that index and perform text analysis to classify data, are now available to automatically connect information to retention and disposal requirements while applying the most up-to-date legal, privacy and regulatory directives to all information.
3. **Take into account the business value of information.** This value must be explicitly determined by business stakeholders and made transparent to legal, RIM and IT. Again, technology solutions now exist that can address this long-standing concern of enterprise data managers by helping users to more easily associate information types (e.g., purchase orders or employee agreements) with specific data sources (e.g., ECM and HR systems or applications like Microsoft SharePoint) and include details on why the information is of business value and for how long.
4. **Identify where information is located.** The retention schedule should include information inventories describing where information is stored, what record classes apply to specific repositories, who was and is responsible for the content, and who manages it. With the help of a reliable data map, data stewards can more easily identify information and understand the value and obligations related to that information according to, for example, lines of business or departments.

> "Clarity encourages compliance."

5. **Communicate retention and disposal obligations in a language that stakeholders can understand.** This involves two elements. First, data users must know what is required of them when creating and identifying information. Second, data stewards must understand their responsibilities related to the disposition of information. For example, IT staff might not make sense of a disposition directive that states, "Comply with record class HUM100." A useful translation might be: "Job applications created by human resources (HR) users and stored on the shared HR drive must be permanently deleted 10 years after the termination of the employee." Clarity encourages compliance.
6. **Build in the flexibility to adapt to local laws, obligations and limitations.** Business users in each functional area and jurisdiction are the most knowledgeable about the value in, and purpose of, the information they create. The retention schedule must have the flexibility to incorporate this local knowledge. In addition, retention schedule technology solutions can be used to catalog all the specific laws and regulations in applicable regions and jurisdictions so that various exceptions and changes can be incorporated into the retention schedule and communicated to the relevant stakeholders to ensure compliance on a global scale.

7. **Include an actionable mechanism that allows legal and IT to collaborate in executing and terminating legal holds.** No retention schedule can achieve the goal of defensible disposal without a clear understanding of what information is subject to legal hold and when the hold has been released. Understanding the physical location of the information is essential, particularly for rigorous protocols such as mandated videotaped shredding of hard disk drives. With linkages clearly established between information value and IT systems, legal departments can syndicate legal holds from around the world and identify relevant records and information with local schedules and individual records flagged and held.
8. **Identify and eliminate duplicate information.** Confusion about what exactly needs to be retained and for how long can invite a tendency to "save everything, just in case." In addition to conflicting with the increasing number of privacy laws (e.g., the US Health Insurance Portability and Accountability Act, the European Directive on Protection of Personal Data) that require the deletion of certain types of information after a period of time, saving everything means that tens or even hundreds of copies of the same file are being retained. Through a transparent governance and management framework, companies can be confident they have retained the required information and disposed of all unnecessary copies.
9. **Update in real time to account for changes in laws to the business and in technology.** With the constant evolution of global legal, regulatory and privacy requirements, it is vital to stay ahead of changes and incorporate new requirements into the retention schedule immediately. Technology solutions can automatically update systems and alert data stewards to relevant changes. Several major legal research database providers also offer tools that enable users to track changing laws.
10. **Automatically apply retention schedules and legal holds to data sources that are now capable of receiving instructions from automated policy tools, and instrument all retention and disposal processes.** This ensures the consistent disposition of unnecessary data, enables legal and RIM to validate hold requests and compliance efforts, and allows information governance leaders to monitor and improve the defensible disposal program.

GOOD GOVERNANCE ACROSS THE INFORMATION LIFE CYCLE

Unprecedented data growth, global business operations, cost concerns, and a complex and constantly changing regulatory environment have created daunting information governance challenges for CIOs. However, the COBIT framework makes it possible to apply proven governance principles to overcoming these challenges by efficiently and cost-effectively shepherding the flow of corporate information through its useful life cycle and automatically eliminating information that no longer has any legal, regulatory or business value. By collaborating with legal, RIM and business stakeholders, IT can also help to create a modern, transparent and executable retention schedule that can ensure compliance while increasing business agility, reducing risk and lowering costs through the defensible disposal of valueless information.

ENDNOTES

[1] The Compliance, Governance and Oversight Council (CGOC), founded by Deidre Paknad, director of information life cycle governance at IBM Corporation, is a forum of more than 1,900 legal, IT, records and information management professionals from corporations and government agencies.
[2] Compliance, Governance and Oversight Council (CGOC), "Benchmark Report on Information Governance in Global 1000 Companies," *www.cgoc.com/register/benchmark-survey-information-governance-fortune-1000-companies*
[3] *Ibid*.

In-memory Computing—Evolution, Opportunity and Risk

William Emmanuel Yu, Ph.D., CISM, CRISC, CISSP, CSSLP, is technology vice president at Novare Technologies. Yu is working on next-generation telecommunications services, valued-added systems integration and consulting projects focusing on fixed mobile convergence and enterprise mobility applications with mobile network operators and technology providers. He is actively involved in Internet engineering, mobile platforms and information security research. Yu is also a faculty member at the Ateneo de Manila University, Philippines, and the Asian Institute of Management, Manila, Philippines.

The advent of cloud computing platforms with massive user bases and high transaction-throughput requirements has made it necessary for enterprises to find ways to scale their services in a quick and cost-effective manner. This puts pressure on system architects to cost-effectively design larger and improved systems. In the era of big data, enterprises are increasingly looking inward at huge caches of under-processed or throw-away data as resources to be mined.

Processing voluminous amounts of data requires a fast and scalable platform. In the past, deployments of these types of platforms were limited to a few large enterprises that could afford such costly data mining solutions. Nowadays, enterprises have more options. This article provides an overview of one of the options available—the in-memory database (IMDB)[1]—its evolution and the risk involved in its adoption.

IMDB technology has been touted as the cure for database performance problems—a key factor is its ability to load and execute all data in memory. This removes a substantial amount of input/output (I/O)-related performance problems associated with database systems. However, IMDB technologies introduce fundamental risk that must be considered in their deployment: durability of data, looser security controls (compared to its full database counterparts) and migration concerns. It is critical that the risk be considered when exploring the use of IMDB technology.

WAYS OF SCALING

There are two ways of scaling applications: horizontally and vertically. Horizontal scaling allows the enterprise to create applications that can take advantage by simply adding computing nodes when they need more capacity. In general, applications that require a large amount of atomic working data or perform a large amount of mutually exclusive/heavily pipe-lined transactions are suitable for horizontal parallelization. Not so long ago, this was called parallel or supercomputing.[2] Large web applications in which each web transaction is atomic and does not depend on other concurrent transactions is an example of horizontal scaling. Thus, each transaction can be routed to separate computing nodes for processing. Horizontal scaling allows Facebook, Linkedin and Twitter to handle millions of users. However, not all applications are easily portable to horizontally scaled platforms. One of the main challenges of horizontal scaling is that applications have normally not been built with horizontal scalability/concurrency in mind. Even typical desktop applications are not built to utilize the multiple central processing unit (CPU) cores available in modern commodity computing platforms. In these and similar cases, enterprises may opt to use vertical scaling.

Vertical scaling involves increasing the internal capacity of a system so it can handle more transactions. This is normally the fastest way to increase capacity without substantially changing the operating environment or the system architecture. Increasing the memory or disk storage of a computing system to handle more transactions is an example of vertical scaling. Vertical scaling is not limited to adding hardware, but can also apply to enhancing the application to get the most out of the existing resources. However, vertical scalability is generally more costly.

IT IS ALL IN RAM

There are also other ways of increasing the scalability of systems vertically. One of these is the use of in-memory computing technology. The art of scaling systems involves identifying bottlenecks when performing transactions. By

determining the key areas of slowdown, system architects can work on optimizing those areas without the need to buy more hardware. Different applications will need different levels of a particular resource and will have different bottlenecks.[3] For data-driven applications, the bottleneck is most likely disk storage or I/O. A key bottleneck exists when the application requires a lot of data interaction and subsequently disk access. A great deal of complex database applications are I/O bound.

On the other hand, memory access is normally measured in nanoseconds while disk storage access is measured in milliseconds.[4] This shows that memory access is orders of magnitude faster than disk storage access. Therefore, a possible solution to I/O-bound applications is the use of in-memory computing. All data are loaded into memory, and all transactions are executed in memory. The most tangible manifestation of in-memory computing is the IMDB. IMDBs provide substantial performance gains by storing all data in the main memory instead of disks. This provides the benefit of being able to execute I/O transactions entirely in memory. A person who memorizes the dictionary can respond faster to a word definition query than a person who did not memorize the entire dictionary and has to look up the word in a printed book.

WHO CAN BENEFIT FROM IN-MEMORY COMPUTING?

The first step in determining the need for in-memory computing is to determine if the application requires a lot of data access and manipulation. Normally, database applications can benefit from IMDB technology. Generally, any type of database transaction will be slower on a disk-based database as opposed to an IMDB. Enterprises are attracted to IMDBs because they allow easy porting of applications from disk-based database systems. Not all specifications and the aspects relating to them will be considered at the outset and used for preplanning the need for, and deployment of, IMDB technology. Sometimes, bottlenecks can be determined during the course of development, user-acceptance testing or even during actual production.

Two common ways to determine I/O bottlenecks are:

1. **I/O issues that manifest as high CPU utilization**—For example, if disk I/O is busy in a system, the I/O wait process can take a substantial amount of CPU time. In some cases, the database process shows high CPU utilization; hence, some people think that it is the CPU (processing power) that needs upgrading. In reality, it is the storage subsystem that is the bottleneck and needs to be addressed.
2. **Operating systems with I/O monitoring tools**—Linux- and UNIX-derived systems come with the highly functional iostat[5] tool. MS Windows-based systems come with perfmon.[6] Administrators must be on the lookout for parameters such as average queue length, average transfer time and percentage disk time. If these values are elevated, there is possible I/O contention.

The best way to determine if an application can benefit from IMBD technology is to try the solutions. There are a number of commercial (Oracle TimesTen,[7] SAP HANA,[8] IBM solidDB,[9] VMWare Gemfire[10]) and open-source (MySQL cluster,[11] SQLite,[12] VoltDB,[13] Druid[14]) solutions available in the market.

IS RAM VOLATILE? ARE MY DATA SAFE?

There are a number of factors that must be considered with any new technology introduced into the market, the first of which is durability. It is the first thing that generally comes to mind when using and selecting in-memory computing technology. Main memory is volatile, so when the power is cut, systems will lose data in memory. Such data loss is particularly damaging for data-driven applications. Nevertheless, the majority of in-memory solutions do have a mechanism for ensuring that data are preserved. The most common mechanism is to write back to persistent storage.

However, this requires depending on (slow) disks. However, the majority of solutions on the market use something called “lazy” or “fuzzy” write-through. This means that the transaction execution is done entirely on data stored in memory. The transactions are then stored in the form of a log buffer that is also in memory. The system will then write the data into disk for persistence. In the event of an outage, there is a chance of data loss if the log buffer was not able to complete its disk write. However, most of the database will be intact. Some IMDB solutions (e.g., Oracle TimesTen) allow one to vary the “laziness” of the write-through depending on the importance of the transactions. Low-value writes (i.e., transaction logging) defer the writes to disk over a longer period and reduce the I/O load compared to high-value writes (i.e., Airtime top-up), which synchronously write to disk for persistence all the time. This allows users to vary the “laziness” to adapt to the application requirements.

This limitation is the reason why IMDB high-availability deployments normally call for the use of replication. Network throughput is still generally faster than disk throughput. It allows multiple instances of the IMDB to synchronize the data contained in the system. The most common setup is to have a single, active database replicated with a standby or read-only database. The probability of all these systems going down simultaneously is far less than the probability of a single one failing.

On the other hand, some in-memory database solutions utilize a shared-nothing technology for replication. This means that data in these databases are distributed across a cluster of computing nodes for both load balancing and high availability. Shared-nothing technology has the additional benefit of scaling the load onto multiple computing nodes and is an example of horizontal scalability at work. Thus, shared-nothing in-memory computing technology is both vertically and horizontally scaled.

MOVING DATABASE APPLICATIONS TO IMBD

In general, most database applications can benefit from IMDB technology, largely because most applications only use a simple subset of the Structured Query Language (SQL) language. However, IMDB solutions generally do not have the full set of functionality available to disk-based relational database management systems (RDBMSs). For example, some IMDBs do not support database triggers and would not have the same level of granularity for field constraints. Limitations on field constraints (i.e., unicode characters, numeric formats) are particularly important as applications might be written to depend on enforcing field constraints at the database level. If moving to IMDB loosens the previously expected constraints, this opens up a number of field validation-related issues such as injection-type attacks.

Some IMDB platforms do not provide the same level of user and rights management that is common in disk-based relational databases. In some cases, access to a database instance provides access to all the data contained in that instance. In such cases, administrators are required to create separate instances of the database for separate applications. This requires a different user management paradigm.

Users must also consider the resources required to support IMDBs. The main resource required is memory. In particular, extremely large databases may not fit in commercially available quantities of RAM. Disk space is typically measured in tens of terabytes now. Memory, on the other hand, is measured in tens of gigabytes. Some IMDB solutions (e.g., solidDB) allow spanning between memory and disk; this limits the amount of main memory and performance that will degrade if the disk is hit. Thus, shared-nothing in-memory systems (i.e., VoltDB/HANA) outweigh those that are not shared-nothing.

Finally, it is important to remember that an application will have many different components and subsystems. Optimizing only the database will yield performance gains, but that may not be the only bottleneck present in the system. It is important to take into account outside considerations. Examples of these database-related bottlenecks outside the IMDB include connection pooling and interface conversions. In some cases, the number of database connections in the connection pool is limited, causing a transaction bottleneck. Another common problem is when an interface to the database, such as a blocking synchronous transaction or processing heavy data transformation (i.e., computations and conversions), creates a scenario where interface limitations throttle transactions and limit potential top performance. Finally, some transactions do not make it on time to the database because of application-level queuing issues (i.e., some real-time and voluminous non-real-time transactions in the same queue can starve real-time transactions).These are examples of performance issues that involve moving data into the database as opposed to performance of the database itself. It is important not to overoptimize in one area.

CHOOSING AN IMDB SOLUTION

The following are key factors to consider when choosing an IMDB solution:

- **ACID compliance/data durability**—Atomicity, consistency, isolation and durability (ACID) are compliance properties that assume that database transactions perform reliably. In particular, durability tends to vary in IMDB

implementations. Most IMDB solutions (e.g., SAP HANA, Oracle TimesTen, VMware Gemfire, MySQL Cluster, VoltDB, SQLite) are ACID-compliant. However, they typically vary when it comes to durability on disk. The "laziness" of the write-through will determine this. Some solutions (e.g., Oracle TimesTen) allow developers to adjust the "laziness" of this write-through, and others (e.g., SQLite) do not support disk write-through.

- **Data volume and scale-out requirements**—How scalable does the application need to be? A number of IMDB solutions support shared-nothing architectures that allow developers to easily create applications that horizontally scale by adding computing/storage nodes. Shared-nothing architectures (i.e., VMware Gemfire, SAP HANA, VoltDB) allow arbitrary scaling by simply adding notes. Their most important feature is that they provide resiliency by not having a single point of data failure (i.e., N+1, mirrored configuration). Some architectures (e.g., Oracle TimesTen) only support aggregate scaling where scaling is also done by adding nodes with a well-partitioned subset of data in them. Therefore, architectures that support shared-nothing can be designed to support horizontally scalable general data warehousing requirements—architectures that do not require developers to design applications for aggregate scaling.
- **SQL compatibility/SQL dialect**—Not all IMDBs are the same when it comes to SQL support. Some provide a basic set of SQL primitives (i.e., Create, Select, Insert, Delete, Update), and others provide a broader set (e.g., foreign key constraints, stored procedures). Simpler packages such as SQLite tend to have simpler SQL primitives' support but also are easier to implement. Packages with support for complex SQL primitives allow easier migration for applications that already use these primitives. This is a key reason why IMDB technology is attractive. The ease of porting depends on how broad a set of SQL primitives the application requires. This is the major reason that enterprises with existing RDBMS-backed applications prefer IMDB over NoSQL.[15]
- **Compression**—Using main memory to process transactions does put a constraint on the absolute size of data that can be processed at any given time and node. This can be circumvented by using compression at the expense of CPU processing time. Some databases (e.g., Oracle TimesTen) support this. However, the whole reason for using IMDBs is to remove a performance bottleneck (I/O). It would be counterproductive to replace it with another (CPU). Therefore, careful planning is necessary.
- **Cost**—There are a number of IMDB solutions that are open-source and commercial. The choice will primarily depend on the previously listed requirements. If the remaining candidates provide an open-source and commercial option, factors such as support and maintenance requirements come into play. Commercial and open-source with paid commercial solutions are recommended options. Open-source solutions are viable when no commercial support is necessary and the open-source package has a robust developer community.

CONCLUSION

IMDB technology is not new. It has been around for specialized high-throughput (e.g., telecommunications) use cases or caching requirements (e.g., network and authentication proxies) for quite some time. Today, the big data trend is compelling enterprises to mine their large internal hoard of data. The additional insight provided by mining this information can be invaluable for creating an enhanced user experience. The use cases, which require fast processing turnaround times, can benefit from in-memory technology. Fortunately, the industry has also adopted offerings that make it easier to consider in-memory technology, such as the introduction of SQL interfaces, shared-nothing replication and fuzzy write-through for durability.

In terms of cost, IMDB technology requires a substantial amount of memory since all data must fit into memory. Memory speeds are 100,000 to one million times faster than mechanical hard disks in terms of access times. The cost of memory is roughly 100 times that of mechanical hard disks. There certainty (1,000 to 10,000 times) is a substantial

ALTERNATIVE IN-MEMORY DATABASE ARCHITECTURE

An alternative to using a dedicated in-memory computing system such as an IMDB would be to use a regular RDBMS on a computing platform that makes exclusive use of memory-based storage devices such as solid-state drives (SSD). Of course, modern computing architecture still treats the SSD disks as I/O devices even if they are made out of internal memory. Therefore, there is still some benefit to a pure RAM implementation. However, as technology gets better, there could be solutions where flash-storage access times become comparable to RAM access times.

performance gain when switching to memory-based solutions. The potential challenge is getting enough memory modules into a machine since most computing hardware accepts only a limited amount of RAM (e.g., dmidecode -t 16).[16] Another option is to utilize solid state disk (SSD) technology with regular RDBMs technology (refer to the Alternative In-memory Database Architecture sidebar).

IMDBs provide an easy path toward reaping the benefits of in-memory computing. The use of the SQL interface has provided a quick option for most enterprises to migrate their existing applications. Write-through and replication can address concerns with respect to load balancing and high availability. The obvious "memory is faster than disk" thinking allows for justification of such an initiative. However, care must be taken to ensure that applications truly benefit from the use of in-memory technology. System designers must ask themselves a few basic questions to determine solution fit (refer to the Questions to Ask When Considering an IMDB sidebar). Once the decision to use in-memory computing is made, additional work must be done to ensure that considerations have been deliberated. In particular, the areas of resources required, functionality and security requirements (confidentiality, integrity and availability) must be reviewed. Most important, enterprises must make an effort to try the technology first.

As more and more people interact on the web, service and application providers have more data and tools in their possession—one of which is IMDB technology—to know their customers better. The proliferation of various solutions—commercial and free—puts traditional high-performance data applications in everybody's hands.

QUESTIONS TO ASK WHEN CONSIDERING AN IMDB

- Will the application benefit from in-memory computing technology? Is it I/O-bound?
- Can the data fit in commercially available amounts of RAM?
- Does the application require an SQL interface? Does the IMDB provide it?
- Does the choice of IMDB support the subset of SQL that the application requires?
- Are there security assumptions that change because of the limits of functionality?
- Are persistence and durability necessary? Does the IMDB support disk-based persistence?
- Is there a chance of data loss when solely depending on disk-based persistence? Is that OK?
- Is load-balancing necessary? Does the IMDB support shared-nothing replication? Can it support this for both load balancing and high availability?

ENDNOTES

1 PC Magazine, "Definition of In-Memory Database," 2013, *www.pcmag.com/encyclopedia/term/44861/in-memory-database*

2 Kumar, V.; A. Grama; A. Gupta; G. Karypis; *Introduction to Parallel Computing*, vol. 110, Benjamin/Cummings, 1994

3 Hess, K.; "Uncover Your 10 Most Painful Performance Bottlenecks," 2010 *www.serverwatch.com/trends/article.php/3912821/*

4 Jacobs, A.; "The Pathologies of Big Data," *Communications of the ACM*, 52(8), 36-44, 2009

5 Godard, Sebastien; "iostat," Man Page, *http://linux.die.net/man/1/iostat/*

6 Microsoft Corporation, Perfmon, *http://technet.microsoft.com/en-us/library/bb490957.aspx*

7 Oracle Corp., "Oracle TimesTen In-Memory Database," *www.oracle.com/technetwork/products/timesten/overview/index.html*

8 SAP, "What Is SAP HANA?," *www.saphana.com/docs/DOC-2272*

9 IBM Corp., "IBM solidDB-Fastest Data Delivery," *www-01.ibm.com/software/data/soliddb/*

10 VMware, VMware vFabric Gemfire, *https://www.vmware.com/products/application-platform/vfabric-gemfire/overview.html*

11 Oracle Corp., MySQL Cluster FAQ, *www.mysql.com/products/cluster/faq.html*

12 SQLite, SQLite In-Memory Database, *www.sqlite.org/inmemorydb.html*

13 VoltDB, *http://voltdb.com/*

14 Sethi, Jaypal; "Druid: 15 Minutes to Live Druid," Metamarkets, *http://metamarkets.com/category/technology/druid/*

15 Janssen, Cory; "Definition—What Does NoSql Mean?," Technopedia, *www.techopedia.com/definition/27689/nosql-database*

16 Nixcraft, Maximum Memory and CPU Limitations for Linux, *www.cyberciti.biz/tips/maximum-memory-and-cpu-limitations-for-linux-server.html*

Solving the Identity and Access Management Conundrum

Srikanth Thanjavur Ravindran is an IT service management (ITSM)/ information security consultant with Cognizant Technology Solutions US Corp. Ravindran has diverse global experience within the energy, life sciences, retail, banking and telecommunications domains in the areas of ITSM, IT governance, risk management, information security, service delivery and program management. He can be contacted at *srikanth.thanjavurravindran@cognizant.com.*

With the adoption of distributed and remote infrastructures, the need for an identity and access management (IAM) solution has become paramount and is a top agenda item for most chief information officers (CIOs). The IAM market is also extremely competitive, with many technology heavyweights and exciting new talent battling it out for the top slot in this space. The options to choose from are many and it is important to have an IAM strategy and an underlying process in place to enable the tool. Effective governance along with automated role management, authentication, user profiling and integration are keys to establishing a holistic IAM solution.

An automated process that provides users with access to systems and revokes access when necessary forms the crux of IAM. Improved discovery, intrusion detection and monitoring technologies along with a rapid increase in the number of technology vendors offering IAM solutions may make it appear easy, but this is not the case.

Companies can spend millions of dollars every year on security initiatives and still struggle to reach the right combination of confidentiality, integrity and availability (CIA). Lack of periodic entitlement reviews and nonexistent links among human resources (HR) systems, active directory and enterprise applications result in inaccurate employee identification and employment status. These are two of the major reasons why IT security regularly comes up short in IAM strategies.

Business process advancements fueled by technologies such as cloud, remote infrastructures, mobility and bring your own device (BYOD), along with changes in the way IT services are provided, such as multivendor outsourcing, Software as a Service (SaaS), multitenancy and virtual infrastructures, have made the IAM puzzle more interesting. The average consumer's life has also changed for the better due to the above technology advancements, but these new technologies also introduced major risk factors to private data.[1, 2]

According to an RSA survey inquiring about the status of IAM within UK businesses, 76 percent of IT directors concurred that IAM is a priority to their organization.[3] Other countries in Europe also have a similar outlook. A survey of CIOs in the UK, France and Germany by Quest Software Inc. found that in 2013 IAM is a priority for more than three quarters of European organizations.[4] Given the industry focus on this in the current milieu, it is important to consider the critical success factors in the IAM journey.

USING A TOP-DOWN APPROACH

As with any investment-centric IT initiative, it is extremely important to get business buy-in for IAM. In addition, IAM is a policy-driven initiative that should be communicated and mandated from the top business levels. This also helps to enforce the IAM policy at the employee level and to emphasize the consequences of noncompliance; it may also help with reducing instances of hacking via popular methods such as spear phishing.

In the RSA survey, respondents identified senior executives/board members as one of the biggest barriers to the implementation of IAM—one-third of IT directors declared cost and lack of funding and 27 percent stated buy-in from the board.[5] The key to convincing the business is to discuss the pain points of system security, IT administration and compliance requirements that IAM would address. Articulation of business values should include improved lead time for new user access provisions, productivity improvements through enterprise single sign-on (SSO), cost cutting through reduced service desk use and improved compliance metrics during audits.

USING A GOOD-BETTER-BEST PROGRESSIVE SOLUTION

An IAM solution is a long-term investment and an evolving initiative. IAM has many components in role management, provisioning, password management and enterprise SSO. Thus, a good-better-best practice should be adopted.

While password management may be a quick win, automated provisioning may have security implications and federated identity systems and SSO may pose challenges in the form of complexity and diverse security architectures, particularly for legacy systems.

The best way to accomplish a good-better-best practice would be to understand the overall objective, break it down into smaller goals and come up with a road map (**figure 1**). Data security, regulatory compliance, competitive advantage, productivity benefits and reduced overhead are some of the goals that can be targeted during the road map phase. The road map should then be used as input for a plan—identifying quick, medium- and long-term wins with consideration for low-, medium- and high-priority goals targeted (**figure 2**).

ESTABLISHING GOVERNANCE FOR CONTINUED BENEFITS REALIZATION

It is important to outline what the IAM solution will enable—it helps if the right expectations are set at all levels and knowing what to measure. User profiling, authentication and rights management are key to kicking off the program. User profiles must be set up with role definitions, access rights, identity verification and user groups. Standard and core services provided, with access times, authentication procedures and approval workflows, should be included.

Figure 2—IAM Target Goals

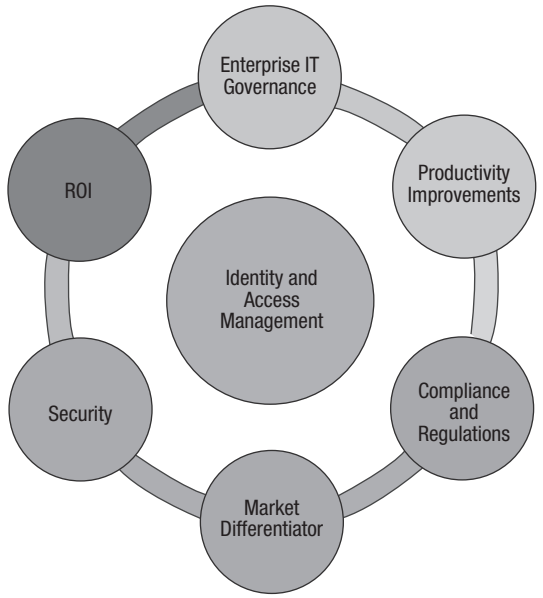
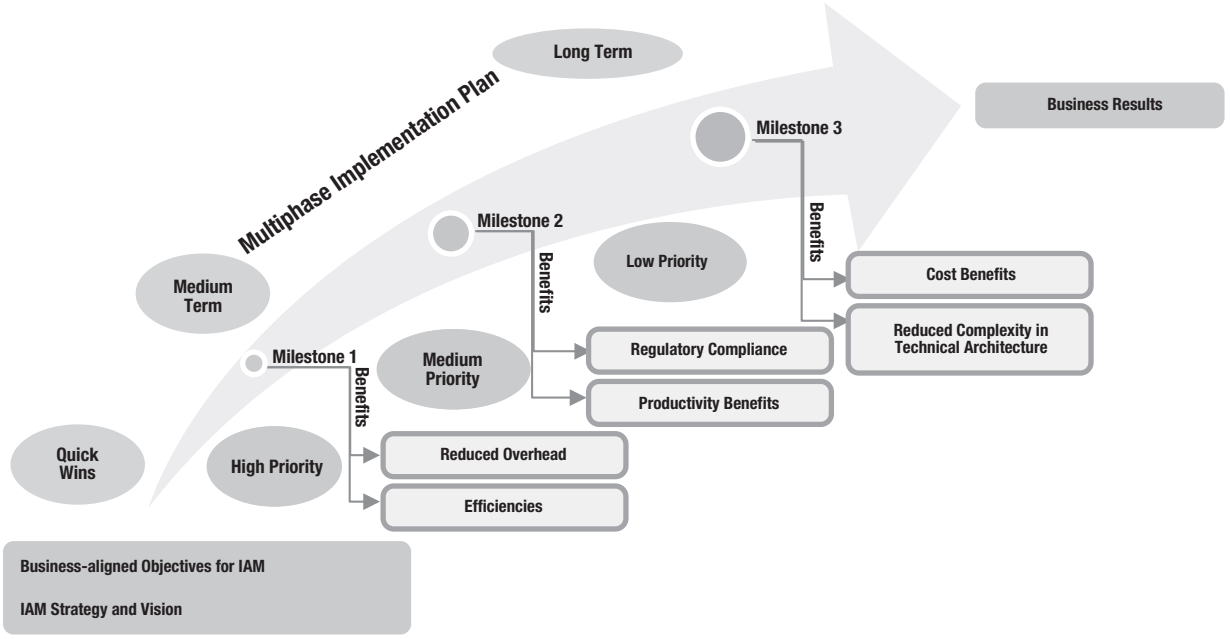


Figure 1—Benefits Realization Through a Phased Road Map



The user life cycle should be documented with procedures for access provisioning, temporary suspension and permanent revocation. Exception procedures should also be documented in accordance with security policies and implemented through IAM. A steering committee should be established to review the progress on a periodic basis. The effectiveness and efficiency of the solution should be tracked and measured using formal metrics. The metrics help the business to understand how the IAM solution has improved security and enabled business benefits in the form of productivity improvements, better compliance numbers and return on investment (ROI). Oracle's functional strategy of categorizing key requirements (such as provisioning, authentication, authorization, self-service and audit/compliance), understanding the current state and building a shared vision of the target state with the business stakeholders is a best practice in this area.[6]

SECURITY AND AUTHENTICATION NEEDS

Additional authentication for critical systems and system life cycle monitoring are two important aspects of IAM. Authentication must be strong enough to prevent hacking while not encouraging bypass attempts with excess security. Some business-critical legacy systems may still be in production but may not have expert support due to outdated technology. Access provision to such systems should be minimal and based on a business case to reduce the risk of extended outages. Other legacy systems may not be supported at all, but may be accessible by users and, therefore, require audits if not decommissioned. In application environments with continuous integration, production data are used for testing as an exception—quite frequently due to data creation and data dependencies. In addition to data masking and the anonymity of personally identifiable information (PII) and sensitive PII (SPII), access control and provisioning of such environments need to be controlled, as hackers might target such nonproduction environments due to their reduced security measures.

Mobile and home users should have an extra layer of authentication such as biometrics and geotagging for location identification. No other breach emphasizes the need for multilayer authentication more than the RSA SecurID intrusion of 2011. It was a wake-up call for IAM vendors and customers alike as it showed the meteoric rise in hacking capabilities, emphasized that reputation in the security industry did not guarantee safety, and paved the way for research on new and improved authentication measures.[7] Service request management (SRM) and standard change models can be used for requesting access, but for systems hosting product know-how and finance details, an extra level of security such as biometrics, government ID verification or manager approval may be required. IAM is also accountable for compliance data provisions, providing a record of access during forensic investigations and complying with user information data protection legislation.

INTEGRATION CONSIDERATIONS

In addition to its affiliation with change management and SRM, IAM is a process with multiple interfaces that are integral to vendor tool offerings and can be achieved through partnerships. The policies executed in IAM are defined in availability and security management. Unauthorized access is detected by intrusion detection (ID) and event management (EM) tools and handled as part of security incident and event management (SIEM). Hence, EM and ID parameters for filtering and triggering responses should be defined accordingly. Integration with HR systems ensures entitlement verification and configuration management record changes to user access in the configuration management database (CMDB).

CONCLUSION

There are significant financial and reputational risk factors associated with losing corporate data, particularly customer data and other sensitive business information. Among organizations that have experienced these data breaches, 33 percent agreed that the enterprise had lost customer trust and 32 percent believed its corporate reputation had been damaged.[8]

The recent hacking of security firm Bit9 is a case in point. Although the full impact of the hack on Bit9's business is yet to be determined, the negative publicity and customer angst expressed after the incident imply severe damage to the firm's reputation.[9]

A must-have for any IAM solution provider is a disaster recovery plan that gives the organization a head start in minimizing damages in case of a hack. Recent security attacks have proven that no amount of preparedness is sufficient in such a situation. For example, after spending US $63 million on a massive outreach program involving more than 60,000 customers, disgruntled clients and industry experts still questioned RSA's response to its security breach.[10]

At the corporate, consumer and government levels, there are major opportunities for improving how to protect private data. The potential for further advancements in the field of technology is enormous, and as with every opportunity, there is an associated risk.

In a world where business processes are increasingly being delivered over social and collaborative platforms, IAM is not only a compliance mandate, but a key differentiator over competitors. It is past the time to question the value of an IAM solution; instead, it is time to protect and differentiate the enterprise by continually increasing the knowledge and understanding of the risk in the enterprise. While unauthorized access and security breaches can be reduced to a great extent with a capable IAM tool, it is the implementation strategy and the underlying processes that can enable the technology to secure the enterprise.

REFERENCES

Asia Pacific Security Magazine, "Quest Software has released the Identity and Access Management (IAM) Index 2012," 1 August 2012, *www.asiapacificsecuritymagazine.com/quest-software-has-released-the-identity-and-access-management-iam-index-2012/*

CA Technologies, "Identity and Access Management Is Vital for UK Business Innovation and Growth, New Survey Reveals," 2013, *www.ca.com/gb/news/Press-Releases/emea/2013/Identity-and-Access-Management-is-Vital-for-UK-Business-Innovation--and-Growth-New-Survey-Reveals.aspx*

Makryllos, Gordon; "Five Steps to Mastering Identity and Access Management," CIO, *www.cio.com.au/article/426548/five_steps_mastering_identity_access_management/*

SearchCIO, "Identity Management Guide for CIOs," TechTarget, *http://searchcio.techtarget.com/feature/Identity-management-guide-for-CIOs*

ENDNOTES

1 Gorodyansky, David; "3 Recent Hacks—What You Can Learn From Them," 11 March 2013, *www.inc.com/david-gorodyansky/3-recent-hacks-what-you-can-learn-from-them.html*

2 The Security Ledger, "Friday Night Massacre: Twitter Hacked, Info on 250k Exposed," 2 February 2013, *https://securityledger.com/friday-night-massacre-twitter-hacked-info-on-250k-exposed/*

3 RSA Security, "Identity and Access Management: A Survey to Understand the Status of Image and Access Management Within UK Businesses," *www.rsa.com/solutions/idmgt/whitepapers/UK_IAM_Survey_05.pdf*

4 Quest Software Inc., "Corporate Data Loss Can Cost Organizations €2.7 Million in Revenue and Fines, According to Quest Software Survey," 12 December 2012, *www.quest.com/news-release/corporate-data-loss-can-cost-organisations-27-million-in-revenu-122012-818962.aspx*

5 *Op cit*, RSA Security

6 Wilson, Yvonne; "Developing an Identity Management Strategy," Oracle Corporation, 2011

7 Savage, Marcia; Michael S. Mimoso; Robert Westervelt; "The RSA Breach: One Year Later," TechTarget, *http://searchsecurity.techtarget.com/magazineContent/The-RSA-breach-One-year-later*

8 *Op cit*, Quest Software Inc.

9 Roberts, Paul F.; "Security Stories to Watch: Security Firm Bit9 Hacked. Also: Microsoft Megapatch and Identity Management," *IT World*, *www.itworld.com/security/341754/security-stories-watch-security-firm-bit9-hacked-also-microsoft-megapatch-and-identi*

10 *Op cit*, Savage, *et al.*

How to Measure Security From a Governance Perspective

Andrej Volchkov is the security program manager in the CSO office at Pictet, a private bank in Geneva Switzerland. Volchkov was previously in charge of security, compliance and internal solutions in Pictet's IT division and responsible for new technologies and architecture, IT methodologies, tooling, and software engineering. Volchkov has a wide range of experience that includes new technology and IT solutions implementation, management of multidisciplinary teams, project management, and software development and research.

Good governance relies on reports or measures that either assess the adequacy of information security, the security program and the return on security investment (ROSI) or the progress toward fixed objectives.

Companies need a pragmatic approach for monitoring the effectiveness of security countermeasures to enable them to adjust their program accordingly and decide on investments. Presented here is an approach for establishing a security dashboard. It is aimed at executive management and provides responses to questions that might arise such as, "Is our security spending justified?" or "Is our security adequate?"

The term "monitoring" is used here to suggest the importance of tracking trends in relationship to precise measures. The term "security" is used rather than "information security," as it is possible to apply the same principles to all security domains including continuity, physical, and human or personal security.

JUSTIFYING SECURITY SPENDING

Security investment decisions are traditionally based on observations, a sense of vulnerability, threat assessments or audit findings. It is not uncommon to see a problem or incident trigger a project that aims to improve the posture or effectiveness of the countermeasures in place. Good governance, however, recommends that executive management be involved in strategic security decisions.[1] The more awareness of the importance of security metrics, or for better coordination of investment—beyond the simple technical IT problem to a concern for the company as whole—the greater the need to justify (i.e., explain) investment in security programs.

Questions such as "Is security spending adequate," or "How good is security?" are not only legitimate but are also part of a natural development toward better governance. The question of appropriateness of security[2] is crucial and is one of the major concerns in all good governance practice. This is precisely why measures need to be expressed in clearly defined units (e.g., hourly cost, incident, risk, budget, strategy) and accepted by all stakeholders in the company.[3]

Companies are increasingly being called on by external auditors who have been hired by their partners or clients to assess the level of security or compliance using norms or best practices. A standard approach to measuring or reporting security should contribute to reducing the cost of these repetitive audits.[4]

The need for justification is also accentuated by the fact that security officials are increasingly reporting to higher levels in companies and often outside of IT. According to a study by Forrester,[5] 54 percent of interviewed chief information security officers (CISOs) were reporting to a member of the C-suite in 2010; this is a 9 percent increase from the previous survey in 2009. The same study revealed that 42 percent of CISOs report outside IT. Similar findings are shown in "The 2011 Global State of Information Security Survey" by PricewaterhouseCoopers (**figure 1**).

Figure 1—CSO/CISO Reporting Level Progression

Percentage of chief information security officers or equivalent information security leaders who report to the followings senior executives:	2007	2008	2009	2010	Three-year % change*
Chief information officer (CIO)	38%	34%	32%	23%	-39%
Board of directors	21%	24%	28%	32%	+52%
Chief executive officer (CIO)	32%	34%	35%	36%	+13%
Chief financial officer (CFO)	11%	11%	13%	15%	+36%
Chief operating officer (COO)	9%	10%	12%	15%	+67%
Chief privacy officer (CPO)	8%	8%	14%	17%	+113%

Source: PricewaterhouseCoopers, "The 2011 Global State of Information Security Survey." Reprinted with permission.

The ability to explain to management the strategy and purpose of security investments using appropriate business language and with a holistic perspective is essential. Senior management is, of course, ultimately responsible for security, which is why they request reports in the form of dashboards that contain stable key point indicators of how adequate the security is regarding the company's needs.[6]

Several surveys also indicate that it is becoming increasingly important to provide justification for investment in security because of the feeling that countermeasures already in place are inadequate. Threats evolve and security countermeasures (and investments) try to keep pace, albeit with a certain delay, but there is a sense of a never-ending race.[7]

WHY IT IS DIFFICULT TO MEASURE SECURITY

Merely observing incidents or studying statistics generated by technical devices does not enable us to form an opinion on the adequacy of security. How many incidents and what type of incidents are allowed in a good security setup? What happens if there are no incidents?

Security tools generate many traces of activity, such as patches applied, detected vulnerabilities, alerts, intrusion attempts, volume of mail processed by antivirus tools, authentication errors, traces of access to systems and changes in privileges. Log management tools can provide correlation of these traces and generate reports that ensure compliance with legal and regulatory requirements. However, high-level metrics require additional efforts to collate these different pieces of information.

Since the benefits (or economic value added [EVA]) of security investments are difficult to observe, why not try to estimate potential losses or annualized losses (annual loss expectancy [ALE]) in order to justify investments?[8] There are various formulas that prevent making investments that exceed the value of the assets under protection. One could also measure the total cost of ownership (TCO) of security and observe its evolution in relation to the estimate of potential losses. Several tools or methods are available to calculate the ROSI on the basis of analysis of losses and investments for specific processes.[9] The main difficulty with these methods stems from the fact that one has to associate the estimate of a loss with its likelihood of occurrence for all units under observation, which could be very random. One accurate calculation method requires statistics over several years with precise indicators on incidents, their nature and the associated expected losses.

Companies do not share their data or statistics on vulnerabilities and incidents because of the negative image that these statistics convey. There is no common definition or terminology that would allow an anonymous exchange on the basis of these statistics. The terms "incident," "attack," "loss" and "investment" mean different things to different companies.

Solution providers emphasize their ability to reduce costs with their solution and often present an associated model for calculating the ROSI for their solution. However, the security solutions sought by companies rarely focus on mitigating a single isolated risk. To optimize its investments, a company seeks comprehensive, flexible and often integrated solutions in suites of products that are usable for multiple purposes. As it is impossible to assign a solution to each specific risk, it becomes difficult to calculate the ROSI because of the side effects (positive or negative) on other risk factors and the ancillary costs associated with maintenance. The constant evolution of threats and the programmed obsolescence of technologies negatively impact a possible measurement program based on the individual components.

> "Being compliant with a standard does not mean having adequate security."

Being compliant with a standard does not mean having adequate security. Different standards (e.g., ISO 2700x, ISO 31000, ISO 38500, ISO/IEC 13335) or best practice guides (ITIL) can be used under certain conditions to assess security posture. However, these standards have stipulations regarding the existence of processes, but do not provide evaluation criteria. There are generally no recommendations about how to effectively manage and measure security.

MANAGERS WANT MEANINGFUL REPORTS

Managers are familiar with analyzing a company's high-level indicators—losses, gains, ratios, political and economic events, and sales targets—to make forecasts or to grasp a particular situation. Decision makers are less interested in operational metrics or calculations of return on investment (ROI) of a particular isolated security component, but rather are interested in reports on the overall efficiency of security countermeasures in place.[10] Because their concerns are revenue generation, cost reduction, improvement of products or services, and control of spending, security reports are appreciated only if they adopt the same approach and the same language (e.g., covering functional and strategic alignment, security performance objectives achievement, compliance management, security team performance, security added value for customers).

The strategy of investment in security has to target the mitigation of high risk areas and the improvement of less adequate or immature processes. For example, if the risk report highlights a significant risk on information leaks and, at the same time, the data access control process is considered immature, it is necessary to implement a data protection solution (such as encryption, improvement of access rights or a data leak prevention tool).

An executive management report should, therefore, contain at minimum the following three sections:

- Explanation of a strategy and security program
- Operational efficiency of a security organization
- Cost of security deliveries

TOOLS TO ASSESS THE STATE OF SECURITY

There are four common tools that each CSO/CISO can use to demonstrate the added value of a security program:

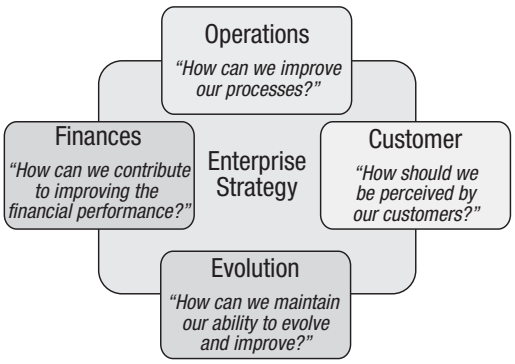
1. Security balanced scorecard
2. Risk management
3. Maturity modeling
4. Diagnostic (or goal-question-metric) method

Security Balanced Scorecard

The balanced scorecard (BSC) is a widespread method for monitoring performance and progress toward the goals fixed to endorse the enterprise's strategy.[11] This tool is well known to management, and it enables security teams to communicate findings on a formal basis. If it is used for monitoring security performance, it will help to position the security team as a partner to the other business lines, making its contribution part of a joint effort. The use of a BSC stimulates executive management into taking ownership of security issues and security's added value.

Financial performance measures alone do not convey all the information needed to assess the contribution of different activities. In addition to finance-related measures, the BSC approach requires measures on three other dimensions or perspectives: operations, customer relationships and evolution (or learning and growth). The four perspectives must contribute to the support of the strategy and the vision of the company. One main question can be associated with each perspective to guide the user in the choice of objectives and associated metrics (**figure 2**).

Figure 2—Four Perspectives of the Balanced Scorecard



The number of objectives should be limited and the number of metrics per objective should be restricted to three or four. The BSC method can also be used for part of the organization or for a specific security domain (e.g., to monitor the business continuity objectives in a company branch or subsidiary).

The BSC-based report has four chapters—each connected with one perspective. Each chapter should contain the objectives to be achieved and the associated metrics. Some examples of objectives with associated metrics are shown in **figure 3**.

Security Risk Management

The aim of investing in security is to mitigate or prevent risk to property or corporate assets. The definition of risk and especially the assessment of risk are essential indicators for high-level management decision making.

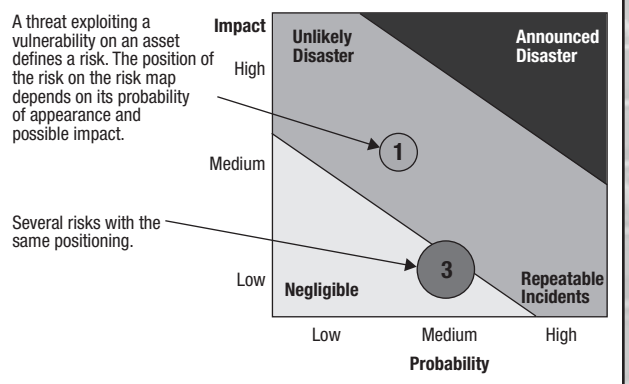
Figure 3—Examples of Metrics in Security Balanced Scorecard		
Perspective	**Objectives**	**Metrics**
Finance	• Manage the cost of security.	• Security total cost of ownership (TCO) vs. number of employees (ratio) • Cost of security incident resolution
	• Improve the efficiency of the information leak controls.	• Number of checks conducted vs. number of employees (ratio) • Percentage of emails covered by controls vs. number of employees (ratio)
Operations	• Reduce the risk of information leakage by negligence.	• Intrusion detection tests • Number of rule breach findings
	• Reduce the number of exceptions and special permissions for mobile workers.	• Number of exceptions per year
	• Improve the access rights management process.	• Number of changes in privileges vs. number of employees (ratio)
Customer	• Reduce the error rate in granting access rights to customers.	• Error rate in the process of granting of access rights • Number of help-desk calls on security issues
	• Reduce by 50 percent the delay in allocating new access rights.	• Delays in assignments of access rights
	• Reduce the delay in processing end-user requests.	• Average delay
Evolution	• Increase the level of understanding of end-user security issues.	• Cost of awareness program vs. number of employees
	• Review the security policy according to the needs of the business.	• Result of the survey conducted in the business lines

A security risk can generally be identified through threats that are likely to exploit one or more vulnerabilities on the company's assets. For example, the risk of penetration of a company's computer network is present because of threats such as intrusion attempts that exploit various vulnerabilities, e.g., social engineering.

The risk is then evaluated on two dimensions, namely the probability of its occurrence and its impact. It is then positioned on a risk assessment matrix (**figure 4**). There are several possibilities for expressing the probability (e.g., frequency of occurrence) and impact (i.e., financial, reputational, human, other).

Probability and impact assessments are based on the same indicators as those used to measure threats and vulnerability. As noted previously, it is impossible to calculate these accurately. It can, however, be roughly evaluated as low, medium or high, using knowledge, statistics, and other endogenous and exogenous factors, which, generally speaking, should be enough to position a risk. In some cases the company may also appoint external experts to assess a specific risk (e.g., penetration test).

Figure 4—Risk Assessment Matrix



Maturity Modeling for Information Security

The risk management process provides information on the dangers, but does not show the level of preparation or the security posture. Therefore, the security process maturity should be evaluated so that initiatives can be prioritized and aimed at addressing weaknesses.

Figure 5—Example of Criteria for Assessing the Degree of Compliance to Point 5.1 of ISO 27002

	Section	Evaluation criteria 0: Incomplete 1: Performed 2: Managed 3: Established 4: Predictable 5: Optimized	Current Level	Desired Level
5	**Security Policy**			
5.1	Information Security Policy	0: There is no documented security policy. 1: The security policy applies to certain departments or units in the organization. 2: Security policy is documented and addresses all areas. 3: Security policy defines the responibilities and sets the framework for all lines of business. The documentation is compiled. 4: Security policy and the associated documentation are reviewed regularly. The policy is adapted for the needs of all business lines. 5: Each employee knows the security policy. The organization regularly adapts the policy, the directives and associated documentation.	2	3

Standards such as ISO 2700x can be used as a reference to build a maturity model. However, these standards recommend the use of a practice, but they do not stipulate any criteria for assessing the level of compliance. For example, point 5.1 of the ISO 27002 standard calls for the existence of a security policy, but it does not specify any gradation that can be found in practice such as "the formal policy does not exist or is not known," or "the policy exists, but is not revised" or "the policy exists and is revised regularly."

To use standards in the maturity assessment process effectively, evaluation criteria must be created for each point of the standard. For this purpose, one could adopt ISO 15504 standard criteria and then establish evaluation criteria for each chapter of the ISO 27002 standard (see **figure 5**).

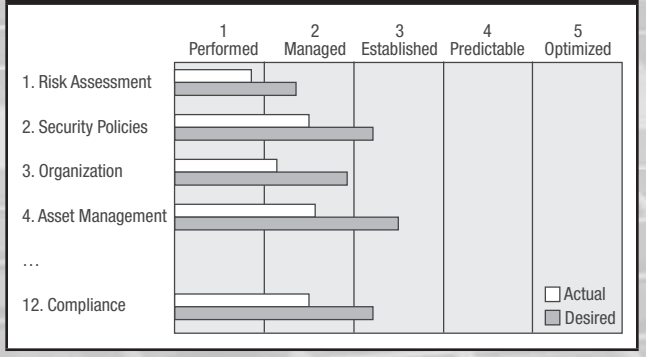
Each maturity model consists of a questionnaire covering all the chapters of one or more standards or frameworks (e.g., ISO 2700x, COBIT, NIST) or proposing its own catalog of measures. Therefore, the current level of maturity for each chapter of the standard should be assessed according to the proposed criteria alongside the desired level. The tool then calculates the averages for each section of the standard or another grouping (possibly weighted measurement) and shows a chart of the state of maturity (**figure 6**).

There are several tools or methods available to measure maturity, such as The Open Group Maturity Model for Information Security Management.[12] Large consulting firms also propose their own models and tools for security maturity assessment, such as Forrester's Information Security Maturity Model.[13]

A maturity model can be used as a tool to communicate security posture to different stakeholders. It also facilitates explanation of the initiatives contained in the security program: *why* information is essential, especially for teams tasked with developing countermeasures, such as IT.

The scope of maturity assessment may be limited for both the business sector and the domains of the model. For example, the maturity of security management at a company's subsidiary can be assessed. Furthermore, the assessment of maturity and the risk assessment are opportunities to discuss and compare views about security with the business representatives, risk managers, auditors and any other stakeholders.

Figure 6—Representation of Maturity: Actual and Desired



The Common Criteria (ISO/CEI 15408) is a standard for security evaluation and certification of a specific system or product. The system certified at one level satisfies all criteria from precedent levels as well as those at the certification level. A similar approach is suggested in the method of measurement of resilience of the Software Engineering Institute (SEI).[14] It evaluates resilience (continuity and IT operations) using the Capability Maturity Model Integration (CMMI) criteria. The resilience is certified as being at a certain level if it meets the requirements of that level as well as requirements from the previous level.

Figure 7—Metrics Associated With a Hypothesis		
Hypothesis	**Subhypothesis**	**Metric**
The management of access rights is no longer appropriate.	Delays in the allocation of access rights increase.	Average delay in a period of time
	Inappropriate access rights increase.	Number of post corrections vs. number of change requests
	The complexity increases (which negatively impacts the risk of error).	Number of different IT systems vs. number of post corrections

Diagnostic Method

The proverb "you cannot improve what you cannot measure" can be adjusted to "you cannot measure if you do not know why you are measuring." Setting goals prior to measuring facilitates the choice of metrics. One of the main purposes of these measurements is to demonstrate a trend or prove a hypothesis.

One strategy is to simplify the definition of metrics, subdivide the hypothesis into subhypotheses or questions, and then define metrics related to each question. One example of the subdivision of a hypothesis and associated metrics is shown in **figure 7**.

The process for constructing this measurement plan is the following:

1. **Determine the hypothesis and goal**—The hypothesis is: The access rights process in an organization is no longer appropriate. The goal would be to improve it according to the result of measuring.
2. **Subdivide into questions or subhypotheses**—The questions associated with the hypothesis or goal are:
   - What are the delays in allocation of access rights? The subhypothesis is that they increase.
   - Is there a progression of errors? The subhypothesis is that incidents or inappropriate access rights increase.
   - Is the complexity of the IT system correlated to the increase in number of errors? The subhypothesis is that the more complex the system, the more errors there are.
3. **Determine the metrics**—The metrics associated with the previous questions could be the following:
   - Average delay (elapsed time between the change request and the availability of the new access rights) measured during a set period of time (e.g., last three months)
   - Ratio between the number of post corrections and number of change requests
   - Evolution over a period of time of the ratio between the number of different IT systems and the number of post corrections

There are different methods of measuring by objective, such as the Diagnostic Method from McKinsey[15] or the Goal-Question-Metric (GQM).[16] The process described for designing metrics is beneficial because it is simple, bounded to the initial hypothesis or goal, and constructed top-down.

EXAMPLE SECURITY DASHBOARD

The ultimate goal of every measurement action is to present a dashboard, a report or a summary of the state of security and associated trends. The following example of a dashboard contains the highlights of measures that respond to issues that can arise in each of the following areas:

1. **Strategy and security program**—What is the security strategy and program?
2. **Operational performance**—How is operational performance changing? What are the main tasks and responsibilities of a security team?
3. **Monitoring the objectives**—Were the agreed-upon objectives achieved?
4. **Costs**—How are security costs distributed?

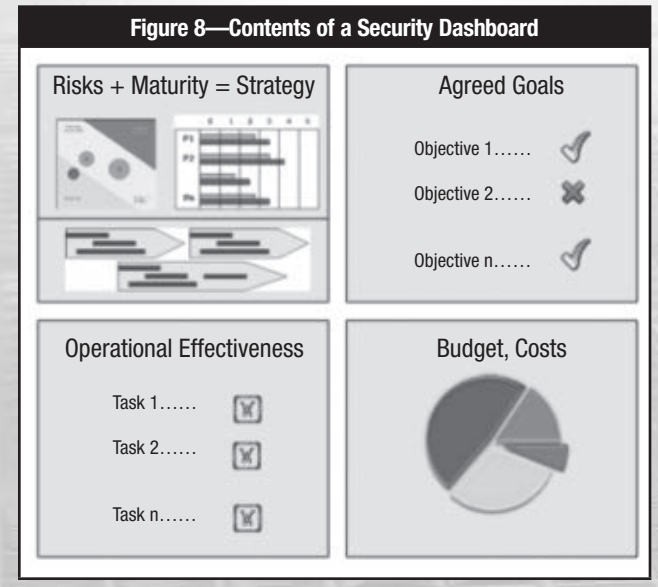
The high-level content of such a dashboard is shown in **figure 8**. It is important that all indicators and metrics used for the report are made available. This helps clarify the conclusions conveyed by the diagrams and tables and answer any additional questions.

Strategy and Security Program

A security program consists of all the initiatives for a given period (usually one year). It contains projects and other activities—all of which are aimed at mitigating high risk factors or increasing a company's ability to protect its assets. It is sometimes called a business plan or investment plan.

The risk assessment and maturity model are two dimensions of the corporate security posture. Any initiative (e.g., IT projects, policy or guideline changes, awareness campaign, acquisition of products) can be viable only if it targets mitigation of risk and/or improvement of one or more immature security processes.

Figure 8—Contents of a Security Dashboard



Presentation in a dashboard or annual reporting can take different forms. The three main elements—risk, maturity and strategy—can be presented on a single page, with particular focus on important risk areas or critical processes that need improvement.

Operational Performance and Cost

Operational performance must be presented using numbers, ratios and trends. **Figure 9** shows examples of operational metrics. Again, these metrics should be chosen according to the measurement objectives and should cover a specific period of time to illustrate the trend. Security costs should be presented alongside the deliverables of a security team.

Follow-up on the Objectives

Security countermeasures should be implemented to overcome the weaknesses identified by the audit findings, maturity assessments or risk analysis. All these objectives should be well defined. The results can be presented in the form of a security balanced scorecard (**figure 10**).

CONCLUSION

Establishing a method for measuring or monitoring security is a necessity in order to meet the demands for justifying an organization's security investments. Security is no longer an obscure and technical area left to the whim of a few specialists. Modern governance standards require executive managers to have a vision of, and development strategy for, security.

It would be a mistake to imagine that one can accurately measure ROSI for a whole security system in one organization. It is wiser to try to answer security-related questions raised by executive managers in a language that they can understand, using tried and tested methods and tools, such as a balanced scorecard, maturity models and risk management.

Security dashboards are a good way of presenting and monitoring security from a governance perspective. They must contain a succinct explanation of the security strategy and

Figure 9—Examples of Operational Efficiency Metrics

Deliveries of a Team	Metric	Trend	Cost	Trend
Awareness efforts	• Cost of awareness program vs. number of security incidents due to poor awareness (ratio)	↓	$	↓
Compliance strengthening	• Average delays in improvements according to audit findings • Number of systems in compliance vs. number of systems to be made compliant (ratio)	↑	$	→
Incidents processed	• Number of security incidents vs. number of employees (ratio)	↑	$	→
Unavailability rate of security components	• Number of hours of unavailability vs. number of components (ratio)	→	$	→
Efforts to ensure that IT projects are compliant	• Number of employees devoted to security projects vs. total cost of complex projects (with high security impact) (ratio)	↑	$	→
Effectiveness of identity management	• Number of accounts still open after end users leave • Number of changes in privileges • Total number of different systems and applications under management • Average delay in processing requests • Error rate	↑	$	↑
Efforts in processing alerts and other security events	• Number of specific investigations • Number of working days spent on analyses vs. number of employees (ratio)	↑	$	→
Effectiveness of controls	• Checks carried out vs. number of employees (possibly by nature of checks or severity of checks) (ratio) • Number of breaches vs. checks carried out (possibly by nature or severity of controls) (ratio)	↓	$	→

Figure 10—Security Balanced Scorecard Example			
	Objective	**Measure**	**Result**
Operations	Improve controls of outgoing emails.	Success in implementing automatic control is achieved.	X
	Reduce security constraints for business.	Help-desk calls regarding security are reduced by 10 percent.	✔
	Be more efficient in the audit findings implementation.	Ninety percent or more of improvements according to audit findings are done on time and on budget.	✔
Customers	Decrease the delay in processing the application of customer access rights.	Delay is reduced to a maximum of one day.	X
Evolution	Reduce the risk of intrusion by email.	Intrusion tests using social engineering is sufficient after sensitizing staff. Target: no more than 5 percent successful intrusions	✔
	Involve security representatives when business-line security directives are drawn up.	More than 50 percent of security representatives have suggested directives.	✔
Finance	Minimize the gap between security budget and actual spending.	The difference between budget and expenditure does not exceed 10 percent.	✔

program, different operational trends based on indicators and metrics, a summary of the progress toward agreed-upon goals, and a presentation of security costs.

ENDNOTES

1 IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, USA, 2006, *www.isaca.org*

2 Allen, Julia; "Governing for Enterprise Security," Carnegie Mellon University, USA, 2005

3 Gartner, "Avoid Inappropriate Financial Justifications of Security Expenditures," 11 July 2007, *www.gartner.com/id=509685*

4 Ferrara, Ed; "Develop Effective Security Metrics," Forrester Research Inc., USA, 17 January 2012, *www.forrester.com/Develop+Effective+Security+Metrics/fulltext/-/E-RES45787?objectid=RES45787*

5 Ferrara, Ed; "Don't Bore Your Executives—Speak to Them in a Language They Understand," Forrester Research Inc., 18 July 2011, *www.forrester.com/Develop+Effective+Security+Metrics/fulltext/-/E-RES45787?objectid=RES45787#/Dont+Bore+Your+Executives+8212+Speak+To+Them+In+A+Language+That+They+Understand/quickscan/-/E-RES58885*

6 Slater, Derek; "Security Metrics: Critical Issues," *CSO Online*, 2012, *www.csoonline.com/article/455463/security-metrics-critical-issues*

7 Brenner, Bill; "Companies on IT Security Spending: Where's the ROI?," *CSO* Online, 25 January 2010, *www.csoonline.com/article/518764/companies-on-it-security-spending-where-s-the-roi-*

8 Fitzgerald, Michael; "Security and Business: Financial Basics," *CSO Online*, 23 June 2008, *www.csoonline.com/article/394963/security-and-business-financial-basics?page=1*

9 Berinato, Scott; "A Few Good Information Security Metrics," *CSO Online*, 1 July 2005, *www.csoonline.com/article/220462/a-few-good-information-security-metrics*

10 Rosenquis, Matthew; "Measuring the Return on IT Security Investments," Intel, 2007, *http://communities.intel.com/docs/DOC-1279*

11 Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business Review Press, USA, 1996

12 The Open Group, "The Open Group Releases Maturity Model for Information Security Management," press release, 2011, *www.opengroup.org/news/press/open-group-releases-maturity-model-information-security-management*

13 Forrester, "Assess Your Security Program With Forrester's Information Security Maturity Model," 2013, *www.forrester.com/Assess+Your+Security+Program+With+Forresters+Information+Security+Maturity+Model/fulltext/-/E-RES56671*

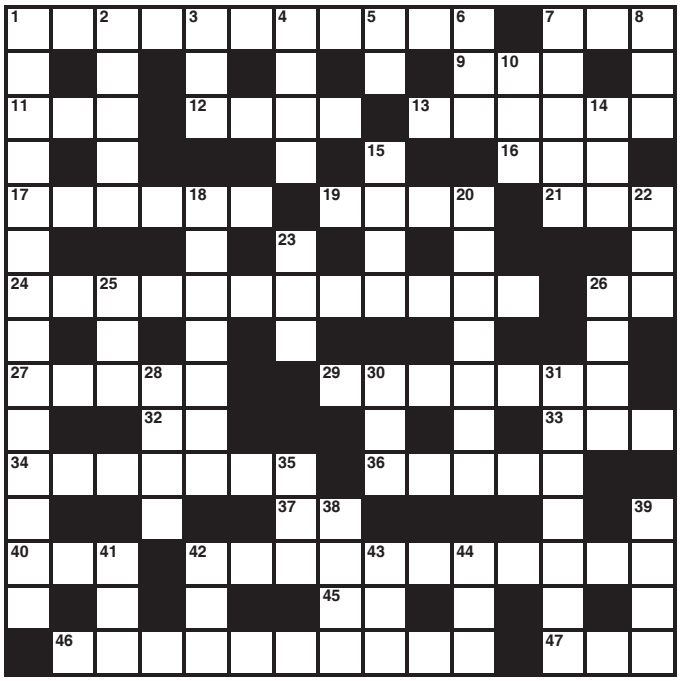
14 Allen, Julia H.; Pamela D. Curtis; "Measures for Managing Operational Resilience," Carnegie Mellon University, USA, 2011

15 Jaquith, Andrew; *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, USA, 2007

16 Hayden, Lance; *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*, McGraw Hill, USA, 2010

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. One of the enemies of antimalware vendors, a feeling of no need for upgrades or security improvements
7. PC "brain"
9. Conceit, sometimes a block on clear thinking
11. Prevent access, for example
12. Overcome
13. Strong and dependable, as a system
16. Excel chart
17. Staggered
19. Fail to locate
21. Dotcom dedicated to ideas worth spreading
24. Leadership culture: vital to getting support for an ethical business environment (4 words)
26. Tech department, abbr,
27. Arrangement of memory elements in one or more planes
29. Hot topic in IT (2 words)
32. Technical dept., for short
33. Part of a cell nucleus, abbr.
34. Computer programs that manage input/output requests from software
36. One of the authors of "*The Web Application Hacker's Handbook, Finding and Exploiting Security Flaws, 2nd Edition*, Marcus ____
37. Quality assurance, abbr.
40. Memory
42. Work together with other employees
45. A complete metric system for scientists
46. Providers of cloud-based integration of databases and marketing tools, with all data securely backed up in real time
47. Global company providing enterprise software and software-related services

DOWN

1. Internet hackers, Trojan installers, malware dealers, etc.
2. Combine two systems, for example
3. Area for experimentation
4. Being expert in these techniques is vital in examining big data, abbr.
5. Turn down
6. Thus far
7. ISACA's good practice framework that includes improving IT security (goes with 15 down)
8. Apply
10. Interruption
14. Sheltered side at sea
15. See 7 down
18. 1,000 petabytes
20. He leaked the processes NSA uses to collect information
22. Type of Internet attack, abbr.
23. Greatest possible, in degree
25. Neither's alternative
26. In 2012 attempts were made to hack into this nation's nuclear program
28. "If it ____ broken, don't fix it"
30. Company providing Internet connection
31. Harmful programs
35. It is used for querying and managing databases
38. As well
39. ____ desk
41. Monitor, Evaluate and Assess; acronym used in COBIT 5
42. Prompt
43. Go public with
44. Bit of binary code

(Answers on page 54)

CPE Quiz

Prepared by Smita Totade, Ph.D., CISA, CISM, CGEIT, CRISC

Take the quiz online:

QUIZ #150

Based on Volume 3, 2013—Big Data

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

TRUE OR FALSE

SETTY AND BAKHSHI ARTICLE

1. The paradigm shift introduced by big data requires a transformation in the way that such information is handled and analyzed, moving away from deriving intelligence from structured data to discerning insights from large volumes of unstructured data.

2. According to a report from Computer Sciences Corporation (CSC), there will be a 4,100 percent annual increase in data generation by 2015.

3. Using predefined criteria determined by the IT department, the big data refinery could flag specific transactions out of a large population of data to investigate for instances of fraud.

4. The only key differentiator for enterprises is the ability to quickly yield and act promptly upon key insights gained from seemingly disparate sources of data.

PATIL ARTICLE

5. Health organizations typically use an EDI gateway system in which such electronic transactions are validated and consumed before they are directed to their respective processing system (i.e., claim adjudication, enrollment, eligibility, billing, payment).

6. A transaction status report is beneficial in that it provides details of all errors that are defined between trading partners.

MOTURI AND BITTA ARTICLE

7. The continuous controls monitoring certification manager is based on actual user activity, is designed for assigning rights to new system users, supports segregation of duties and is network-based.

8. All of the four existing IdA applications report on actual user access activity and policy exceptions as they track user activity and, thus, they do not lack that critical information.

9. A system user agent also enables compliance by performing updates on the users' job descriptions based on access violation reports from the reporting agent.

10. The management agent also defines new policies on access to be implemented by the coordinator agent.

11. To consistently audit what users access within a database application, three key aspects must be considered: system user roles as captured in the job description, the organization's IS policy on access to applications and the access log as extracted from the database.

BOGDANOV AND KALU ARTICLE

12. Stored encrypted and signed data are protected from third-party access during processing.

13. Secure multiparty computation (SMC) and homomorphic encryption (HE) are two new technologies that preserve cryptographic security during processing.

14. The International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) is scheduled to publish a standard for a security architecture framework (ISO/IEC 29101) that describes ways to use SMC for PII storage.

15. Secret sharing is a form of anonymous encryption that splits confidential values into several pieces that individually leak no information about the original secret value

16. SMC cannot be used for securely outsourcing information processing of a single stakeholder to the cloud.

ISACA Journal
CPE Quiz
Based on Volume 3, 2013—Big Data

Quiz #150 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC # _____

Quiz #150

True or False

SETTY AND BAKHSHI ARTICLE

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

MOTURI AND BITTA ARTICLE

7. _____
8. _____
9. _____
10. _____
11. _____

PATIL ARTICLE

5. _____
6. _____

BOGDANOV AND KALU ARTICLE

12. _____
13. _____
14. _____
15. _____
16. _____

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 C	O	2 M	P	3 L	A	4 C	E	5 N	C	6 Y	■	7 C	P	8 U
Y	■	E	■	A	■	A	■	O	■	9 E	10 G	O	■	S
11 B	A	R	■	12 B	E	A	T	■	13 S	T	A	B	14 L	E
E	■	G	■	■	■	T	■	15 F	■	■	16 P	I	E	■
17 R	E	E	L	18 E	D	■	19 M	I	S	20 S	■	21 T	E	22 D
A	■	■	■	X	■	23 N	■	V	■	N	■	■	■	O
24 T	O	25 N	E	A	T	T	H	E	T	O	P	■	26 I	S
T	■	O	■	B	■	H	■	■	■	W	■	■	R	■
27 A	R	R	28 A	Y	■	■	29 B	30 I	G	D	A	31 T	A	■
C	■	■	32 I	T	■	■	■	S	■	E	■	33 R	N	A
34 K	E	R	N	E	L	35 S	■	36 P	I	N	T	O	■	■
E	■	■	T	■	■	37 Q	38 A	■	■	■	■	J	■	39 H
40 R	A	41 M	■	42 C	O	L	L	43 A	B	44 O	R	A	T	E
S	■	E	■	U	■	■	45 S	I	■	N	■	N	■	L
■	46 S	A	L	E	S	F	O	R	C	E	■	47 S	A	P

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 November 2013)

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)
2208 Sampling (G10)

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*.

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

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

COBIT

COBIT® 5 for Risk
213 pages—**CB5RK**

Member TBD | NonMember TBD

Ebook—**WBC5RK**

Member TBD | NonMember TBD

Configuration Management: Using COBIT® 5
60 pages—**CB5CM**

Member TBD | NonMember TBD

Ebook—**WCB5CM**

Member TBD | NonMember TBD

Internet and Related Security Topics

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

Member $40.00 | Nonmember $50.00

Transforming Cybersecurity: Using COBIT® 5
Print Format—190 Pages, 2013—**CB5TC**

Member $35.00 | Nonmember $60.00

Ebook—**WCB5TC**

Member FREE | Nonmember $60.00

Vendor Management: Using COBIT® 5
Print Format—196 Pages, 2013—**CB5VM**

Member $35.00 | Nonmember $60.00

Ebook—**WC35VM**

Member FREE | Nonmember $60.00

FEATURED...

www.isaca.org/featuredbooks

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
236 pages, 2013—98WSC

Member $75.00 | Nonmember $85.00

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

Member $35.00 | Nonmember $59.00

Ebook Format—WRTC

Member Free | Nonmember $59.00

The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, 2nd Edition
784 pages, 2013—4JBSS

Member $74.00 | Nonmember $84.00

The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition
912 pages, 2012—97WWAH

Member $50.00 | Nonmember $60.00

* Published by ISACA and ITGI

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

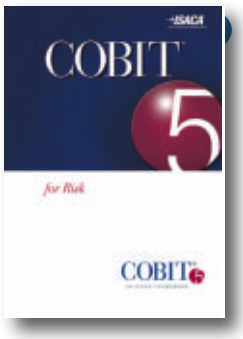
All prices are listed in US Dollars and are subject to change

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

https://www.isaca.org/bookstore/Pages/New-Arrivals.aspx

SUPPLEMENT

NEW/FEATURED BOOKS www.isaca.org/newbooks



COBIT® 5 for Risk

By ISACA

NEW

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

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

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

Print Format—213 pages, 2013—**CB5RK** Member TBD Nonmember TBD

Ebook—**WBC5RK** Member TBD Nonmember TBD

Configuration Management: Using COBIT® 5

By ISACA

NEW

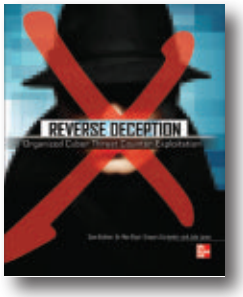
Change is imminent, as enterprises and technology become larger and more complex. Change without proper communication and coordination leads to business disruptions, inefficiencies and potential financial loss. Configuration management is a key component to help enterprise leaders manage change and minimize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

Practice shows that enterprise stakeholders have varied ideas about the meaning of the term "configuration management" and what it entails, causing misalignment in the implementation of CM and the possibility of unmanaged expectations. Configuration management is a strategic capability that supports many other activities within an enterprise, not a standalone process with simple objectives.

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

Print Format—60 pages—**CB5CM** Member TBD Nonmember TBD

Ebook—**WCB5CM** Member TBD Nonmember TBD



Reverse Deception: Organized Cyber Threat Counter-Exploitation

By Sean Bodmer, Dr. Max Kilger, Gregory Carpenter, Jade Jones, Jeff Jones

NEW

In-depth counterintelligence tactics to fight cyber-espionage

"A comprehensive and unparalleled overview of the topic by experts in the field."—Slashdot

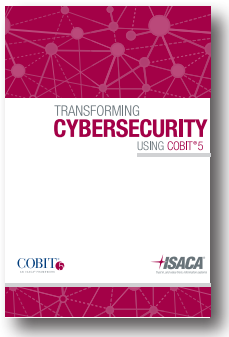
Expose, pursue, and prosecute the perpetrators of advanced persistent threats (APTs) using the tested security techniques and real-world case studies featured in this one-of-a-kind guide. *Reverse Deception: Organized Cyber Threat Counter-Exploitation* shows how to assess your network's vulnerabilities, zero in on targets, and effectively block intruders. Discover how to set up digital traps, misdirect and divert attackers, configure honeypots, mitigate encrypted crimeware, and identify malicious software groups. The expert authors provide full coverage of legal and ethical issues, operational vetting, and security team management.

Print Format—464 pages—**31MRDO** 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

Transforming Cybersecurity: Using COBIT® 5

By ISACA



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

Print Format—190 pages, 2013—**CB5TC** Member $35.00 Nonmember $60.00

Ebook—**WCB5TC** Member FREE Nonmember $60.00

Vendor Management: Using COBIT® 5

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 $35.00 Nonmember $60.00

Ebook—**WCB5VM** Member FREE Nonmember $60.00

EXAM REFERENCE MATERIALS

2013 CISA® EXAM REFERENCE MATERIALS

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

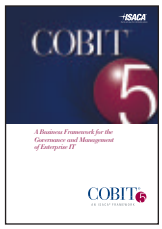

CRISC Review Manual 2013*


CRISC Review Questions, Answers & Explanations Manual 2013*


CRISC Review Questions, Answers & Explanations Manual 2013 Supplement*

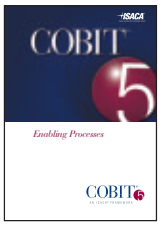
COBIT 5 PUBLICATIONS

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

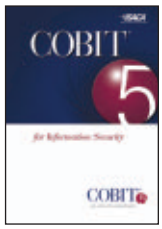
Member FREE
Nonmember $135.00

COBIT 5 Implementation
CB5IG

Member $35.00
Nonmember $150.00

WCB5IG, EBOOK PDF FORMAT

Member FREE
Nonmember $150.00

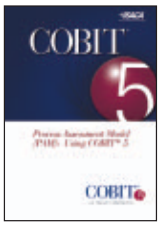


COBIT 5 for Information Security
CB5IS

Member $35.00
Nonmember $175.00

WCB5IS—EBOOK PDF FORMAT

Member $35.00
Nonmember $175.00

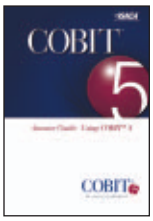


COBIT Process Assessment Model (PAM): Using COBIT 5
CPAM5

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

See New COBIT Titles in our New/Featured section!

* 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 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 December 2013 CISM exam, order ◆

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 December 2013 CGEIT exam, order ◆

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 December 2013 CRISC exam, order ◆

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® 5

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
CB5R*	Romanian	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
WCB5IGJ	Japanese, Ebook—PDF format (purchase online only)	150.00	FREE
CB5IGJ	Japanese, Print Format	150.00	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 5 for Risk			
WBC5RK	Ebook—PDF format (purchase online only)	TBD	TBD
CB5RK	Print format	TBD	TBD
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 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 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
Configuration Management: Using COBIT® 5			
WCB5CM	Ebook—PDF Format (purchase online only)	TBD	TBD
CB5CM	Print Format	TBD	TBD
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
Transforming Cybersecurity: Using COBIT® 5			
WCB5TC	Ebook—PDF Format (purchase online only)	60.00	FREE
CB5TC	Print Format	60.00	35.00
Vendor Management: Using COBIT® 5			
WCB5VM	Ebook—PDF Format (purchase online only)	60.00	FREE
CB5VM	Print Format	60.00	35.00

COBIT® 4.1

COBIT and Application Controls: A Management Guide			
WCAC*	Ebook—PDF format (purchase online only)	55.00	FREE
CAC*	Print format	75.00	35.00
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
CB4.1*	COBIT 4.1	190.00	75.00

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

Code	Title	Nonmember	Member
COBIT® 4.1			
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 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*.

VAL IT™/RISK IT

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
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	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
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

Code	Title	Nonmember	Member
AUDIT, CONTROL AND SECURITY—ESSENTIALS			
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
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
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 December 2013 CISA exam—see page S5

CISM Examination Reference Material
Study aids available in Japanese and Spanish for the December 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
CB5R*	Romanian	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
WCB5IGJ	Japanese, Ebook—PDF format (purchase online only)	150.00	FREE
CB5IGJ	Japanese, Print Format	150.00	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)

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			
Configuration Management: Using COBIT® 5			
WCB5CM	Ebook—PDF Format (purchase online only)	TBD	TBD
CB5CM	Print Format	TBD	TBD
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
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
31MRDO	Reverse Deception: Organized Cyber Threat Counter-Exploitation	50.00	40.00
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)	60.00	FREE
CB5TC	Print Format	60.00	35.00
Vendor Management: Using COBIT® 5			
WCB5VM	Ebook—PDF Format (purchase online only)	60.00	FREE
CB5VM	Print Format	60.00	35.00
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

Code	Title	Nonmember	Member
IT GOVERNANCE AND BUSINESS MANAGEMENT			
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
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. 5-13

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.**

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. ™

Risk Profiles | Assessments | Audits | Vendor Compliance Management | Findings | Investigations | Actions | Incidents | Compliance Objectives Library | Data Privacy | Enterprise Architecture | Enterprise Risk | Reporting | & more

AdaptiveGRC™

Flexible. Interconnected. Comprehensive.

Your GRC obligations span beyond your network into cloud, social media, suppliers and mobile devices

So does AdaptiveGRC

www.adaptivegrc.com

- Instantly present a visual dashboard that concisely summarizes your company's state of operational compliance
- Instantly report risk and compliance management information from multiple stakeholder perspectives e.g. Data Protection Officer, CFO, CISO
- Your system up and running in days, rather than months or years
- Correlate the results of different assessments across multiple regulations
- Rapidly profile your riskiest vendors, technologies and departments to identify your audit and assessment priorities

Visit our booth at the ISACA events in London (September) and Las Vegas (November)!

info@adaptivegrc.com

US: +1 678 591 6965 **UK:** +44 207 022 4884 **Poland:** +48 22 323 73 60