Volume 4, 2014

ISACA® Journal

Governance and Management of Enterprise IT (GEIT)

Featured articles:

Leveraging Metrics for Business Innovation

Align Business Initiatives and IT Solutions

Enhancing IT Governance With a Simplified Approach to Segregation of Duties

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

ISACA®

Trust in, and value from, information systems

"I'M RECOGNIZED FOR **MY CERTIFICATION**.

I'M VALUED FOR **WHAT I DO WITH IT**."

— KETAN DHOLAKIA, CISM, CRISC

MANAGING PARTNER, MACLEAR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2007

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

INFLUENCE MORE

Register online to save US $75

Register early for a December exam and save an additional US $50!

UPCOMING EXAM DATES:

6 September 2014*

CISA and CISM Only
Final Registration Deadline: **21 July 2014**

13 December 2014

Early Registration Deadline: **20 August 2014**
Final Registration Deadline: **24 October 2014**

CISA® Certified Information Systems Auditor®

CISM® Certified Information Security Manager®

CGEIT® Certified in the Governance of Enterprise IT®

CRISC™ Certified in Risk and Information Systems Control™

*HELD IN SELECT LOCATIONS

www.isaca.org/register14-Jv4

Information is the key to protecting information. That's why our security solutions are backed by world-class intelligence to help you identify threats in real time and keep your information safe. Learn more at symantec.com/security-intelligence

When you can do it safely, you can do it all.

#GoKnow

Go ahead, you've got Symantec™

VOLUME 4, 2014

ISACA® Journal

Columns

Features

Plus

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

Journal Online

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

Online Features
The following articles will be available to ISACA members online on 1 August 2014.

An Enhanced Risk Formula for Software Security Vulnerabilities
Jaewon Lee, CISA, CGEIT, CRISC, CIA, CRMA

Book Review: Penetration Tester's Open Source Toolkit, 3rd Edition
Reviewed by Joyce Chua, CISA, CISM, CITPM, ITIL, PMP

A Social Approach to IT Governance
Giuliano Pozza

Potential Impact of IT-directed Investor Relationship Management on Employment
Pascal Lélé, Ph.D., Frank Bezzina, Ph.D., Ronald Zhao, Ph.D., Simon Grima, Ph.D., Robert W. Klein, Ph.D., and Paul Kattuman, Ph.D.

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

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

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

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

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

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

ADVANCE YOUR ROLE AND **YOUR GOALS.**

EMBRACE ISACA'S **WORLD-CLASS TRAINING.**

2014 ISACA® TRAINING WEEK SCHEDULE

Upcoming Training Weeks courses include:

21-24 July • Boston, MA, USA
Social Media in Your Enterprise:
Mitigating the Risk and Reaping the Benefits

11-14 August • Seattle, WA, USA
COBIT 5: Strategies for Implementing IT Governance
Foundations of IT Risk Management
Governance of Enterprise IT
Introduction to Information Security Management

18-21 August • Miami, FL, USA
An Introduction to Privacy and Data Protection

15-18 September • Chicago, IL, USA
Network Security Auditing

22-25 September • New York, NY, USA
Cloud Computing: Seeing through the Clouds—
What the IT Auditor Needs to Know

SHARPEN YOUR EDGE. TRAIN AT THE HIGHEST STANDARDS.

Advance your knowledge, skills and career by registering today for an upcoming ISACA Training Week course. Learn from leaders as you interact with our expert trainers. In addition, each course offers up to 32 CPE credits to help you get or stay certified. Stay ahead of the curve in 2014 with ISACA Training Week!

LEARN MORE

Register today or learn more at:
www.isaca.org/2014training-jv4

ISACA®
Trust in, and value from, information systems

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersinc.com.*

Bear Acceptance

You have probably heard this one.

> *Joe and Fred are running in the woods, with Joe slightly in front. Suddenly, Fred shouts, "Joe, we are being chased by a bear. We have to go faster to outrun him." Joe replies, "No, I just need to outrun you, Fred."*

THE REALITY OF CYBERATTACKS

So what does this have to do with cybersecurity? Joe accepted the fact that he was under attack, and he had a plan to mitigate the threat.

In my last article, I dealt briefly with acceptance and would like to go a bit deeper here. I assert that everything that ISACA® stands for—security, control, risk management, auditing, governance—is based on a recognition that all the benefits of information technology have a negative component that must be dealt with effectively. There is nothing wrong with focusing on the many benefits that technology has and will bring society, provided that the view not obscure the fact that error and malice can undermine those advantages. And, I believe, the time has come to accept that cyberattacks are a global reality—malicious forces in the world have gone beyond vandalism toward institutionalized espionage, sabotage and crime.

> "All the benefits of information technology have a negative component that must be dealt with effectively."

There is no need for me to give examples to prove that the threat is real; daily newspapers are doing that job perfectly well. My purpose is to encourage the readers of the *Journal* to articulate to their management teams that they must accept the reality of the threat and do something about it.

DISPOSING OF COUNTERARGUMENTS

Unfortunately, too many organizations are not yet ready to voice their acceptance.[1] At some executive level, the realization is just not there. So let me start by disposing of some of the counterarguments that might be used to hinder effective protection.

- **It is all hype and scaremongering.** If it is just mass hysteria, then some very large companies are reporting some very large losses just to flimflam the public. One example will do: After it was victimized by cyberattacks, the retail chain, Target, attributed a projected loss of up to 25 percent of earnings per share and profits declined 34 percent.[2]
- **We have had hacking incidents for years and IT did not collapse.** Yes, there have been hackers, and because of them, there has been a massive investment in security systems[3] that have kept the world of IT from breaking down. There was a significant difference in the hacks of the past. They were essentially vandalism with the intent of widespread, but undirected, harm. Today's cyberattackers are governments, terrorists and criminals who have the intent and the wherewithal to steal from or demolish a specific organizations' data. These are qualitatively different from the "script kiddies" of yesteryear.
- **Our data are not important enough to attract an attack.** This may be true for an organization that has no employees, no customers, no trade secrets and no money. All others are targets.

THE NOTHING-CAN-BE-DONE ARGUMENT

The most insidious counterargument is to attribute otherworldly powers to cyberattackers. In just the past few weeks, I have had several IT executives say to me, "If the bad guys want my data, there is nothing I can do to stop them." Of course, there is a grain of truth to this canard. Since ancient times, if there were enough barbarians and they tried hard enough and long enough, they could breach any castle wall. There were a number of possible countermeasures: Inflict such losses on the barbarians that they would just go away. Do not keep all the gold in one castle. Build a second wall within the outer one within the moat. And, with reference back to our friends running through

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

the woods, make an attack on your castle so difficult that the barbarians would choose someone else's for their depredations.

One school of thought is that those targeted should counterattack.[4] This may be a viable response if you happen to have an army to back it up, are willing to risk a war and do not have laws preventing such things.[5] Perhaps some less drastic measures should be tried first. For example, an organization could examine its information portfolio and determine what an attacker might want to steal. Then keep credit card numbers, for example, separate from customer names.[6] Keep the especially sensitive information on a super-protected system and do not allow remote access to it. (Military forces do this.) Consider a security architecture that goes beyond perimeter protection and limits data access within a system, the so-called Zero Trust Model.[7] Implement an information security program that is as restrictive as budgets will allow and then some. Monitor it closely to ensure that an attempted breach will be seen.

ACCEPTANCE = BUDGET

The above paragraph is a bear summary[8] of the potential strategies for resisting cyberattacks. They are all based on the acceptance that systems are under active attack—because they are. Important to many information security professionals: From acceptance flows funding. So, push the message that cyberattacks are real as high as it will go—to IT management, executive management, to the board of directors. At the same time, make certain that the message includes that countermeasures are real, too.

ENDNOTES

[1] At least not publicly or to the relevant regulatory authorities. I will give just a few statistics to demonstrate that reluctance. The insurance broker Willis reported in August 2013 that 45 percent of the Fortune 500 and 57 percent of the second 500 made no reference to cyberrisk protection in their filings with the US Securities and Exchange Commission and that only 6 percent of either group had insurance to cover cyberrisk.

[2] Target, "Target Provides Update on Data Breach and Financial Performance," press release, *http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance*

[3] The publicly available figures vary so widely that I have no idea what the actual expenditure might be, except that it is large. The most conservative I have seen is US $6 billion in 2012 (Canalys, "IT Security Spend to Reach $30.1 Billion in 2017," 2013, *www.canalys.com/newsroom/it-security-spend-reach-301-billion-2017*). At the other extreme, Gartner states that the figure is *ten times* higher (Gartner, "Gartner Says Worldwide Security Infrastructure Market Will Grow 8.4 Percent," 2012, *www.gartner.com/newsroom/id/2156915*).

[4] Baldor, Lolita C.; "US Ready to Strike Back Against China Cyberattacks," Yahoo News, 19 February 2013, *http://news.yahoo.com/us-ready-strike-back-against-china-cyberattacks-225730552--finance.html*

[5] Consider, for instance, the US Computer Fraud and Abuse Act and the British Computer Misuse Act of 1990. See: Westby, Jody; "Caution: Active Response to Cyber Attacks Has High Risk," *Forbes*, 29 November 2012, *www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk.*

[6] This is good privacy practice anyway. What, in fact, is cybertheft of credit card information but a privacy breach?

[7] National Institute of US Standards and Technology, "Developing a Framework to Improve Critical Infrastructure Cybersecurity," USA, 8 April 2013

[8] I could not resist the pun. Apologies to all.

ISACA
Trust in, and value from, information systems

Expand Your Expertise with ISACA's New, Interactive Bookstore eCatalog

ISACA's new, interactive Bookstore eCatalog makes it easy to find the most-timely expert insight on emerging trends, best practices and business. The newly redesigned Bookstore eCatalog provides access to a peer-reviewed collection of industry publications that will keep you ahead of the curve in rapidly evolving topic areas and beyond.

Easily browse the latest research, thought leadership and expert analysis in all the hottest-topic areas, anywhere, anytime.

Topic Areas

- COBIT 5 and family of products
- Certification exam prep materials
- Emerging trends such as Big Data and Cloud Computing
- Cybersecurity
- Much More

Explore the new Bookstore eCatalog today at *www.isaca.org/bookstore*

Trial by Fire in Cloud Development Pays Dividends: Dual Role as User and Provider Drives Vital Learnings About Cloud Adoption

Tim Myers is chief information officer of Cbeyond Inc., where he is responsible for technology and operations strategy and execution that support the growth and transformation priorities of the company. Myers has more than two decades of experience in broad enterprise infrastructure delivery, application portfolio management and delivery, e-commerce, and IT program management.

As a national provider of broadband network connectivity and cloud services to small and medium businesses and a user of cloud technology, Cbeyond has had a unique vantage point that informs how the company itself is embracing the cloud. Three key dynamics drive its cloud strategy:

- Developing and testing on itself first and owning the "trial by fire" that so often occurs when rolling out new cloud services. This allows Cbeyond to battle test its services before rolling them out to customers.
- A keen focus on deepening its cloud expertise and enhancing its in-house cloud capability, performance and support while growing its cloud services business
- Friendly licensing terms and agreements that allow for cost-effective cloud solutions, particularly when moving from on-premise to cloud or when doing upgrades of hardware and business applications

The fact that Cbeyond delivers and manages cloud services to several thousand customers creates a natural bias toward cloud migration for its internal systems. However, as with many of its customers, Cbeyond's cloud use is continually evolving.

Today, Cbeyond operates in a hybrid environment in which portions of its enterprise IT infrastructure and applications are cloud-based and portions are still on a physical platform. Some of its enterprise functions, such as finance, accounting and customer relationship management (CRM), run primarily, albeit not totally, in a Software as a Service (SaaS) environment. Cbeyond is also in the process of moving the bulk of its applications development and testing to the cloud as it is far more efficient and cost-effective.

The main reason Cbeyond is not completely in the cloud is that the organization does not have projects that require full SaaS implementation (or, in some cases, the projects are not yet SaaS-friendly), so for timing and cost-control reasons Cbeyond has taken a modular approach, based on business process priority and availability of SaaS-based solutions for its business systems. Its ability to develop, test, implement and support cloud applications is continually getting stronger, so much so that it now has a strong bias toward cloud-ready systems and makes many IT purchasing choices based on growth in cloud use.

Its cloud customers are also benefitting from its growing in-house expertise. Cbeyond infuses its services with the knowledge and best practices it has gained from piloting cloud applications and processes on its internal platform. For example, before introducing its mobile-to-private branch exchange (PBX) Communications on the Go solution to customers, it tested it with its own internal teams and sales force in parallel with its IT beta testing and got immediate feedback, which it then used to implement necessary changes to make the solution market-ready.

ALL OR NOTHING?

Being on both the owned and offered sides of cloud services has given Cbeyond valuable insights into what works and what does not as a business moves to the cloud. One critical priority is to establish the level and depth of support the business needs. More than any other consideration, support requirements should drive choice in cloud management strategy.

Until recently, cloud-hosting choices fell primarily into all-or-nothing management categories. Businesses could choose between a cloud provider that offered a fully managed cloud services platform, or they could pursue a self-service model in which the company could self-administer and provision most of the necessary services. There were no good choices available that offered a hybrid approach using both scenarios.

In developing its own cloud strategy, Cbeyond found that each model has strengths and weaknesses that make them more or less optimal options based on the nature of the business and its technology requirements. For instance, a fully managed public cloud service's platform offers

strong support, but eliminates the ability for fully flexible customization and limits the addition of some value-added services. On the other hand, self-service cloud service platforms are highly customizable, but offer little or no support and can require additional administrative time and expense.

What Cbeyond envisioned for itself—and ultimately its customers—was a more flexible cloud-based platform: one that could enable varying degrees of scalability and customization based on the dynamic needs and requirements of a rapidly changing, growth-oriented company. The platform would support full, light or no management within a solid and standardized framework.

Cbeyond also wanted a platform that would support more complex and advanced cloud services requirements. It had to be an enterprise-class infrastructure that could enable such advanced self-service capabilities as virtual machine (VM) provisioning and management, while also allow for customized proprietary applications as well as standard a la carte services to be layered in as needed. Businesses have varying degrees of technical ability from very basic to very advanced, either with their own in-house IT staff or through technical partners. Thus, Cbeyond developed its multiple cloud products with this flexible approach and consideration to offer what makes financial and technical sense so its customers can maximize their cloud experience and investment.

As Cbeyond surveyed the marketplace to find this type of cloud platform, nothing really met the criteria. So, Cbeyond decided to create it. The organization made a calculated investment in the people and tools to make this process easier for customers and itself. It continues to use its cloud products in-house for its own teammates so it is actively gathering feedback from its own use as well as examining customer feedback to continue refining its cloud product offerings so the company can exceed customer expectations and is competitive in the market.

Being a consumer of its own services has also allowed Cbeyond to fine-tune the planning, implementation and testing processes necessary for successful cloud migration. Cbeyond has leveraged that experience to create replicable methodologies. The following are some key considerations:

- Determine where data and applications reside in the organization's current platform. Develop a diagram or design plan that maps so the same scheme can be created and replicated in the cloud.
- Prioritize network availability so the most critical business applications get the highest quality of service. Consider the impact of choosing different providers for network and cloud services. On-net providers of network and cloud, such as Cbeyond, have a significant advantage when it comes to cloud performance, support, integration and security.
- Take a phased approach or easier path to migrating data and applications based on business priority.
- Choose a partner that knows the components of the cloud and will learn your particular business, develop a plan, provide the level of support needed to migrate to the cloud, and protect and backup data.
- Decide what "access anywhere from the cloud" means in the organization and ensure that the application, network and infrastructure provider(s) support it.

GOVERNANCE OF THE CLOUD—BEST PRACTICES

A firm foundation for business continuity, disaster recovery, off-site backup and data replication is essential for cloud governance. These functions are increasingly important for compliance-focused businesses, such as law practices, medical practices and financial services firms.

It is also important to know how best to use public and private cloud platforms. The private cloud is best suited for applications and data that require the highest levels of security and protection, e.g., financial and patient health data. Applications such as web sites or development/test systems that have lower data security concerns are best suited for the lower-cost public cloud.

Since most businesses outsource cloud technology and services, there are important considerations in selecting a provider:

- Accessing the cloud through a single provider that operates both the cloud platform and the network ensures service level agreements (SLAs) on both and offers a true private cloud that is secure at all end points.
- The provider must be able to offer individual security policies, segmenting its platform to create a dedicated, private, true multitenant cloud.
- The cloud backup and restore service must support multiple server image rollbacks and multicenter data replication for disaster recovery.

CONCLUSION

Although implementing cloud computing can be complicated, following the three dynamics of cloud strategy can help organizations maximize the benefits of cloud computing.

Beyond the IT in IT Audit (Part 2)

Understanding How to Add Value to Your Role

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.

It is obviously necessary that IT auditors do their job with quality, and, therefore, knowledge, skills and abilities related to IT are critical success factors. But there are some other critical success factors that go beyond IT.[1] To understand how IT auditors maximize the value of their role, it is important to describe certain factors and issues critical to that goal. The truth is that the future of IT audit is about adding value to the role of IT audit.

GENERAL COMMUNICATION "RULES"

Adding value to the role of the IT auditor is based on a quality performance followed by effective communications. There are several communication rules that IT auditors should follow to maximize their value:

- **Rule 1:** IT auditors, like any other affinity group, tend to have their own language—commonly referred to as "geek speak." The first rule is do not use geek speak when talking to those outside the IT audit group. Communicate the issues, results of audits, etc., to others in plain English, without referring to unique acronyms and language.
- **Rule 2:** Always keep the perspective of your audience in mind when communicating. If it is middle management, convey information within the perspective of middle management. The audience is always translating and trying to understand and apply information from a perspective of their position and role.
- **Rule 3:** Be transparent in delivering information. Do not try to hide or obfuscate certain pieces of information or the point of any findings. When something is bad and would be perceived as bad from the audience's perspective, do not try to make it sound good. Likewise, when it is moderately bad, from the audience's perspective, do not try to make it sound really bad.
- **Rule 4:** Convey all information with the entity as a whole in mind. This rule especially applies when conveying information to senior management. First, remember that the IT space is only one component of the entity. The bigger picture includes other factors and issues. For example, IT risk is only one component of enterprise risk management (ERM). IT auditors should become familiar with as much of the enterprise's ERM as possible in order to properly align IT risk with all the risk factors of the entity. All risk factors need resources, evaluation, consideration for remediation and management. Those resources are scarce and must be judiciously applied to risk. That fact should be considered when conveying information about IT risk. Second, give a broad view of results and not just the IT space view. That is, consider the impact of the IT information on the business entity as a whole and not just the IT space. For instance, there may be a downstream manual control in another space of the entity that can adequately compensate for the IT risk in the IT space. To be able to meet this goal, the IT auditor needs to understand the business as a whole, interrelated processes, controls and potential compensation. Last, it is the role of the IT auditor to be an effective teacher—to help management understand when it comes to IT risk and information. For example, the IT auditor could ramble on about advanced persistent threats (APTs), how serious particular threats are and how something must be done immediately. However, the effective thing to do is to help management understand what APTs are, how they can affect the business in question, and why the business needs to be protected. And, always remember this communication should be done without geek speak.
- **Rule 5:** Be more of a consultant and less of an auditor when communicating with management. Develop two hats: one for the IT space and one as a consultant to management of the entity. And, then, be sure to wear the latter hat when communicating with management. For example, focus more on results and risk as part of ERM and put less focus on rules and violations of IT rules. IT auditors need to take on the role of teacher, not judge, when conveying information if they want to add value in their role.

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:

- **Rule 6:** Be actively engaged with changes to the business. Be alert, listen and assimilate changes to the business that impact the IT space. Such changes will sometimes give the IT auditor an opportunity to add value by forewarning management of the downside of an impending change or of communicating potential synergies as a result of an impending change.
- **Rule 7:** Look for opportunities to brainstorm around risk related to emerging IT or business changes and their impact on the entity as a whole, rather than just the impact on the IT space. Be known as someone who can effectively brainstorm and solve problems before they become problems by proactively engaging in brainstorming sessions, formal or informal.

DO NOT OVERSTATE THE IT RISK

One thing with which virtually all IT auditors would agree is that there is almost always something in the IT space that, from an IT perspective, is broken and needs to be fixed. While they do need attention, so do many other things in the entity as a whole. Therefore, IT auditors need to be careful how they report IT risk and, in particular, not to overstate the risk of something broken in the IT space. That is, the news should be placed in the context of ERM and the entity as a whole.

In addition, IT auditors should be effectual in reporting IT risk and audit results. Specifically, an assessed level of risk has a probability and a magnitude component. It is easy to get caught up in the frightful outcome of some threat or risk and not be realistic about the probability of that threat. Always take both components into consideration and report each. For example, the perimeter could have a weakness that itself is significant; however, controls at the application layers and server layers may be strong enough to prevent most malicious activities that would emanate from that weakness. So, while it is a significant weakness by itself, in the big picture, it may be more of a moderate weakness.

> "View the IT risk from management's perspective and not just IT's perspective."

As stated earlier, a key aspect in reporting IT risk is to view the IT risk from management's perspective and not just IT's perspective. By taking this approach, IT auditors should be able to report IT risk in a more realistic and holistic manner.

When there is a relatively high IT risk, communicate it effectively. Again, do not use geek speak. If possible, find a reasonably similar case and use it as an example. Such a conversation might go like this: "Let me show you what will happen if this risk follows its natural path. First, …will occur, which will affect our business by…."

Some examples of overstating IT risk include:

- **Y2K**—The magnitude was high, but the probability turned out to be quite low. Results: No big deal to almost every entity. Was it overhyped? Probably.
- **Distributed denial of service (DDoS)**—While DDoS may be relevant and assessed as high, most executives will not be able to adequately comprehend it because it is highly technical. Find a relevant, high-profile case, such as Google.com or *The New York Times*, and make the comparison as relevant as possible.
- **Disaster recovery planning (DRP)**—The truth is that a pandemic disaster has a low probability, especially as compared to a system failure—thus the need for business continuity planning (BCP). It may be better or more reasonable to talk about BCP risk. Be factual in the magnitude and probability of DRP.

RECOGNIZE MANAGEMENT'S PRIMARY CONCERNS

There are at least two primary concerns of management as it relates to IT:

1. **Management does not want to be surprised.** Therefore, be honest and transparent about the risk that exists or will exist, the remedies being recommended, and what can happen if remedial action is not taken. Some examples of the latter are what happened to Target and TJ Maxx regarding security vulnerabilities that were not properly addressed. But, it also includes surprises totally contained within the entity. For example, suppose an entity is planning to switch to a new technology (e.g., HTML v.5); some questions that the IT auditor should be answering are: Is the new IT adequately understood? Have the risk and potential outcomes from using this new IT been effectively communicated to

management? Have all communications been completed from management's perspective?

2. **Management typically does not understand IT and the IT space.** Management comes from a perspective of education or experience in management and/or a product/service, and those individuals likely have not built a body of knowledge, skills and abilities in IT. Also, IT is only one component of the business for which management is responsible. However, management does want to know what is going on in the IT space; therefore, the same three questions apply to the IT space and communications with management.

KEEP UP TO DATE ON IT

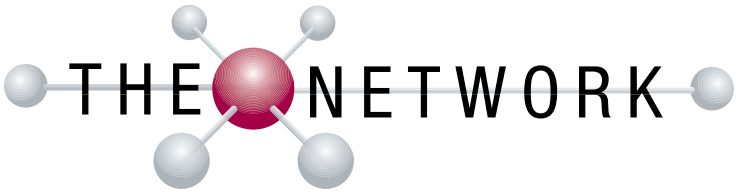
While the focus of this article is beyond IT, nothing will cause IT auditors to lose value more quickly or more deeply than getting behind on IT. Communications will suffer if that happens. For instance, IT auditors could inadvertently report out-of-date information or information invalidated by IT changes. IT auditors should make sure that they are aware of emerging technologies or emerging issues with technologies. Cloud computing, mobile computing and social media are some current examples of emerging technologies. But, one must also be aware of changes in programming. The role of scripts, for example, continues to evolve and new programming techniques may also be relevant.

CONCLUSION

Much has been said about IT audit "having a seat at the table" and of IT audit playing a major role in business decisions and direction. IT auditors will have a seat at the table not because it is IT, but because those IT auditors bring value to all the things the business does, especially in communicating with senior management. This article attempts to identify how IT auditors can add value and what the future role of IT audit will likely be. Many seasoned professionals know this information and have used it to enhance their careers and add value to all they do. The future of IT audit is for all IT auditors to add value to all they do with the perspectives identified herein.

ENDNOTES

[1] See this column in vol. 3, 2008 for my initial attempt to identify and address some of those factors: understanding the business, risk assessment and soft skills. This 2014 article addresses these and other factors to demonstrate the future role of the IT auditor and how to add value to it.



Robert E Stroud, CGEIT, CRISC

Robert E Stroud, CGEIT, CRISC, is international president of ISACA and vice president of strategy and innovation at CA Technologies (New York, USA). A member of ISACA's Professional Influence/Advocacy Committee, he has served ISACA as international vice president, member of the Strategic Advisory Council, chair of the COBIT Steering Committee and ISO Liaison Subcommittee, and member of the ISACA Framework Committee.

Stroud spent more than 15 years in the finance industry successfully managing multiple initiatives in both the IT and retail banking sectors. He joined CA from the Australian computer security company Cybec, where he was responsible for the company's global expansion.

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:

Q: *As ISACA's newly elected international president and the vice president of strategy and innovation at CA Technologies, how do you see ISACA® growing and adapting to the constantly changing marketplace and needs of its constituents over the next year?*

A: The world is becoming a smaller place thanks primarily to technology. Technology, previously used to drive process automation and productivity and treated as a back-office function, is now a pivotal part of everything. Think for a moment about the banking industry, my former career. How long has it been since you walked into a bank branch? Your banking today is done over the Internet and, increasingly, your mobile device.

One of the big changes taking place today is the personalized use of technology within and outside of IT, not only by IT, but directly within the business itself. Some might say that this is simply a cyclical change, but I am not convinced. Now a fundamental component of the business, IT is the vehicle through which disruptive and changing business practices are being delivered.

Q: *Can you briefly describe your role at CA Technologies? What is your role as a vice president and global advocate? What in your past experience best prepared you for this position?*

A: My role at CA Technologies is to act as an advocate for the future, understanding emerging technologies and the opportunities they offer. This requires an understanding of the innovation that businesses are currently undertaking and their use of emerging and disruptive technologies. Prior to joining CA, I spent 15 years in banking and then worked with a security start-up. While in banking, I spent time developing retail banking solutions, implementing automation solutions across the data center and several years in IT security. I was challenged to change the perception of security, a challenge that I accepted and relished, and my team developed a solution for retail banks. My time with the start-up was a great experience, teaching me how to work in an organization devoted to rapid innovation and growth.

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

A: When hiring, I am typically looking for certifications that are not only book learning, but also show true experience in the domain. ISACA currently has four certifications that meet the criteria: Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™). In my banking career, working where I worked within security, I would have looked for CISA or CISM certification among applicants. Regarding my current role at CA Technologies, I typically look for employees who are strategic in nature and go beyond the tactical day-to-day environment. For me, the most appropriate certifications are CGEIT and CRISC, certifications that I myself hold.

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

A: Having a career requires the constant reinvention of one's self. Moving from Australia to the US involved two countries that speak English (different spelling) and have similar cultures, but different rates and paces for change. But the largest challenge I faced was when I moved into IT security from supporting retail banking. I made the move with no formal training—all learned in my spare time. Our time frames were tight as we had to support the emergence of Internet banking, our branch and our back-office systems. To develop my skills, I had a brilliant mentor who guided me immediately to an industry support group of professionals, an education program and certificate programs to develop my skills. This was done in conjunction with an excellent lab where I could test and rapidly develop my skills. This experience taught me the importance of having a support network and constantly updating my skill set. Ultimately, thanks to being developed in a strong team environment, we delivered a world-leading solution.

WHAT'S YOUR FAVORITE BLOG?
Those I contribute to, of course, including CA.com blogs, ISACA Now and HDIConnect. I am a strong advocate for social media, blogs, Twitter, LinkedIn and so on. Those I read regularly:

- ISACA Now—*www.isaca.org*
- The National Football League (American football)—*www.NFL.com*
- The Australian Football League—*www.AFL.com.au*

WHAT'S ON YOUR DESK RIGHT NOW?

- My treasured family photos
- The Wasserman Award that I received last year from the ISACA New York City Chapter
- A copy of *COBIT® 5: Enabling Processes*
- Three screens for my computer
- My iPad

WHAT ARE YOUR MAIN GOALS FOR 2014?

- Reach and hear as many ISACA members as possible globally
- Ensure that they are getting value from their membership
- Help ISACA expand into mainland China (more on that soon)
- Ensure we support our growing membership outside of North America
- The successful launch of Cybersecurity Nexus (CSX)

WHO ARE YOU FOLLOWING ON TWITTER?
Industry luminaries; journalists; governance, risk and security professionals; a number of ISACA members; and, of course, @ISACANews—1,125 as of this writing. (I'm sure it will have grown by publication!) Rather than individuals, I typically use Twitter hashtags to follow trends. Follow me at @RobertEStroud.

WHAT'S YOUR NUMBER ONE PIECE OF ADVICE FOR OTHER RISK AND COMPLIANCE PROFESSIONALS?
Never stop learning and be open to change. Change is the only constant.

Ethical Hacking: The Next Level or the Game Is Not Over?

Viktor Polic, Ph.D., CISA, CRISC, CISSP, has been an information and communication technology professional with the United Nations and several specialized agencies since 1993. His current position is chief of the information security office at the International Labour Organization. Polic is also an adjunct faculty member at Webster University (Geneva, Switzerland), teaching courses on information security and telecommunications within the Computer Science Department of the School of Business and Technology, and serves as a member of the Scientific Committee for Advanced Studies in Information Security at the Department of Management Studies of the Faculty of Economic and Social Sciences at the University of Geneva (Switzerland).

Internal audit work plans tend to focus on priorities based on risk with the highest operational impact. For many organizations this results in IT audits focused on financial applications, human resources (HR) applications, enterprise resource planning (ERP) systems and the like. Many other systems remain out of audit scope due to limited audit resources and medium or low priorities in the annual audit plan. Other assurance functions, such as information security, struggle with the same resource constraints. Performing detailed technical information security risk assessments that involve manual tasks, specific skills and tools are costly and, therefore, performed only on those systems exposed to risk with the highest business impact. However, a detailed information security risk assessment in the form of ethical hacking is the most accurate method to estimate risk likelihood.

Information security vendors have recognized the need to optimize the process of managing ethical hacking projects with the goal to reduce their costs. They start offering ethical hacking services in the form of Security as a Service (SecaaS) solutions. The ability to acquire ethical hacking security assessment for information systems with medium or even low business impact would allow organizations to build more complete and accurate risk treatment plans and optimize resources for information security management.

MEASURING IT RISK

COBIT® 5[1] recommends following best practices for effective IT risk management:

1. Make sure the IT risk management framework fits with the risk management objectives of the enterprise. Use similar risk classification principles and, wherever possible, classify and manage IT risk in a business-driven hierarchy, for example:
   - Strategic
   - Program
   - Project
   - Operational
2. Define standard scales for IT risk assessment, covering impact and probability aligned with the organization's enterprise risk management (ERM) framework.[2]
3. Align the IT risk management appetite and tolerance levels with the ERM framework.

Risk indicators are defined as metrics capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite. If carefully selected and measured with due diligence, these metrics represent a powerful management tool for making strategic decisions in governing the IT function within an enterprise. The following criteria should be taken into account for selection of information-security-related risk indicators: potential impact on vital information assets, efforts required to exploit information systems (IS) vulnerability, reliability of critical IT assets and sensitivity of information.

The likelihood of successfully exploiting a vulnerability is determined by the degree of difficulty in performing the exploit, the skill of the attacker, and the popularity or availability of the vulnerability. A vulnerability that is known to be popular among malicious hackers carries a higher probability of success. Industry-standard tools for assessment of vulnerabilities are software-based vulnerability scanners. These automated tools compare detected applications, operating systems and other components on audited hosts against proprietary or public databases of known vulnerabilities. They provide reports on detected gaps and recommend implementation of security patches, if available, or vendor-suggested work-around solutions. However, they do not put vulnerabilities in a business context and, thus, impact estimates could be misleading. A determined hacker is more likely to exploit even the low-scaled vulnerability if it is on a high-value business asset.

Moreover, automated vulnerability scanners do not provide information on interrelated

risk as described in the referenced identity theft case. Their scans are target-centric rather than information-centric or business-process-centric. Therefore, human intervention is required to adjust scanning methodology. Ethical hacking and penetration testing supplements automated risk assessment and adds more certainty in estimation of risk likelihood. When measuring risk, standard deviation from statistical averages of security events occurrence is what counts the most. One needs to better sense outliers, not be surprised when they occur. The primary information security objective is to prevent false negatives rather than false positives. False positives in information security are collateral damage that is reduced by fine-tuning risk mitigation measures in the perpetual process of information security management. False negatives are foreseen, but unexpected, security events that result in impact on business. Particularly critical are extremely rare events with devastating impact, known as black swan events. Due to the lack of information on the past occurrences of such events, it is very difficult to quantify related risk and plan adequate mitigation. Ethical hacking could provide additional perception of such risk by identifying paths that may lead into high-impact breaches of information security or major IT infrastructure interruptions.

> "The primary information security objective is to prevent false negatives rather than false positives."

In today's dynamic business environment where boundaries of responsibilities blur in cloud computing, outsourcing and virtualization on all scales, it is difficult to dedicate resources to continuous audit of all IT assets. Moreover, qualified ethical hacking is costly and time-consuming. Nevertheless, there are new tools for information security managers—hybrid solutions in the form of combined automated vulnerability scanners with manual ethical hacking. These less costly SecaaS tools can be used more frequently than dedicated penetration tests. They can be applied as regular periodic security assessments on critical information systems.

The systems that are the best candidates for such audits are web-based information systems. These systems are particularly vulnerable at the application layer.[3] The competitive advantage of hybrid vulnerability scanners over traditional automated scanners is in their ability to adapt attack strategies to the most vulnerable components of a target. Ethical hackers working in the back office of a SecaaS provider mimic the approach of malicious attackers. Attackers start with reconnaissance with the objective to collect intelligence about the target. Attackers use port scanning, DNS zoning, web searches for details on the company, its staff, its web identity, forums and social network searches, and other information gathering methods. Automated vulnerability scanners use only those methods that are technically feasible. Advanced correlation techniques are possible only manually.

When attackers collect enough information and identify the weakest links, they begin manual attacks. The weakest link in the security chain is typically a component of the information system that is not up to date, with a vulnerable version where publically known exploits already exist. Other weak links could be those that are misconfigured, disclosing unnecessary information or permitting brute-force attacks on authentication systems and other similar types of attacks. However, to be efficient, attacks have to be optimized and adapted to bypass other security controls, such as intrusion detection/prevention systems, firewalls, reverse proxy servers and others. Automated tools cannot adapt their attack scripts for sophisticated evasion techniques. Undoubtedly, malicious hackers can and so can ethical hackers. Advanced hybrid vulnerability scanners such as ImmuniWeb[4] offer custom-built scripts in the assessment reports in the form of exploit proof of concept. This is a valuable tool for information security teams to verify the likelihood of risk materializing and to adapt mitigation controls.

In addition, comprehensive vulnerability scanners use industry standards for definition of Common Vulnerabilities and Exposures (CVE) and Common Weaknesses Enumeration (CWE).[5] Priority levels of identified vulnerabilities are represented in accordance with the Common Vulnerability Scoring System (CVSS).[6] The application of standards in

assessment reports ensures that results are comparable with those from other tools and methodologies. Good assessment tools allow for customization of CVSS to adjust reports to the criticality of information assets in the particular business context for each customer. This facilitates comparison of periodic assessments and provides a quick overview of the organization's risk posture. It also puts an emphasis on the most critical risk and more vulnerable information assets.

Good vulnerability assessment tools also highlight gaps from security standards and industry best practices. In 2011, the European Committee for Standardization adopted standards for burglar-resistant doors and windows.[7] According to this standard, doors and windows are classified in six security classes relative to their resistance to burglar attacks. For each security class, the standard defines force and tools used and minimum time of resistance. In the information security area, unfortunately, international standards that define resistance classes to particular levels of attacks do not exist. The ISO/IEC 27002:2005 standard, for example, recommends the best control measures and protection practices in different information security areas. The Payment Card Industry Data Security Standard (PCI DSS) takes a similar approach, defining areas of control for data protection. Certification audits assess the existence of controls, but do not require measurement of their efficiency. Ethical hacking or penetration testing performs measurement of efficiency of existing security controls analogous to the previously mentioned burglar resistance tests. This is an added advantage the hybrid vulnerability assessment scanners have over automated scanning tools.

> "In the information security area, unfortunately, international standards that define resistance classes to particular levels of attacks do not exist."

Automated vulnerability scanners can identify existing security patches from software vendors. However, these are not always provided in a timely manner. Waiting for software vendors to provide a patch could expose critical information to unacceptable risk levels. Alternative risk mitigation measures could reduce exposure of information until security patches become available. Security researchers who discover new vulnerabilities sometimes suggests the selection of appropriate work-around mitigation controls. Ethical hackers participating in hybrid vulnerability assessments typically present several alternative remedies for each risk identified in their reports.

CONCLUSION

Hybrid vulnerability scanners offered as SecaaS have brought ethical hacking services to the broader market, allowing even small companies to contract such services. At a time when malicious attackers are more frequently part of a determined criminal group, as opposed to the "script kiddies" of yesteryear, availability of such tools permits information security teams to remain proactive. The information security game is not over, it has entered another level.

ENDNOTES

[1] ISACA, COBIT® 5, Align, Plan and Organize process, APO12 *Manage risk,* 2012, *www.isaca.org/cobit*

[2] ISACA, *Transforming Cybersecurity Using COBIT®* 5, 2013, *www.isaca.org/cobit*

[3] The Open Web Application Security Project (OWASP), 2013, *www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*

[4] High-Tech Bridge, 2013, *https://www.htbridge.com/immuniweb/*

[5] MITRE, 2012, *http://cve.mitre.org/*

[6] FIRST, *www.first.org/cvss*

[7] European Committee for Standardization, EN 1630-2011, *Pedestrian door sets, windows, curtain walling, grilles and shutters—Burglar resistance—Test method for the determination of resistance to manual burglary attempts,* 2011

Leveraging Metrics for Business Innovation

Where Measurement Meets Transformation in IT Governance

Yo Delmar, CISM, CGEIT, is vice president, GRC Solutions at MetricStream with more than 30 years of experience in IT and management, focusing on governance, risk and compliance (GRC). She has broad experience developing GRC program strategies and security programs for large organizations. Yo can be reached at *ydelmar@metricstream.com.*

The title of a blog post on the *Harvard Business Review* web site made the following claim, "IT governance is killing innovation."[1] This argument raises an important question. If technology is at its best when it is transformative, forging pathways to innovation, how can IT organizations ensure that their governance programs do more than simply manage the performance of their operations environment? How can they foster IT innovation as a means to spurring growth and competitive advantage?

Over the past decade, the global IT industry has undergone a significant transformation. By now this story is familiar. From the proliferation of digital tools and the rise of social media, to the growth in mobile networking and the datafication[2] of everyday life, technological advancements have fundamentally altered traditional patterns of work and connectivity. And yet, as IT has become increasingly pervasive, IT departments have faced their own sets of challenges. Not without a sense of irony, in a world in which technology has made nanoseconds the new normal, IT departments have had to battle the perception that they are sluggish and out of touch with larger organizational goals, unable to keep pace with the changing needs of today's hyperconnected and hypercompetitive business environment.

In response, IT governance frameworks emerged, broadly speaking, to facilitate the proper alignment between the IT department and the larger enterprise as well as to maintain optimal levels of IT investment and performance.[3] However, to ensure that the proper foundation is in place for IT to not only support and improve business performance, but also become a source of innovation, organizations cannot put their faith in the blind adoption of abstract metrics. Instead, companies need to thoughtfully design, develop and adapt metrics that are aligned with and support organizational strategy and goals. How can organizations leverage metrics for successful business innovation?

Также на русском
www.isaca.org/currentissue

METRICS ARE FOUNDATIONAL TO CREATING AND SUSTAINING COMPETITIVE ADVANTAGE

Metrics[4] have become ubiquitous as of late and with good reason. The advancement of data-driven decision making across just about every industry has made metrics integral to demonstrating the value and performance of business programs and their supporting IT processes, within organizational boundaries and through supplier and customer ecosystems. Moreover, an emphasis on metrics and analytics has allowed business and IT to better adapt and refine strategic initiatives, as well as optimize resources with an eye toward sustaining and growing competitive advantages.

To be sure, there are a number of ways in which metrics play a crucial role in maintaining a robust IT governance framework:

- Tracking metrics is fundamental to developing predictive models and assessing the key factors for future IT success.
- Metrics are the building blocks of larger analytics.
- Metrics are needed to ensure sufficient allocation of resources that focus on IT innovations.
- Metrics help in making specific processes visible, thus enabling organizations to isolate specific aspects of IT operations for tracking, measurement and assessment.

As Peter Weill and Jeanne Ross argue, "Measurement and accountabilities are critical to any good [IT] governance design. Articulating who is responsible for what and how they will be evaluated provides clarity, ownership and tools to assess governance performance."[5] Tracking metrics and the ways in which they change over time are also fundamental to developing predictive models and assessing the key factors for future IT success. For example, as an increasing number of companies migrate critical

enterprise applications to the cloud, reaping the benefits of increased agility and efficiencies, IT departments have looked to establish metrics around third-party governance. Specifically, these metrics translate into accountabilities around availability, performance, backup, recovery, archiving and compliance that can be incorporated into service level agreements (SLAs) to ensure that those third parties become effective extensions of IT, and are aligned with the organization's overall operational requirements.

Most important, metrics play a key role as the building blocks of larger analytics programs. Though often used interchangeably, metrics and analytics are not synonymous. According to COBIT® 5, metrics represent specific numerical data that act as operational, day-to-day indicators for goal achievement. In this regard, metrics allow an enterprise to assess the proximity or distance from specific organizational objectives. Analytics, on the other hand, aggregate data from numerous sources and make use of a series of metrics to identify organizational trends, patterns and correlations. By analyzing large volumes of data in real time, or near real time, analytics not only help organizations sustain and improve IT performance, but also provide deeper insights for innovative business strategy. For example, IT may measure mean incident recovery cost, mean time to incident recovery and mean time to patch. Looking at the trends and correlations among these metrics moves one into the realm of analysis and leading indicators, where one can gain insight into root cause and take steps to address potential risk, control failures or inefficiencies. Analytics, however, are only as good as the foundation upon which they are built. The predictive power of analytics actually depends on establishing the right set of metrics.

Each of these examples suggests that the ongoing improvement of IT governance initiatives is simply not possible without appropriate metrics.[6] But while IT departments require metrics that measure and enhance operational performance, metrics are also needed to ensure a sufficient allocation of resources that focus solely on cultivating IT innovation. Innovation groups within IT departments can look across industries to gain an understanding of how industry leaders with similar processes are evolving and building an appropriate set of metrics by leveraging industry baselines. For example, a company that distributes goods can adopt aspects of how FedEx, a leader in distribution, uses mobility and social media to enhance the customer experience for its own processes across the supply chain and customer communities. Organizations adopting bring your own device (BYOD) policies might leverage processes and metrics that leaders such as Apple use to manage their own teams' devices internally. Beyond FedEx and Apple, every business should be asking itself questions such as, "What are the most innovative companies doing to measure the effectiveness of IT in their organizations?," and, "How can these metrics be used to inform the metrics being developed in our own organization?"

At the core, metrics play an important role in making specific processes visible. By establishing a particular set of metrics, organizations isolate distinct aspects of IT operations for tracking, measurement and assessment. The flipside, of course, is that because metrics highlight certain aspects of the process, while rendering others invisible, focusing on an incomplete or irrelevant set of metrics can actually prove to be detrimental.

Given the speed with which technology changes, IT departments are constantly trying to hit a moving target. Knowing what to measure and how to measure it is no easy task. "Enterprises have struggled to understand the value of IT-related initiatives because value cannot always be readily demonstrated through a traditional discounted cash flow analysis."[7] This speaks to the challenge at the heart of designing metrics that accurately convey the value and performance of an organization's IT infrastructure. For IT to be a force for innovation and competitive advantage, it is crucial to keep focused on providing the right set of metrics that align with business strategy and performance goals to the right set of stakeholders.

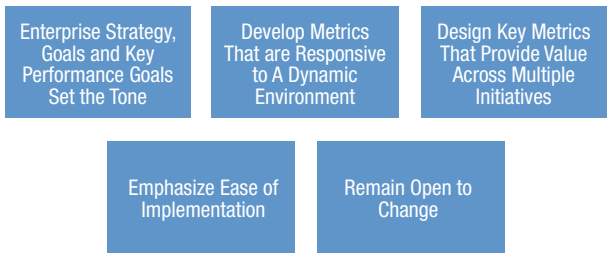
DEVELOPING EFFECTIVE METRICS: FIVE THINGS TO CONSIDER

Metrics, like the organizations that use and rely on them, are not one-size-fits-all. Metrics that are not tailored to particular

enterprise needs and business goals will ultimately prove ineffective. These challenges make clear why the metrics organizations adopt cannot and should not be the result of blind implementation.

In fact, the COBIT 5 guidelines speak directly to this point. Although the COBIT 5 framework is equipped with a rich set of built-in metrics that correspond to more than 100 IT-related processes and subprocesses,[8] the implementation guide is explicit about the importance of adapting the framework to meet specific enterprise needs. This imperative is perhaps best articulated in the section detailing the COBIT 5 goals cascade, which notes that, "because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context…translating high-level enterprise goals into manageable and specific IT-related goals and mapping these to specific processes and practices."[9] In light of the need to adapt IT governance frameworks to meet specific enterprise objectives, a central question remains: How can organizations ensure the development and adoption of effective IT performance metrics?

Figure 1—Five Considerations While Developing Effective Metrics



Source: Yo Delmar. Printed with permission.

There are five things (**figure 1**) to consider when developing effective metrics:

1. **Enterprise strategy, goals and key performance goals set the tone.** The aim of IT governance is to establish synchronicity among IT, business and third parties, as well as to measure the performance of IT in relation to larger business objectives. As a result, it is essential to develop performance metrics that are defined by enterprise goals and not the other way around. Key performance indicators (KPIs) can play a critical role in helping meet this demand because they are specifically designed to measure performance against larger organizational objectives.[10] But building an IT framework closely aligned with larger business goals depends not only on understanding the structural needs of the enterprise, but also the innovation that the enterprise requires to retain competitive advantage. Doing this effectively requires a set of metrics that are focused on emerging technologies and the ways in which they can be used strategically to improve organizational efficiency and customer experience. For instance, as social media has become an integral part of corporate practice, IT departments have struggled to understand its impact on the delivery of enterprise products and services. Rather than ceding social media efforts to other parts of the organization, such as corporate communications or marketing, IT departments should proactively partner with these business units to develop solutions and metrics that help leverage the power of social media to support business strategy. This will ensure that IT departments become a partner in creating competitive advantage rather than remaining myopically focused on their own operations.
2. **Develop metrics that are responsive to a dynamic environment.** Today's business environment is anything but static. Companies find themselves engaged in continuous cycles of change, innovation, renewal and reassessment. Given the pace at which technological changes have disrupted traditional workflows, this dynamism is inherent to the situation IT departments face on an ongoing basis. Against this backdrop, performance metrics need to be able to adapt to both organizational and technological change to generate valuable insights and business intelligence. This will empower organizations to make IT decisions that improve efficiency and have the potential to transform core business functions. For example, the rapid influx of mobile devices and the rise of BYOD policies at many organizations have resulted in increasingly porous enterprise boundaries. With the lines now blurred between personal and proprietary data, IT departments find themselves grappling with the need to develop new sets of metrics that assess the business performance of mobile devices, as well as the ability of the enterprise to meet the rigorous security requirements this new mobile environment demands.
3. **Design key metrics that provide value across multiple initiatives.** In recent years, shrinking technology budgets and

economic uncertainty have forced enterprises to do more with less. In response, organizations should develop metrics that can be deployed in a number of contexts to yield the greatest possible results. To maximize operational resources, metrics should enable organizations to become more efficient by helping identify aspects of legacy infrastructure in the IT ecosystem that have become obsolete or redundant. The true value lies in developing metrics that act as a foundation for larger analytics, which provide insights with the power to inform these types of business decisions. For instance, the rise in distributed denial-of-service (DDoS) attacks over the past few years has demonstrated a shift in the cybersecurity landscape, driving a focus on new types of monitoring systems to ensure the availability of critical web-facing services. Amid this new reality, IT performance metrics that measure the impact of availability from these and similar types of attacks can be leveraged across security, business continuity, disaster recovery and crisis management teams. By developing metrics that give a 360-degree view of processes to a wider group of stakeholders, organizations can more effectively protect critical processes and sensitive data with a defense strategy that is valuable to all.

4. **Emphasize ease of implementation.** Strong analytics are only as good as the foundations on which they are built. As previously mentioned, metrics are the building blocks of analytics, which means that it is necessary to adopt metrics that can be easily implemented and understood. Ultimately, metrics will only be effective if, "employees know what is being measured, how it is calculated, what the targets are, how incentives work and, more important, what they can do to affect the outcome in a positive direction."[11] To take this point a step further, when it comes to metrics, organizations cannot allow the perfect to be the enemy of the new. This can happen when IT departments face the formidable task of having to operate in uncharted territory, reacting to rapid and unexpected changes in the external business environment. Take business continuity as an example. Natural disasters, such as Hurricane Sandy in New York City, New York, USA, in 2012, or the tsunami that triggered Japan's Fukushima's nuclear disaster in 2011, have caused IT departments to rethink their approaches to business resilience and recovery metrics. Business continuity and disaster recovery teams have typically been contained to a small unit within the enterprise that leads recovery efforts. However, many organizations have experienced the pervasiveness of IT, making business continuity essential to an interconnected web of mobile employees, global customers and third-party vendors. As a result, crisis communication is quickly becoming integrated with business continuity as organizations must now reach a wider range of stakeholders. Guidance and direction must be provided to employees; response teams must be mobilized; and communication must be initiated with media, external partners, suppliers, partners, first responders, public and government officials, and more. Only 14 percent of organizations believe communication was effective in their last invocation of a disaster recovery plan, and 52 percent of organizations do not have a crisis management team.[12] IT departments today increasingly require metrics that can be implemented expeditiously, measured easily and incorporated seamlessly into larger analytics to respond to and analyze changing data in real time.
5. **Remain open to change.** As important as metrics are, it is crucial to avoid becoming locked into a static set of metrics that no longer measure what really matters. Organizations should never discount the importance of continued analysis and appraisal of performance metrics. Constant reevaluation of metrics and their relevance to changing business goals is ultimately what will ensure the long-term success of a governance program. For example, metrics that measure the remediation of noncritical vulnerabilities on noncritical infrastructure, supporting information that is neither sensitive nor regulated, provide little value in the overall security equation. Metrics that outlive their utility or no longer provide vital data should be reconfigured accordingly.

MEASURING IT PERFORMANCE: FROM OPERATIONS TO CENTERS OF INNOVATION

Certainly, there are many partisans of IT governance who would take issue with the claim that strong governance can stifle innovation. In fact, an effective governance program with the right metrics actually facilitates business innovation and growth. Weill and Ross, for example, note that all top performing organizations share one aspect in common when it comes to their IT governance programs. That is, "their governance made transparent the tensions around IT decisions given as standardization versus innovation."[13] This suggests that a sound metrics program properly assesses and lays bare strategic, practical and operational considerations, which can empower organizations to invest in and support IT-related projects with transformative power.

Surprisingly, a report by A. T. Kearney found that, "most companies dedicate the fewest resources to innovation"

despite the fact that it "represents the biggest opportunity to increase shareholder value."[14] Being able to measure the effectiveness of technology investments and expenditures across the various areas of the IT department can serve to not only increase efficiency and reduce operational costs, but also provide valuable insights that stimulate targeted innovation. It is precisely at this intersection that measurement meets transformation head on.

Metrics enable businesses to measure the effectiveness of resource allocations between the various layers that comprise the IT department, from operational maintenance and business enablement functions to those tasked with imagining and inventing truly transformative IT. The right performance metrics also allow organizations to measure the effectiveness of transformative initiatives, as well as evaluate how they align with business goals and industry standards. In turn, this type of measurement can be used to enhance the efficacy of future investments in IT innovation.

CONCLUSION: A CALL TO ACTION

Effective metrics are critical to ensuring that the IT department aligns with the enterprise and increases organizational efficiency. Beyond that, however, metrics can play a central role in repositioning the IT department as a source of innovation and competitive advantage, rather than as a drain on organizational resources. To this end, IT departments must constantly strive to achieve the right balance between standardization and innovation by tying their metrics to a larger organizational analytic framework. This will often mean creating a cultural shift to be proactively attentive to opportunities to partner with business units to further enterprisewide goals. In today's business environment, technology is crucial to business strategy and offers some of the most exciting opportunities to create disruptive innovation. With the right set of metrics, closely aligned to organization strategy and performance objectives, IT departments can become hubs of innovation that not only support sustained operational effectiveness, but lead the process of creating competitive advantage.

"Technology is crucial to business strategy and offers some of the most exciting opportunities to create disruptive innovation."

ENDNOTES

1 Horne, A.; B. Foster; "IT Governance Is Killing Innovation," *Harvard Business Review*, HBR Blog Network, 22 August 2013, *http://blogs.hbr.org/2013/08/it-governance-is-killing-innov/*

2 Elliott, T.; "The Datafication of Daily Life," *Forbes*, 23 July 2013, *www.forbes.com/sites/sap/2013/07/24/the-datification-of-daily-life/*

3 Schwartz, K. D.; "IT Governance Definition and Solutions," *CIO*, 22 May 2007, *www.cio.com/article/111700/IT_Governance_Definition_and_Solutions*

4 For the purposes of this article, we use the definition for metrics outlined in the COBIT 5 framework: "A quantifiable entity that allows for the measurement of achievement of a process goal. Metrics should be SMART—specific, measurable, actionable, relevant, timely." ISACA, COBIT 5, USA, 2012. This definition was chosen as a point of departure for two reasons: First, it specifically highlights the fact that metrics represent specific numerical information. Second, and perhaps more important, it emphasizes that metrics should be action-oriented and capable of factoring into larger data aggregations and calculations that can inform strategic decision making.

5 Weill, P.; J. W. Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, 2004

6 Consulting Portal, "Necessary Frameworks for IT Governance: Clarifying the Tangled Web," 28 February 2007, *www.ioptsyn.com/Necessary%20Frameworks%20for%20IT%20Governance.pdf*

7 *Op cit*, Weill and Ross

8 *Op cit*, COBIT 5

9 *Ibid*.

10 IBM Software, "A Business Risk Approach to IT Governance," September 2011

11 Eckerson, W.; "12 Characteristics of Effective Metrics," TDWI Blog, 19 April 2010, *http://tdwi.org/blogs/wayneeckerson/2010/04/effective-metrics.aspx*

12 Forrester Research, "2012: The State of Crisis Communication & Risk Management," *Disaster Recovery Journal*, *www.drj.com/resources/forrester-surveys.html*

13 *Op cit*, Weill and Ross

14 A. T. Kearney, *The 7 Habits of Highly Effective IT Governance: Powerful Lessons in Transforming Business and Information Technology*, 2008, *www.atkearney.com/documents/10192/c60a495f-326c-4ab7-8f7a-093e90bb7df1*

Align Business Initiatives and IT Solutions

Collaboration Is Critical for Effective IT Governance

Ikumi Miyagi, CGEIT, CRISC, is the chief executive officer (CEO) of K.K. AStar and KK AStar Institute.

Hiroshi Monden, CISA, CIA, CRMA, is an internal auditor of a public corporation.

Mitsuko Azuma, CISA, is a business consultant, with 13 years of experience in operational and IT strategy, organizational development and change management.

Reiso Kimura, CISA, CIA, is CEO and founder of Dream IT Research LLC, CEO of Esperanto Co. Ltd., and managing director of the Innovation Fusion Society of Japan.

Masatoshi Aramaki, CISA, CRISC, CIA, is a business consultant advising on IT governance, internal control and information security.

Kan Hara, CISA, CPA, is an independent accounting and technology professional.

Takashi Ishijima, Ph.D., CPA, is professor of accounting at the Hosei Business School of Innovation Management (Toyko, Japan).

Management should bear in mind that information sources and IT strategy should be linked with the needs of the user. That strategy should be based on efficient business processes and compatible with effective IT processes.

A methodology is needed to establish effective IT governance based on the business process and to disseminate integrated IT governance throughout the organization effectively.

To construct effective information systems, it is essential to involve relevant members from management all the way through to field workers, beginning with the planning stage, and to generate agreement among staff by sharing and acknowledging their information, interests and challenges.

ALIGNING BUSINESS AND IT—A MANAGEMENT CHALLENGE

In recent years, the alignment of IT with planning and deployment of the business strategy has become increasingly important for corporate management in light of IT's contribution to business development.

However, the 2013 Cisco Global IT Impact Survey shows that business leaders and other non-IT teams roll out new applications without engaging IT (76 percent) and that IT professionals are brought into the planning and deployment process late (38 percent),[1] which indicates that IT introduction planning is not considered as important as business planning, even now (**figure 1**).

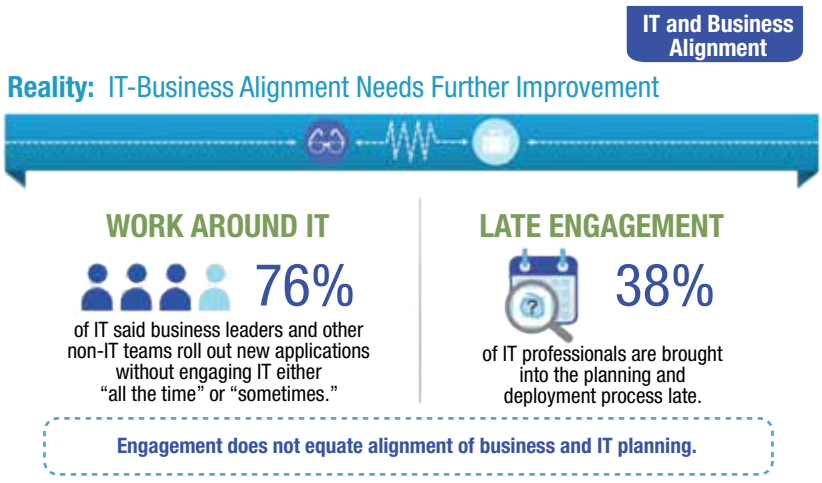
These situations are quite similar in Japan. The 2012 Japan Users Association of Information Systems (JUAS) survey indicates that among the primary tips for successful business innovation are close communication between the IT department and management, or other head office divisions, and understanding of the business process across relevant divisions to reach total optimization for the organization (**figure 2**).[2]

Under these circumstances, alignment of business process with IT remains a big challenge for organizations.

According to a survey of 10 large or medium-sized vendors and clients by Information Technology Promotion Agency, Japan, (IPA), the top three challenges they face on the upper process are ambiguous role sharing and organizational structure, incompleteness or low quality of the requirements definition, and a gap between the business strategy/planning and the required systemization (**figures 3** and **4**).[3, 4]

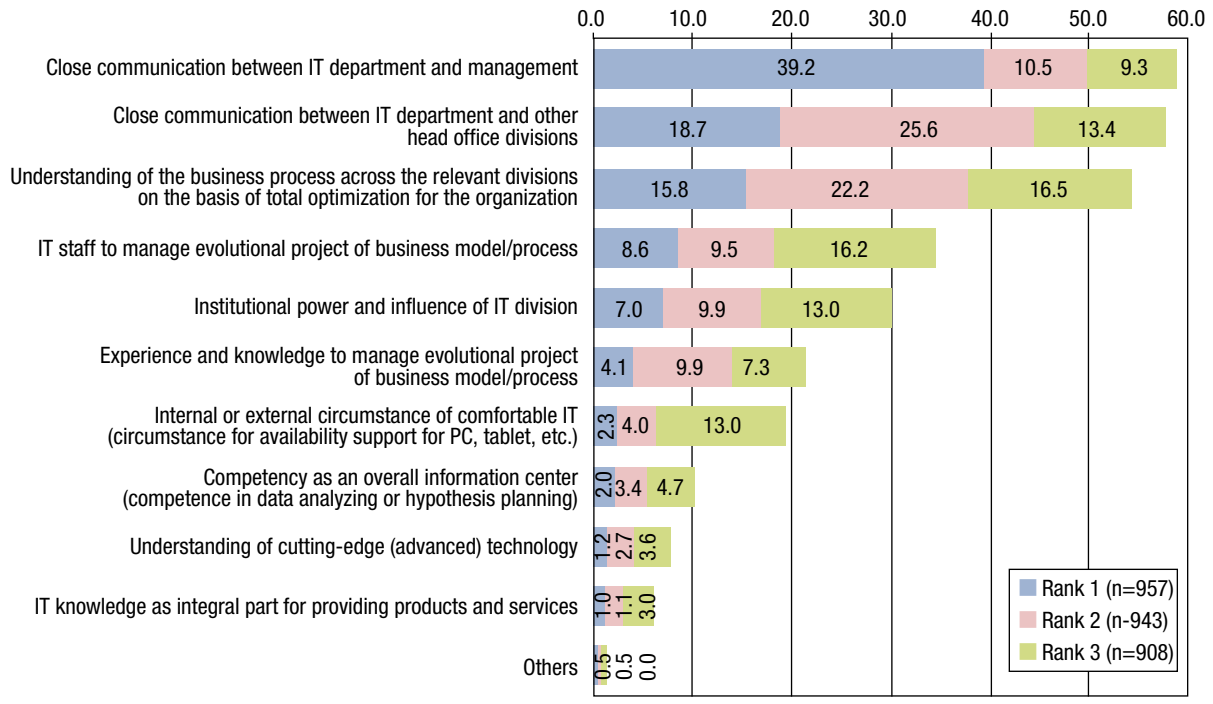
The insufficient involvement of management and relevant business divisions, particularly the

Figure 1—2013 Cisco Global IT Impact Survey/IT and Business Alignment



Source: Cisco. Reprinted with permission.

Figure 2—Tips to Lead Projects to Success



Source: Japan Users Association of Information Systems. Reprinted with permission.

operation leaders and planning staff, other than system users, can be derived from these results.

In IT projects, as a matter of fact, there is a tendency by project managers to define the scope of management involvement on the users' division or the system's division directly related to the system's development, leaving management and other indirectly related divisions insufficiently involved.

On the upper or hyper-upper process of an IT project, the organizational and progressive involvement by management and the business divisions is essential to preserve the alignment of the business process with IT, which could eventually optimize the effect brought about by the introduction of IT.

MODEL CASE AND EVALUATION FOR EFFECTIVE IT GOVERNANCE

In Japan, more than 70 percent of IT projects are recognized as failed projects. Two major causes are:

- Common project goals are not identified clearly so project stakeholders and all project members cannot share the same focus.
- Management intentions are not defined in the first phase of the IT project.

A potential solution for these issues is collaborative discussion with stakeholders based on the following models to understand all stakeholders' intentions for the project:

1. **Business model**—Usually, each stakeholder has slightly different expectation for certain IT projects. It is necessary to correspond those intentions with the objects of the IT project. Clear goal setting is the first step to success. The goal then leads to strategies. Strategies break down to business objectives, which achieve strategies. Business objectives break down to abilities, which achieve business objectives. Strategies are differentiator factors from competitors. Business objectives are internal objectives to achieve strategies. Activities are actions or capabilities to achieve business objectives. This model ensures that stakeholders clearly understand what business initiatives are expected to be achieved.
2. **Business process model**—Organizations must define ideal business processes to achieve the business model. The ideal

Figure 3—Categories and Number of Issues for Each Phase						
	Categories	Business Strategy/ Business Planning	IT Orientation	IT Planning	IT Requirement	Total
1	Gap between business strategy or plan and required systemization	12	10			22
2	Ambiguous priority order of requirements to deal with	8		2		10
3	Insufficient understanding of user's requirements	5				5
4	Ambiguous role sharing and organizational structure	4	10	13	13	40
5	Insufficient review of the business products or services		9	3		12
6	Ambiguous objective of project		7	3	4	14
7	Insufficient information of contracts or estimates		3	13	3	19
8	Insufficient business knowledge, experience and skill		3	6	7	16
9	Ambiguous vision of organization		2			2
10	Ambiguous specification of existing systems		1	1		2
11	Introduction of new technology and services		1			1
12	Insufficient review of development policy and planning			7		7
13	Insufficient management of project			3		3
14	Insufficient review of cost and effect			3		3
15	Incompleteness or low quality of the requirement definition				26	26
16	Ambiguous conditions to complete requirement definition				6	6
17	Inadequate risk management				1	1
	Total	29	46	54	60	
Source: Information Technology Promotion Agency, Japan. Reprinted with permission.						

business process might be different from current business processes. "As-is" describes the current business process, and "to-be" describes the ideal business process. Optimized business processes must be created from a goal-centric perspective as to-be.

3. **IT solution model**—This is the ideal solution overview to support the ideal business process. The business process contains not only tasks that are executed manually, but also tasks that should be supported by an IT solution to obtain an effective result (**figure 5**).[5]

This methodology defines the procedure to create those models with stakeholders based on collaborative discussion among each layer's stakeholders, including members of management who define strategies; middle managers who define business objectives; and experts and leaders who define activities as as-is, to-be and return on investment (ROI).

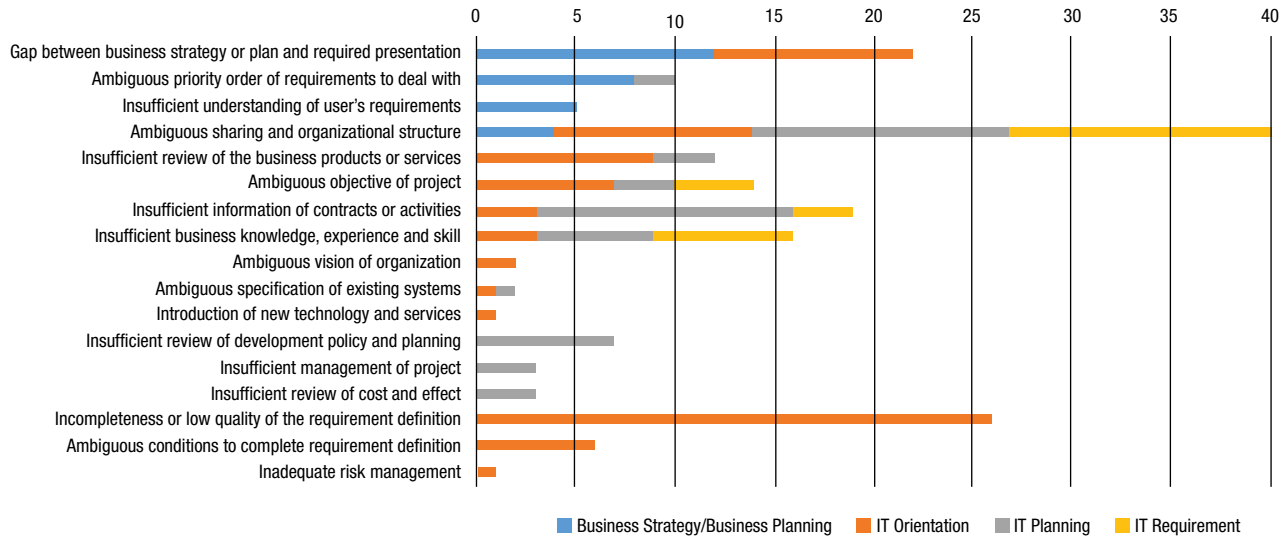
This collaborative discussion must take place as a workshop facilitated by an individual who is familiar with the methodology. It is effective when used to generate consensus among all stakeholders and create metrics. This method has been used effectively in industries ranging from telecommunications, to automotive original equipment manufacturing (OEM) and high-tech.

During the workshop, strategies, business objectives and abilities are organized based on importance and priority. The workshop must be facilitated to forge agreement among all participants based on proper information sharing and effective discussions. **Figure 6** illustrates an example of the output of the workshop.

As a result, all stakeholders recognize that the achievement of the abilities gives good impact to strategies.

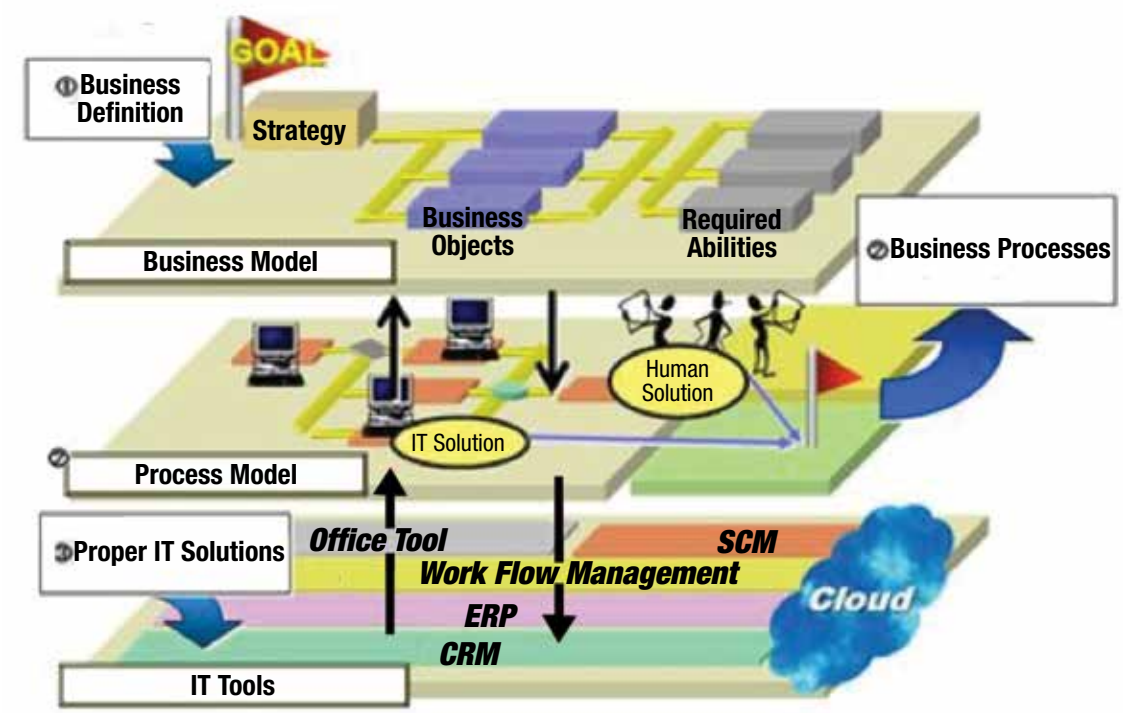
Figure 7 illustrates how the effects of the project can be estimated in the workshop.

Figure 4—Categories and Number of Issues for Each Phase



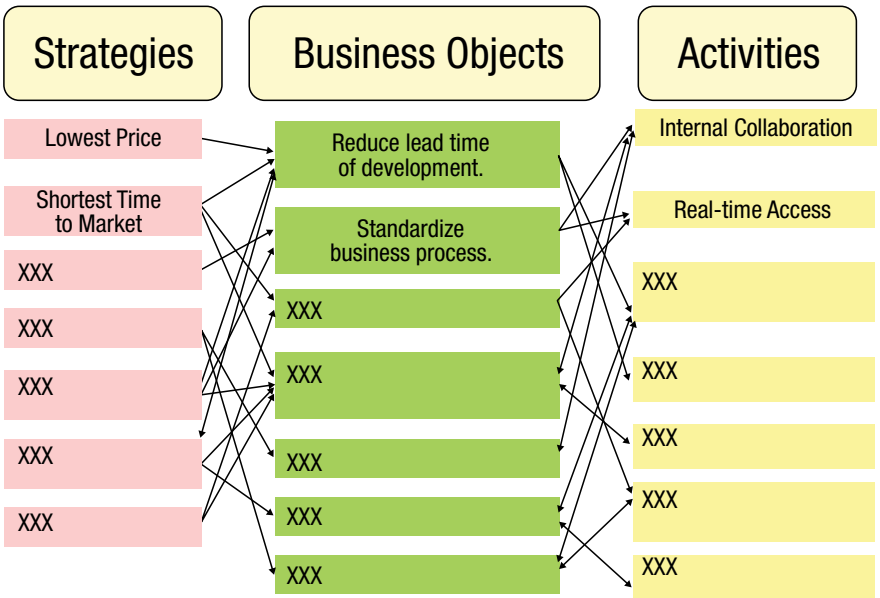
Source: Information Technology Promotion Agency, Japan. Reprinted with permission.

Figure 5—Total Optimization for Business Process and IT Based on Strategy



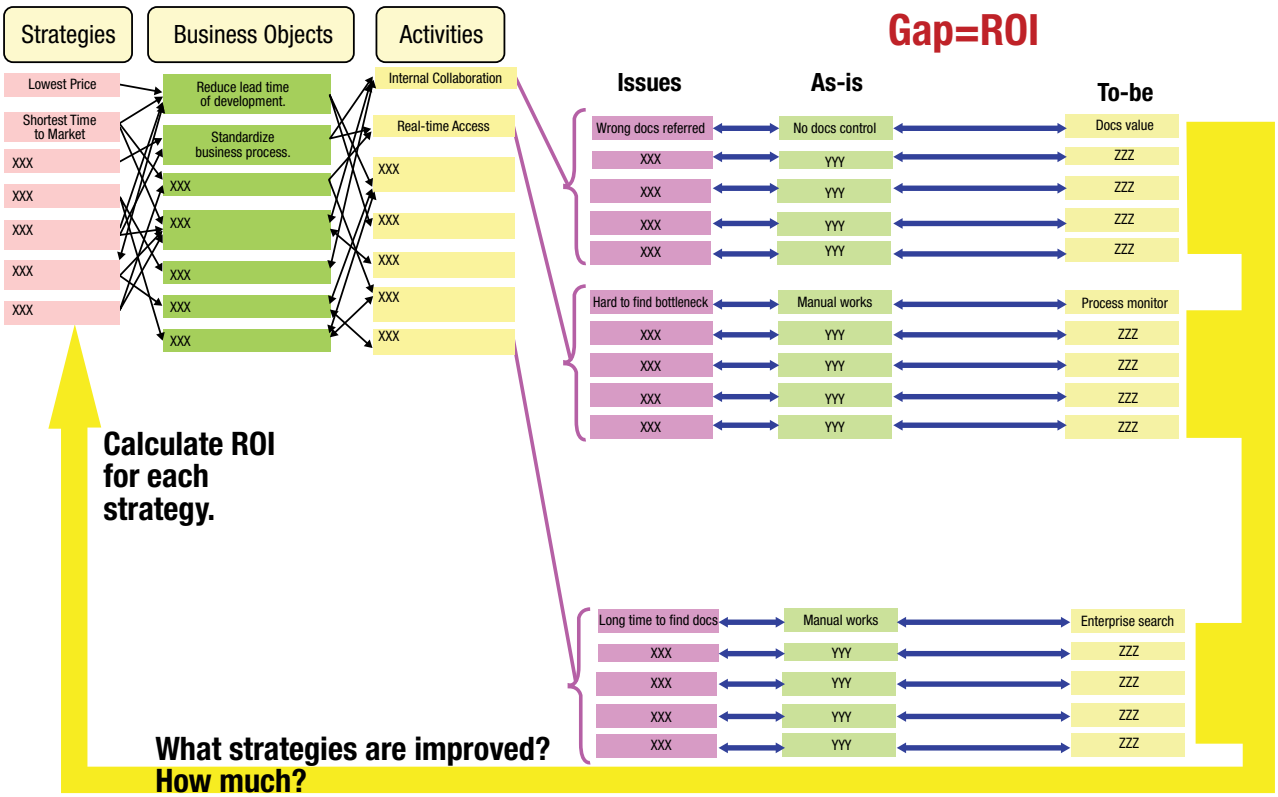
Source: Dream IT Research LLC; "Proper Project Plan Creation Methodology, SUSD," *Science of Success of IT Project*. Reprinted with permission.

Figure 6—Example of Workshop Output



Source: Dream IT Research LLC; "Proper Project Plan Creation Methodology, SUSD," *Science of Success of IT Project*. Reprinted with permission.

Figure 7—Concept of ROI Analysis



Source: Dream IT Research LLC; "Proper Project Plan Creation Methodology, SUSD," *Science of Success of IT Project*. Reprinted with permission.

Enjoying this article?

- Learn more about and collaborate on governance of enterprise IT (GEIT) in the Knowledge Center.

www.isaca.org/topic-governance-of-enterprise-it

Each ability defined in the workshop must be achieved to reach the goal. This means the abilities have not been realized because of some issue(s). Current business processes that include issues are called as-is. Those issues must be removed via process change or new IT solutions. Then, the ideal, to-be process is created.

A gap between as-is and to-be items exists. Gap analysis is executed by:

- Identifying issues that prevent execution of the abilities. Some issues may be already known/recognized. First, identify the cause of the issue, then identify the as-is item that is causing the issue, and finally define the to-be items to remedy the cause.
- Identifying which strategies have a positive effect on closing the gap between the as-is and to-be items and then estimating the effect (i.e., shorten time, reduce cost, increase revenue)
- Calculating the effects for each strategy based on the results of the gap analysis

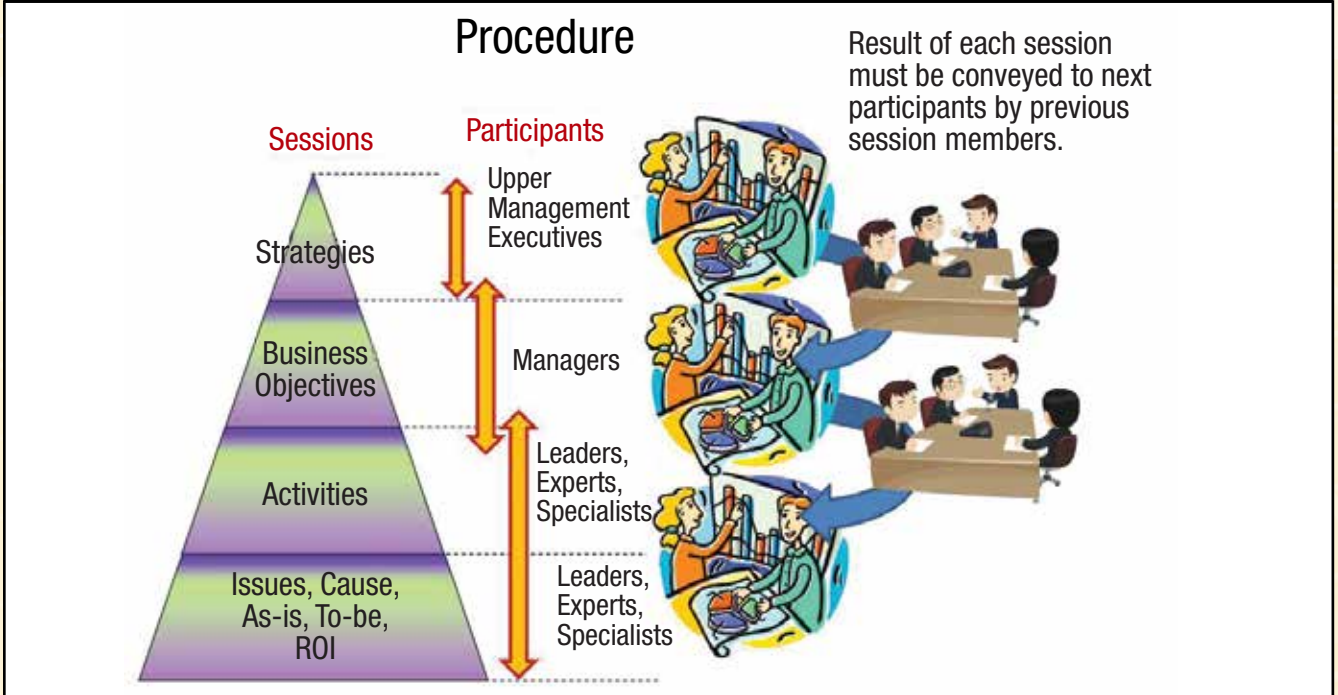
As a result, business goals can be properly mapped to processes and solutions. An integrated business, process and IT solution model is created. Every project member can recognize the project's big picture, any current issues, as-is and to-be items, and expected effects through the workshop and its deliverables.

The solution for the second cause, "management intentions are not defined in the first phase of IT the project," is illustrated in **figure 8**.

The workshop is developed to establish mutual understanding between management and lower-level team members. The goal of the workshop is to get agreement among all stakeholders.

All defined items are scored and prioritized and sorted by importance of agreement among all participants. The intentions of each participant are shown as points and visualized to expedite understanding of other people's intentions. Information

Figure 8—Method to Establish Agreement Among All Layers



Source: Dream IT Research LLC; "Proper Project Plan Creation Methodology, SUSD," *Science of Success of IT Project*. Reprinted with permission.

sharing and compromises are completed during the workshop. Points and visualized images not only expedite understanding, but also help to sort out items.

The workshop is split into three sessions: the strategy session, the business objectives session and the ability session. At the end of each session, the results and an overview of that session are described to participants of the next session by current participants of the previous session. Participants of the next session can ask questions and engage in discussion until all team members come to an agreement.

Each step of the workshop procedure is designed to understand other participants' background and intentions and to arrive at a consensus.

The results of the workshop include:

- Goals are clearly set with discussion of each stakeholder's intentions and removal of any misunderstandings. Gaps between stakeholders are adjusted. The risk of change requests and errors in development processes is drastically reduced.
- ROI and key performance indicators (KPI) are clearly defined in the project planning phase, which helps to evaluate the effect of the project after deployment.
- Investment in the project can be fully optimized. Only valuable IT solutions are implemented and only the most efficient processes defined.

Workshop support materials include templates, tools and other resources designed to execute a productive, efficient workshop to ensure consensus among all stakeholders.

CONCLUSION

By promoting involvement of management layers at each level of the business sector, it is possible to overcome management challenges related to alignment of business and IT.

In some IT projects, it is effective to proceed consciously with the involvement of other departments that senior management and project managers are not managing directly. When utilizing this methodology, it will increase the effectiveness and consistency with the strategy developed in the project-planning phase. In any project, from the individual project to organizationwide endeavors, it is essential to connect each process with the organizational strategy.

ENDNOTES

[1] Cisco, *The 2013 Cisco Global IT Impact Survey, www.cisco.com/en/US/solutions/collateral/ns1015/Cisco_IT_Impact_Survey_Results_2013.pdf*

[2] Japan Users Association of Information Systems (JUAS), The 19th Corporate IT Trend Survey, 2012

[3] Information Technology Promotion Agency, Japan, "Corporate Challenges and Countermeasures for High Quality on the Hyper-upper Process—Survey Report in Respect of the Improvement of the Precise Review on the Hyper-upper Process," March 2013. The author has translated to English from original contents (Japanese). In any case of mistranslation, the original is correct.

[4] *Ibid*.

[5] Dream IT Research LLC, "Proper Project Plan Creation Methodology, SUSD," *Science of Success of IT Project*

The Business Case as an Operational Management Instrument—A Process View

Kim Maes is a Ph.D. candidate in the department for information systems management at the University of Antwerp (Belgium) and IWT Fellow of the Agency for Innovation by Science and Technology.

Steven De Haes, Ph.D., is an associate professor at the University of Antwerp and Antwerp Management School (Belgium), co-editor-in-chief of the *International Journal on IT/Business Alignment and Governance (IJITBAG),* and academic director of the IT Alignment and Governance (ITAG) Research Institute.

Wim Van Grembergen, Ph.D., is a professor at the University of Antwerp and Antwerp Management School (Belgium), academic director of the ITAG Research Institute, and co-editor-in-chief of the *IJITBAG*.

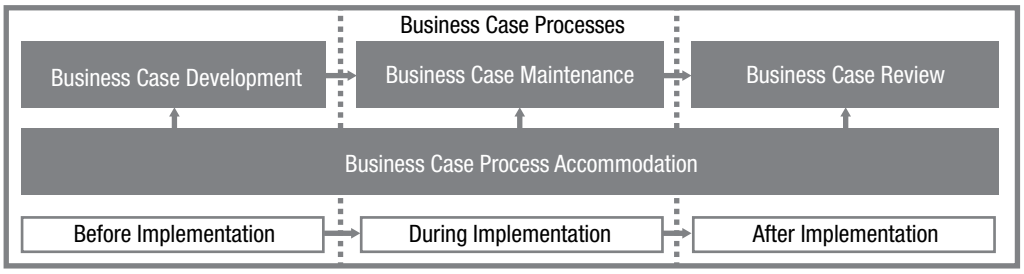
Many business cases are weakly developed or gather dust after the investment has formally been approved.[1] It is, however, recognised that using a well-developed business case throughout the investment life cycle can increase the investment success.[2, 3] Looking from a process perspective, a conceptual model of a business case process can facilitate continuous business case use throughout the investment life cycle.

To understand through which practices such a business case process can be implemented, a group of international experts from academia and practice were surveyed. In total, 31 business-case practices were defined, evaluated and labelled into categories of business case development, maintenance, review and accommodation. The findings show that practices focusing on stakeholder inclusion and what the investment wants to realise are fundamental. Taking into account the return on effort, organisations can preferably focus on practices that support business case development and maintenance.

CONCEPTUAL MODEL

A business case is a formal investment document that includes a structured overview of relevant investment information and provides a justification to support well-founded decision making.[4] Using such a business case throughout the investment life cycle requires a transformation of the formal business case static document into a living document.[5] A conceptual model can take a more process-oriented view towards the business case supporting its continuous use (**figure 1**). This business case process runs in parallel with an investment life cycle and consists of three distinct, but consecutive phases (development, maintenance and review) supported by an accommodating layer (**figure 2**). The four components are further operationalised through a set of logically related practices.

Figure 1—The Business Case Process Aligned With an Investment Life Cycle



Source: Maes, De Haes and Van Grembergen. Reprinted with permission.

Figure 2—Definition of the Business Case Process Model Components

Component	Definition: A Set of Logically Related Practices to…
Business case development	Identify relevant investment information that is integrated in a structured way with adequate and objective argumentation to provide a rationale and justification for the initial investment idea.
Business case maintenance	Monitor whether the investment is implemented in accordance with the business case (e.g., objectives, changes, costs), and update the business case with the prevailing reality (e.g., assumptions, risk).
Business case review	Monitor benefit realisation resulting from the utilisation of products and services, and facilitate the evaluation of the overall investment success.
Business case process accommodation	Facilitate an adequate execution of the business case process adjusted to the investment and organisational context.

Source: Maes, De Haes and Van Grembergen. Reprinted with permission.

EXPERT VIEW ON BUSINESS CASE PRACTICES: APPROACH

Twenty-four academic and practitioner experts distributed across various countries and industries were surveyed. The overall objectives were to determine initial definitions (obtained from literature and case research) of the business case practices validated and to examine the perceived effectiveness and ease of implementation of each practice to learn about its potential contribution. The research process employed to achieve the first objective will not be discussed here, but the resulting business case practice definitions can be found in **figure 3**. These definitions are necessary to discuss the research findings of the second objective. The background information of all experts is included in **figure 4**.

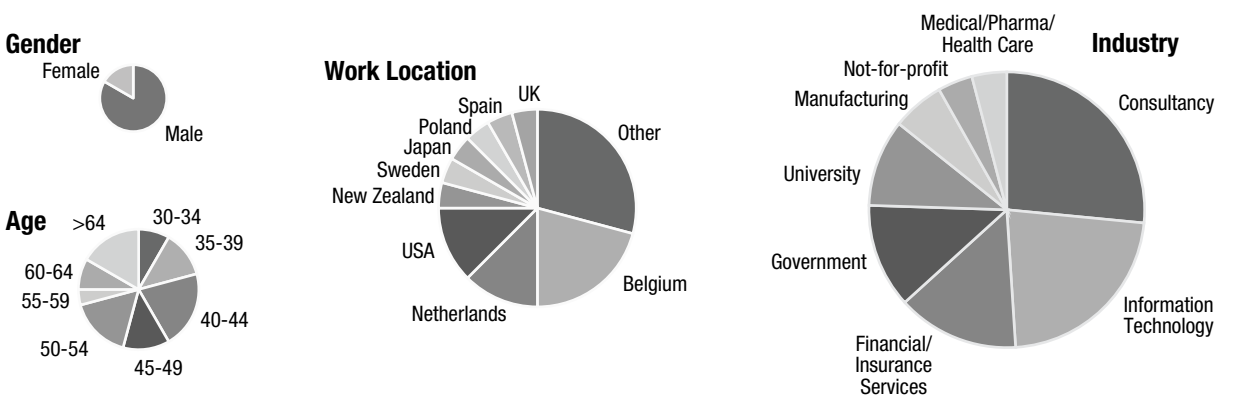
Figure 3—Validated List of Business Case Practices and Definitions

Code	A Business Case Is Developed by…	Definition
BCD01	Capturing investment vision	Capture the investment vision, and establish the appropriate investment context.
BCD02	Capturing business drivers	Capture the business challenges and opportunities that drive the investment and how they contribute to the achievement of the organisational strategy.
BCD03	Identifying stakeholder expectations	Identify the stakeholders' expectations, needs and requirements in terms of delivered benefits.
BCD04	Identifying technology opportunities	Identify proven and emerging technologies that support the business drivers and may realise the investment objectives.
BCD05	Identifying investment scope	Identify what will be done in the investment and what will not, and explain why.
BCD06	Identifying investment assumptions	Identify realistic assumptions and their logic for business drivers, investment objectives, investment solution(s), benefits and costs.
BCD07	Identifying investment objectives	Identify and categorise what objectives the investment should achieve.
BCD08	Identifying investment solution(s)	Identify what organisational and technological changes are required, design one or more alternative investment solutions and implementation scenarios, and assign change owners.
BCD09	Identifying investment benefits	Identify and categorise what benefits will be created by the investment based on relevant evidence, define their explicit measures, and assign benefit owners.
BCD10	Identifying investment costs	Identify and categorise what costs will be created by the investment based on relevant evidence, and define their explicit measures.
BCD11	Identifying investment risk	Identify and evaluate the impact and probability of investment risk and critical success factors, and determine preferred solutions to take a proactive approach.
BCD12	Developing benefit realisation plan	Develop a structured plan by when each benefit will be realised in relevant phases and with appropriate consideration of organisational factors.
BCD13	Evaluating investment feasibility and viability	Evaluate the feasibility and viability of each alternative investment solution.
BCD14	Evaluating cost/benefit analysis	Capture identified investment costs and benefits with measures and values, and evaluate the cost-benefit analysis to support the financial argumentation.
Code	**Maintained by…**	**Definition**
BCM01	Monitoring business case relevance	Monitor the business drivers, objectives and assumptions, and control whether they are still relevant and realistic.
BCM02	Monitoring investment scope	Monitor the investment scope and realisation of changes, and control whether it is still in line with the business case relevance.
BCM03	Monitoring investment costs	Monitor whether the investment costs are consumed according to the scope and identified changes.
BCM04	Monitoring investment risk	Monitor the investment risk, and evaluate its impact on the business case.
BCM05	Updating the business case to react adequately	Update the business case frequently based on business case monitoring, and identify adequate actions.

Figure 3—Validated List of Business Case Practices and Definitions *(cont.)*		
Code	**Reviewed by…**	**Definition**
BCR01	Identifying objective evaluation criteria	Identify and communicate objective criteria with predefined weighting that helps to evaluate the investment effectiveness and efficiency.
BCR02	Evaluating investment effectiveness	Monitor benefits realisation, and evaluate the contribution of investment objectives and changes.
BCR03	Evaluating investment efficiency	Evaluate the effort and costs that were consumed to realise the investment.
Code	**A Business Case Process Is Accommodated by…**	**Definition**
BCPA01	Establishing an adaptable business case approach	Establish an adaptable business case approach according to investment, and accept a growing maturation and granularity through its development and usage.
BCPA02	Establishing business case templates, training and guidance	Establish standard business case templates and tools, and accommodate training and guidance on what constitutes business case practices and how to employ them adequately.
BCPA03	Establishing maximum objectivity in business case usage	Maximise objectivity to support well-founded and comparable decision making without influence from politics, lobbying or institutional powers.
BCPA04	Establishing simple and dynamic business case usage	Describe and employ business case practices and their content in a simple, straightforward and dynamic manner to encourage their usage.
BCPA05	Establishing business case practices as a standard approach	Establish and evangelise business case practices as a standard way of working.
BCPA06	Ensuring business case practice improvements	Ensure business case practice improvements further through experience and continuous learning.
BCPA07	Ensuring communication and involvement with stakeholders	Ensure clear communication and active involvement with all stakeholders in order to gain insight, commitment and ownership.
BCPA08	Ensuring stakeholder confirmation	Ensure formal confirmation from relevant stakeholders on the (updated) business case to increase their commitment.
BCPA09	Evaluating business cases regularly	Evaluate all business case documents in order to make well-founded decisions to approve, continue or stop the investment.

Source: Maes, De Haes and Van Grembergen. Reprinted with permission.

Figure 4—Background Information of the Final 24 Experts



Source: Maes, De Haes and Van Grembergen. Reprinted with permission.

OVERVIEW OF BUSINESS CASE PRACTICES

An initial set of business case practices was identified during a systematic literature review complemented with five exploratory case studies. In a preliminary round of the Delphi study, several experts were interviewed individually to get feedback on the suggested practices and their respective definitions in order to derive a validated set of business case practices. The resulting 31 practices and definitions can be found in **figure 3**.

PERCEIVED EFFECTIVENESS AND EASE OF IMPLEMENTATION

What has been learned about the perceived effectiveness and ease of implementation of each business case practice?

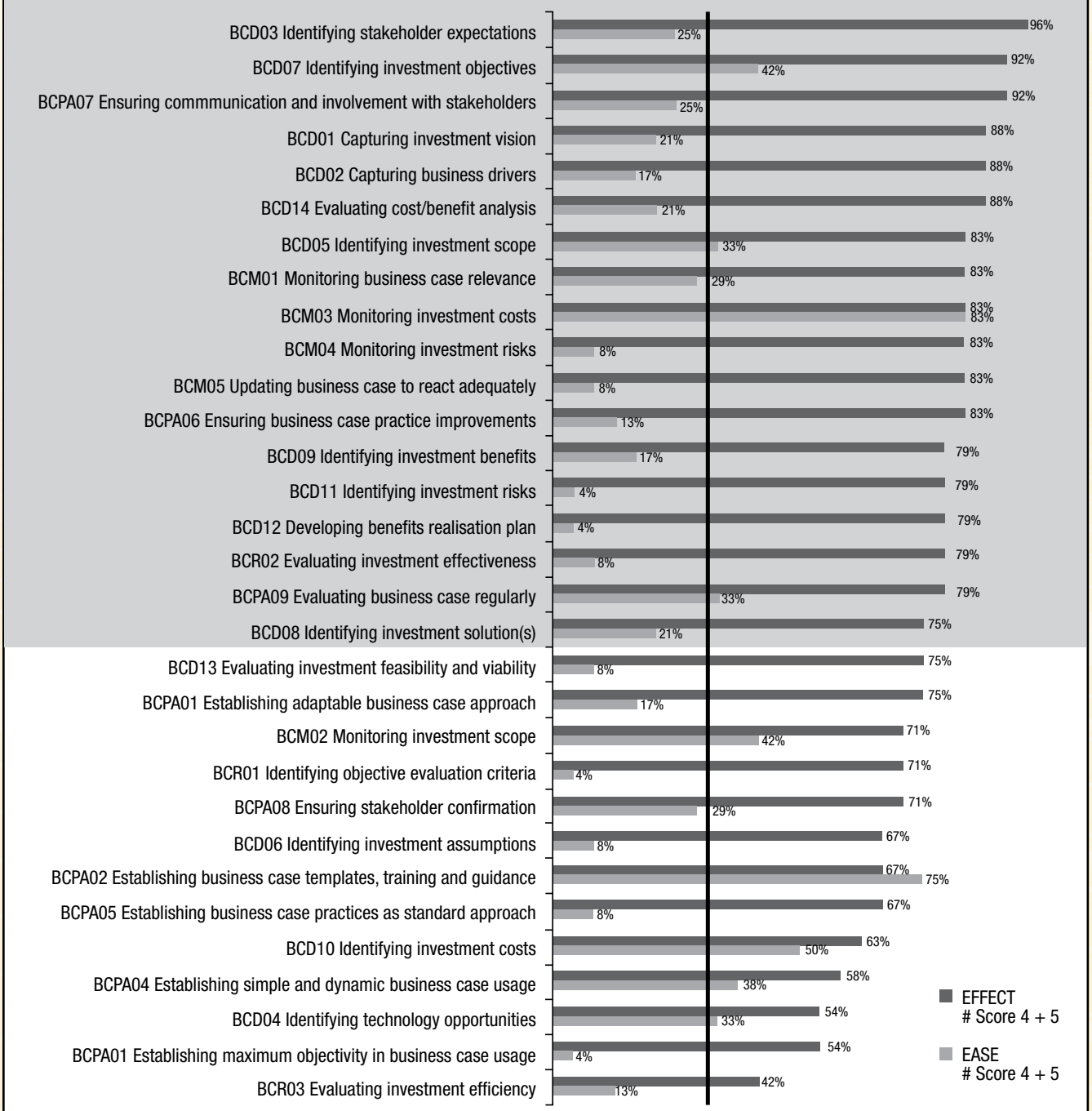
In the online survey, each expert was asked to score the practices on the two quality criteria by way of a five-point Likert scale. During the analysis, the number of experts who perceived a practice as highly effective (score 4-5) and easily implemented (score 4-5) were aggregated per practice. **Figure 5** displays the aggregated percentage of experts who attributed a score of 4-5 on the two quality criteria. The figure shows that the majority of experts (greater than 70 percent) perceived the upper 23 practices in the grey rectangle as highly effective. The highest levels of consensus were achieved on practice BCD03, BCD07 and BCPA07, while eight practices did not reach the 70-percent-consensus level for being perceived as highly effective.

In general, it was observed that stakeholders' attention is found to be highly effective; identifying their expectations (BCD03) and ensuring their active involvement (BCPA07) are positioned within the top three of highly effective practices and reach a very high level of consensus among experts. This does not come as a surprise as various academics have stressed the importance of stakeholder involvement and commitment.[6, 7] Another set of practices that is perceived to be highly effective deals with what the investment wants to realise. One expert clarifies, 'It is of utmost importance to (1) know exactly what problem you want to solve, (2) understand how this will be solved, and (3) obtain and maintain the desire to achieve this'. Although the latter refers mostly to the importance of stakeholder attention and involvement, the other two can directly be linked to BCD01, BCD02, BCD05 and BCD07. Indeed, the development of a business case should start from these fundamental practices.[8]

The consensus levels on perceived ease of implementation are much lower and analysis demonstrated that experts have great difficulty agreeing on the ease of implementation. In **figure 5**, the light grey bars for 25 practices do not reach the 30 percent consensus level indicated by the vertical black line. In other words, experts reached a high consensus level (greater than 70 percent) that these 25 practices are difficult or moderately difficult to implement. Likewise, many organisations still struggle with business case usage.[9, 10] IT people are often in the driver's seat when developing a business case, although the responsibility should be positioned on the business side. IT people are less able to perform this job as they have difficulties estimating the added value that comes from strategic and tactical business opportunities such as flexibility, service and market innovation.[11]

If an analysis is performed on the consensus levels per the business case process component, one can observe that the business case maintenance (BCM) component has achieved the highest consensus on its effectiveness, closely followed by those in the business case development (BCD) component (**figure 6**). The consensus level for business case process accommodation (BCPA) practices is still within the high consensus cut-off level (greater than 70 percent), while only 64 percent of the experts perceive business case review (BCR) practices as effective. Although all four components received a low to very low consensus rate on perceived ease of implementation, again, practices from the BCM component achieved the highest rating. Hence, one might reason that organisations will achieve the highest return on effort when they implement the practices from the BCM component. Following up on the relevance of the business case is certainly important,[12] because the business drivers and objectives can be impacted by a shift in market, organisational or technological issues. If an organisation wants to understand how it needs to react to these changes, this impact should be investigated. In case a dramatic change threatens the business case relevance, one should reassess the fundamental

Figure 5—Consensus Levels on Perceived Effectiveness and Perceived Ease of Implementation of Business Case Practices

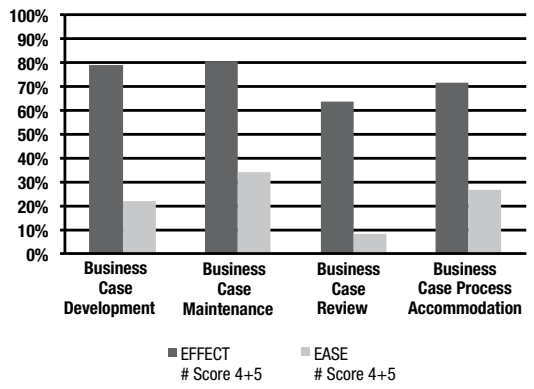


Source: Maes, De Haes and Van Grembergen. Reprinted with permission.

assumptions and perform a new cost-benefit analysis.[13, 14] It seems experts perceive the effectiveness of these BCM practices as high since they possess the ability to have a direct impact on last-minute changes and to contribute greatly to the effects of ongoing investment decision making.

The lowest return might be expected from practices in the BCR component, as those score lowest on effectiveness and ease of implementation. Potentially, experts have reasoned that the job is done by then and that these practices have no direct impact on the final result. This is, however, not entirely true because monitoring benefit realisation is included in BCR02 and believed to be critical after the resulting products and services from the investment have officially been launched.[15]

Figure 6—Consensus Levels on Perceived Effectiveness and Perceived Ease of Implementation of Business Case Practices Per Process Model Component



Source: Maes, De Haes and Van Grembergen. Reprinted with permission.

BUSINESS CASE PROCESS AND COBIT 5

After reviewing how a business case process can be executed and which business case practices are most effective to realise a successful investment outcome, how does one apply these findings? *COBIT® 5: Enabling Processes* offers various opportunities. For instance, the *Manage innovation* (APO04) process from COBIT® 5 helps an organisation be on the lookout for innovation opportunities and plan how it can benefit from innovation in relation to business needs. The business case practices BCD02 and BCD04 can be of direct help by identifying technology opportunities and capturing the business drivers of these opportunities in relation to the enterprise environment (COBIT 5's APO04.02 *Maintain an understanding of the enterprise environment* and APO04.03 *Monitor and scan the technology environment*). To understand how the organisation can benefit from these technology-enabled innovations, it can employ BCD09 and BCD12 to assess the potential of emerging technologies and innovation ideas (APO04.04). While BCD09 helps with the identification of the anticipated benefits, BCD12 outlines when these benefits should be realised. Practices from the BCM component can be of specific value for management practice APO04.06 by monitoring 'the implementation and use of emerging technologies and innovations during integration, adoption and for the full economic life cycle to ensure that the promised benefits are realised'.[16]

COBIT 5 process BAI01 can be used as a second example. It covers the entire investment life cycle of a programme/project, so it can be argued that multiple practices spread across the business case process can be of importance. As a practice to develop and accommodate the business case process, stakeholder inclusion is perceived to be highly effective in achieving a desirable investment outcome (supporting BAI01.03 *Manage stakeholder engagement*). As part of the management practice BAI01.02 (*Initiate a programme*), confirmation should be achieved from stakeholders on their active participation as a sponsor or member of the programme board or committee. The development of a benefit realisation plan (BCD12) and the continuous act of reviewing and updating the business case (BCM05 and BCPA09) are also foreseen in this management practice (BAI01.02). In addition, it is advisable to use practices BCM01 and BCM02 to evaluate whether the investment is still in line with the drivers and objectives and on track with the implementation of the required changes (BAI01.06 *Monitor, control and report on the programme outcomes*). The practices BCR01, BCR02 and BCR03, on the other hand, help to evaluate the investment contributions against predefined review criteria (BAI01.11 *Monitor and control projects*). The management of programme and project risk (BAI01.10) can be safeguarded by way of the business case practices to identify and monitor investment risk (BCD11 and BCM04). These two examples demonstrate that the business case process and its individual practices can be of use in parallel with the execution of some enabling processes from COBIT 5.

Figure 7—Mapping Diagram of Business Case Practices to Two Enabling Processes of COBIT 5		
	Manage Innovation (APO04)	**Manage Programmes and Projects (BAI01)**
BCD01 Capturing investment vision		
BCD02 Capturing business drivers	APO04.02	
BCD03 Identifying stakeholder expectations		BAI01.03
BCD04 Identifying technology opportunities	APO04.03	
BCD05 Identifying investment scope		
BCD06 Identifying investment assumptions		
BCD07 Identifying investment objectives		
BCD08 Identifying investment solution(s)		
BCD09 Identifying investment benefits	APO04.04	
BCD10 Identifying investment costs		
BCD11 Identifying investment risks		BAI01.10
BCD12 Developing benefit realisation plan	APO04.04	BAI01.02
BCD13 Evaluating investment feasibility and viability		
BCD14 Evaluating cost/benefit analysis		
BCM01 Monitoring business case relevance	APO04.06	BAI01.06
BCM02 Monitoring investment scope	APO04.06	BAI01.06
BCM03 Monitoring investment costs	APO04.06	
BCM04 Monitoring investment risks	APO04.06	BAI01.10
BCM05 Updating business case to react adequately	APO04.06	BAI01.02
BCR01 Identifying objective evaluation criteria		BAI01.11
BCR02 Evaluating investment effectiveness		BAI01.11
BCR03 Evaluating investment efficiency		BAI01.11
BCPA01 Establishing adaptable business case approach		
BCPA02 Establishing business case templates, training and guidance		
BCPA03 Establishing maximum objectivity in business case usage		
BCPA04 Establishing simple and dynamic business case usage		
BCPA05 Establishing business case practices as standard approach		
BCPA06 Ensuring business case practice improvements		
BCPA07 Ensuring communication and involvement with stakeholders		BAI01.03
BCPA08 Ensuring stakeholder confirmation		BAI01.02 BAI01.03
BCPA09 Evaluating business case regularly		
Source: Based on ISACA, *COBIT 5: Enabling Processes*, 2012, *www.isaca.org/cobit.*		

CONCLUSION

Observing the findings of this study, it is strongly advisable that organisations consider the application of a business case process with regard to their IT-enabled investments. As an essential starting point, organisations need to spend sufficient time and resources to understand what the investment is about and what they want to realise. The inclusion of relevant stakeholders, their active involvement and formal confirmation can be considered a second critical ingredient to achieving a successful outcome. Organisations do not need to start with the implementation of all 31 business case practices, but they can start with those practices that are considered to be most effective by experts.

> "Consider the application of a business case process with regard to IT-enabled investments."

This study can be used to help in the selection of appropriate business case practices in order to start implementing a business case process. Moreover, organisations that have already implemented COBIT 5 can benefit from the link between these business case practices and the COBIT 5 enabling processes.

This study was executed within the context of large for-profit organisations, but it would be interesting to undertake future research on the applicability of the business case process and practices in other environments. For instance, small- and medium-sized companies or governments might need other, or more focused, practices in each specific context.

REFERENCES

Flynn, D.; G. Pan; M. Keil; M. Mähring; 'De-escalating IT projects: The DMM Model', *Communications of the ACM 52*, vol. 10, 2009, p. 131-134

Fonstad, N.; D. Robertson; 'Transforming a Company, Project by Project: The IT Engagement Model', *MIS Quarterly Executive* 5, vol. 1, 2006, p. 1-14

Luftman, J.; E. McLean; 'Key Issues for IT Executives', MIS *Quarterly Executive* 3, vol. 2, 2004, p. 89-104

ENDNOTES

1 ISACA, *COBIT® 5: Enabling Processes*, ISACA, 2012

2 Swanton, B.; L. Draper; 'How Do You Expect to Get Value From ERP If You Don't Measure It?', AMR Research, 2010

3 Ward, J.; E. Daniel; J. Peppard; 'Building Better Business Cases for IT Investments', *MIS Quarterly Executive*, vol. 7, no. 1, 2008

4 Maes, K.; S. De Haes; W. Van Grembergen; 'Investigating a Process Approach on Business Cases: An Exploratory Case Study at Barco', *International Journal of IT/Business Alignment and Governance*, vol. 4, no. 2, 2014

5 *Op cit*, ISACA

6 Davenport, T.; J. Harris; J. Shapiro; 'Competing on Talent Analytics', *Harvard Business Review*, vol. 88, no. 10, 2010

7 Smith, H.; J. McKeen; C. Cranston; M. Benson; 'Investment Spend Optimization: A New Approach to IT Investment at BMO Financial Group', *MIS Quarterly Executive*, vol. 9, no. 2, 2010

8 *Op cit*, Ward, Daniel and Peppard

9 Franken, A.; C. Edwards; R.Lambert; 'Executing Strategic Change: Understanding the Critical Management Elements That Lead to Success', *California Management Review,* vol. 51, no. 3, 2009

10 Jeffrey, M.; I. Leliveld; 'Best Practices in IT Portfolio', *MIT Sloan Management Review*, vol. 45, no. 3, 2004, p. 41-49

11 Taudes, A.; M. Feurstein; A. Mild; 'Options Analysis of Software Platform Decisions: A Case Study', *MIS Quarterly*, vol. 24, no. 2, 2000, p. 227-243

12 Al-Mudimigh, A.; M. Zairi; M. Al-Mashari, *et al*; 'ERP Software Implementation: An Integrative Framework', *European Journal of Information Systems*, vol. 10, no. 4, 2001, p. 216-226

13 *Op cit*, Franken, Edwards and Lambert

14 *Op cit*, Jeffrey and Leliveld

15 Iacovou, C.; A. Dexter; 'Turning Around Runaway Information Technology Projects', *California Management Review*, vol. 46, no. 4, 2004, p. 68-88

16 *Op cit*, ISACA

Fire Protection of Computer Rooms—Legal Obligations and Best Practices

Haris Hamidovic, Ph.D., CIA, ISMS IA, is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the North Atlantic Treaty Organization (NATO)-led Stabilization Force in Bosnia and Herzegovina. He is the author of five books and more than 70 articles for business and IT-related publications. Hamidovic is a certified IT expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina and the Federal Ministry of Physical Planning of Bosnia and Herzegovina.

Considering that the issue of fire protection in computer rooms is not specifically addressed in many national regulations, the US National Fire Protection Association (NFPA) Standard for the Fire Protection of Information Technology Equipment (NFPA 75) can be used as a recognized fire protection technical standard for these environments. This standard is also recommended by the Telecommunications Industry Association (TIA).[1]

In addition to complying with fire safety regulatory requirements, the recommendations of the NFPA 75 standard can also help organizations address the following concerns:

- Fire threat of the installation to occupants or exposed property
- Economic loss from loss of function or loss of records
- Economic loss from value of equipment
- Business interruption

Although the probability of occurrence of fire originating in digital equipment (servers, storage units) is very low because there is little energy available to any fault and little combustible material within the equipment,[2] risk may be significant considering IT equipment has become a vital and commonplace tool for business, industry, government and research groups.

TECHNICAL AND ORGANIZATIONAL MEASURES

For computer rooms, there are recommended measures (technical and organizational) to prevent the spread of fire and ensure sufficient fire alerts and effective fire extinguishing. The following measures are, therefore, recommended: [3]

1. Construction measures:
   - The IT equipment room shall be separated from other occupancies in the IT equipment area by fire-resistant rated construction (not less than 1 hour).
   - Every opening in the fire-resistant rated construction shall be protected to limit the spread of fire and to restrict the movement of smoke from one side of the fire-resistant rated construction to the other.
   - Noncombustible material shall be used.
2. Installation of automatic fire detection and fire alarm systems:
   - Automatic detection equipment shall be installed to provide early fire warning. The equipment used shall be a listed smoke-detection-type system.
   - The alarms and trouble signals of automatic detection or extinguishing systems shall be arranged to annunciate in a constantly occupied location.
3. Installation of automatic fire protection systems:
   - Where there is a critical need to protect data in process, reduce equipment damage and facilitate return to service, consideration should be given to the use of a gaseous clean agent[4] inside units or total flooding systems in sprinklered or nonsprinklered IT equipment areas.
   - The ideal system would incorporate a clean gas system and a pre-action water sprinkler system in the ambient space. Gas suppression systems are friendlier to the hardware in the event of a discharge. There is some concern regarding the use of water on sensitive electronic equipment, whereas the hardware in a room subjected to a gas discharge can often be brought back online soon after the room is purged.[5] Gas systems are, however, one-shot designs. If the fire is not put out in the initial discharge, there is no second chance. The gas system cannot be reused until it is recharged or connected to a backup source. Water systems can continue to address the fire until it has been brought under control. While a water system is more likely to damage the hardware, it is also a better means of protecting the building structure. Water-suppression systems are often preferred or mandated by building owners or insurance companies. Water systems are also highly recommended in areas containing a high level of combustible material use or storage. The decision of what means of fire suppression to utilize must incorporate numerous factors, including the mission and criticality of the data center operations.[6]

- Effective room sealing is required to contain the clean agent so that effective concentrations are achieved and maintained long enough to extinguish the fire.
- NFPA recommends that the electronic and heating, ventilation, and air conditioning (HVAC) equipment be automatically shut down in the event of any suppression system discharge, although the reasoning behind this is different for water-based and clean-agent systems. Electronic equipment can often be salvaged after contact with water so long as it has been de-energized prior to contact. With water-suppression systems, the automatic shutdown is recommended primarily to save the equipment. With clean-agent systems, the concern is that an arcing fault could reignite a fire after the clean agent has dissipated. In either case, however, the decision to provide for automatic shutdown is ultimately the owner's, who may determine that continuity of operations outweighs either of these concerns.[7]

4. Additional organizational and other measures:
   - Designated IT equipment area personnel shall be continually and thoroughly trained in the functioning of the alarm system, desired response to alarm conditions, location of all emergency equipment and tools, and use of all available extinguishing equipment. This training shall encompass the capabilities and the limitations of each available type of extinguisher and the proper operating procedures of the extinguishing systems.
   - Listed portable fire extinguishers of the carbon dioxide type or a halogenated agent type shall be provided for the protection of electronic equipment. A sign shall be located adjacent to each portable extinguisher and shall plainly indicate the type of fire for which it is intended.
   - There shall be a management-approved written, dated and annually tested fire plan, damage control plan, and recovery procedures for continued operations.
   - Whenever electronic equipment or any type of record is wet, smoke damaged or otherwise affected as a result of a fire or other emergency, it is vital that immediate action be taken to clean and dry the electronic equipment. If water, smoke or other contamination is permitted to remain in the equipment longer than absolutely necessary, the damage can be grossly increased.
   - Seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

POTENTIAL DAMAGE TO ELECTRONIC EQUIPMENT

The primary damage to electronic equipment is caused by smoke that contains corrosive chloride and sulfur combustion by-products. Smoke exposure during a fire for a relatively short period of time does little immediate damage. However, the particulate residue left after the smoke has dissipated contains an active by-product that will corrode metal surfaces in the presence of moisture and oxygen.[8]

The most important asset to be preserved following the loss is corporate media (company database). Severe damage to disk read/write heads and tape transport mechanisms is probable if an attempt is made to operate with media that are not clean. A "head-crash," caused by particulate on the surface of a disk, will not only damage the drive, but result in a loss of data. Dirty tapes will stick and break, causing loss of data.[9]

IT equipment and materials for data recording and storage can incur damage when exposed to sustained elevated ambient temperatures. The degree of such damage will vary depending upon the exposure, equipment design and composition of materials for data recording and storage. The following are NFPA guidelines concerning sustained high ambient temperatures:[10]

- Damage to functioning information technology equipment can begin at a sustained ambient temperature of 79.4°C (175°F), with the degree of damage increasing with further elevations of the ambient temperature and exposure time.
- Damage to magnetic tapes, flexible discs and similar media can begin at sustained ambient temperatures above 37.8°C (100°F). Damage occurring between 37.8°C (100°F) and 48.9°C (120°F) can generally be reconditioned successfully, whereas the chance of successful reconditioning lessens rapidly with elevations of sustained ambient temperatures above 48.9°C (120°F).

- Damage to disc media can begin at sustained ambient temperatures above 65.6°C (150°F), with the degree of damage increasing rapidly with further elevations of sustained ambient temperatures.
- Damage to paper products, including punch cards, can begin at a sustained ambient temperature of 176.7°C (350°F). Paper products that have not become brittle are generally salvageable.
- Damage to microfilm can begin at a sustained ambient temperature of 107.2°C (225°F) in the presence of steam or at 260°C (500°F) in the absence of steam.

NFPA 75 also states that it is a popular misconception that electronic equipment exposed to water and moisture is permanently damaged. Water that is sprayed, splashed or dripped onto electronic equipment can be easily removed. Even equipment that has been totally submerged can be restored. However, in every case of water damage, immediate countermeasures are imperative. It is most important to turn off all electrical power to the equipment.

Automatic fire suppression systems provided in computer rooms should be selected with due consideration of the hazards being protected and the impact of the agent on energized information and communications technology (ICT) equipment or on unprotected emergency responders performing depowering functions. Detection and actuation systems should be periodically reviewed to avoid unwanted discharges of the automatic fire suppression systems. Accidental discharge of extinguishing agents can cause damage to equipment or danger to personnel. Fire suppression agents should not cause severe damage to the ICT equipment. Suppression agents such as those containing dry chemical agents or corrosive wet agents in fixed systems should not be used in any area containing ICT equipment.[11]

CONCLUSION

The formal implementation of protective measures will not be effective if these measures are not functional. For example, installation of the most expensive automatic fire extinguishing system will not produce results if the unit is defective.

Personnel responsible for fire protection have to stay informed on the building's changes, such as upgrades and renovations, to maintain projected technical characteristics of buildings with regard to fire protection.

In addition, it is necessary to maintain the good working condition of all installed equipment that allows the functioning of the designed fire-protection system.

Also, provision should be made for loss of critical equipment through fire, particularly where interruption to operations is not tolerable or where replacement times for equipment are beyond an acceptable period of interruption to operations. The fire protection strategy for computer rooms should be formulated after determination of, or in conjunction with, the choice of a disaster recovery plan. Small oversights might turn into economic disaster.

ENDNOTES

[1] Telecommunications Industry Association (TIA), TIA-942, "Telecommunications Infrastructure Standard for Data Centers," 2005

[2] Mangs, Johan; Olavi Keski- Rahkonen; "Full-scale Fire Experiments on Electronic Cabinets," VTT Building Technology, Publication 269, Finland, 1996, *www.vtt.fi/inf/pdf/publications/1996/p269.pdf*

[3] National Fire Protection Association (NFPA), NFPA 75, Standard for the Fire Protection of Information Technology Equipment, USA, 2013, *www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=75*

[4] A "clean agent" is an electrically nonconducting, volatile or gaseous fire extinguishant that does not leave a residue upon evaporation. National Fire Protection Association (NFPA), *Standard on Clean Agent Fire Extinguishing Systems*, USA, 2012, *www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=2001*

[5] British Standards Institution (BSI), BS 6266:2011, *Fire protection for electronic equipment installations—Code of practice*, UK, 2011

[6] Sun Microsystems Inc., *Sun Microsystems Data Center Site Planning Guide. Data Centers' Best Practices*, 2003

[7] *Op cit*, TIA

[8] *Op cit*, NFPA, 2013

[9] *Ibid*.

[10] *Ibid*.

[11] National Fire Protection Association (NFPA), NFPA 76, *Standard for the Fire Protection of Telecommunications Facilities*, USA, 2012, *www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=76*

Feature

Enhancing IT Governance With a Simplified Approach to Segregation of Duties

Kevin Kobelsky, Ph.D., CISA, CA, CPA (Canada), is an assistant professor of accounting at the University of Michigan—Dearborn College of Business (USA). Prior to academia, Kobelsky was an IT audit manager in the Toronto office of Ernst & Young and the manager of internal audit at Canadian Tire Corp. His research on the impacts of IT on organizational performance, market value and internal control has been published in several leading journals including *The Accounting Review*, *Journal of Information Systems* and the *International Journal of Accounting Information Systems*. His research has been funded by the US National Science Foundation (NSF) and profiled in *InformationWeek*. He is a member of the editorial boards of the *Journal of Information Systems* and the *International Journal of Accounting Information Systems*.

The effective design and implementation of segregation of duties (SoD) is a central topic in the governance of IT-based systems. It is one of six important characteristics to be considered in the selection and development of control activities (Principal 10's Points of Focus) in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control—Integrated Framework*[1] and is cited in the Public Company Accounting Oversight Board's (PCAOB) Audit Standard No. 5[2] and in the American Institute of Certified Public Accountants' (AICPA) AU 314.[3] While its objective is simple, the allocation of work so that an employee cannot both perpetrate and conceal errors or fraud,[4] its implementation is not. As has been observed, "…companies struggle with SoD compliance, and it … repeatedly stifles IT, internal audit and finance departments."[5] This is in large part due to the lack of consensus about best practices for SoD,[6] particularly for IT-related duties. This lack of consensus is clear in the segregation creep of ever-larger control matrices, identifying incompatible functions[7, 8] and the lack of development of general principles that can be applied effectively to a variety of practical settings. This is a particular problem for smaller firms in which SoD weaknesses occur in the majority of reportings of material weaknesses in internal control.[9]

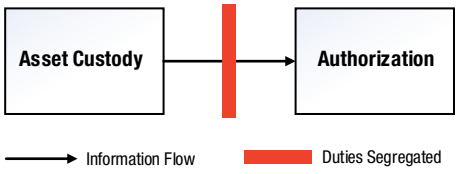
A simple, but powerful approach to identifying IT-based SoD conflicts has been developed and is based on fundamental organizational principles for control.[10] This approach allows organizations to strengthen SoD using fewer segregated duties than conventional approaches, helping small and large organizations enhance internal control and improve process efficiency and flexibility.

PRIMARY SOD: ASSET CUSTODY VS. AUTHORIZATION

To provide a conceptual foundation for SoD in IT-supported tasks, one must start with the most fundamental SoD: asset custody and authorization (**figure 1**). Absent independent authorization, employees who have custody of assets could misappropriate or reduce the value of assets without detection.

Также на русском
www.isaca.org/currentissue

Figure 1—Fundamental Segregation of Duties: Custody/Execution and Authorization



Source: Adapted from Kobelsky, K; "A Conceptual Model for Segregation of Duties: Integration Theory and Practice for Manual and IT-based Processes, *International Journal of Accounting Information Systems*, Forthcoming.

Asset custody includes duties in which, as part of a transaction, things of value to the organization are handled (physically or virtually), assigned a value or committed to, and poor performance of that duty could result in a loss to the organization. In the sales cycle, examples of these duties and related potential losses include:

- **Sales order pricing.** An example of asset valuation without physical custody, assignment of an inappropriately low price by a salesperson would result in a loss to the organization.
- **Picking and shipment of inventory.** All handling involves the risk of theft or damage by employees. Understatement of quantities input as shipped would result in a loss, while overstatement would lead to the overbilling of customers.
- **Receiving payments or other financial assets from customers,** which can be stolen, lost or inaccurately recorded

While a transaction may involve a simultaneous exchange of assets, often the selling organization

obtains a promise to receive payment. This records-based asset exists only in the records of the firm where it is vulnerable to manipulation and destruction. Employees who can enter transactions in these records are also considered to have asset custody. Examples of such duties and related threats include:

- Calculating the invoice total amount based on quantity shipped and price and recording this total in accounts receivable
- Reducing accounts receivable, both due to write-offs and payments received

Each transaction arising from these custody duties must be authorized by an independent employee having expertise or guidance sufficient to evaluate it.[11] For example, if prices for complex custom-made products in a dynamic business setting are negotiated in the field by the sales agent, the authorizer must possess sufficient knowledge to assess whether the prices are appropriate. If a price list has been preapproved, the authorizer must use this list. The authorizer should not directly or indirectly report to the asset custodian. Authorization by peers of the asset custodian is possible; however, peers can often be influenced, undermining their independence and increasing the risk of collusion. Independence is also essential in the opposite direction: The authorizer should not initiate or otherwise direct any custody transaction that he/she is responsible for authorizing. This prevents the authorizer from initiating and authorizing an inappropriate transaction with a colluding external entity.

A MODEL FOR PRIMARY SOD IN AN IT-SUPPORTED PROCESS

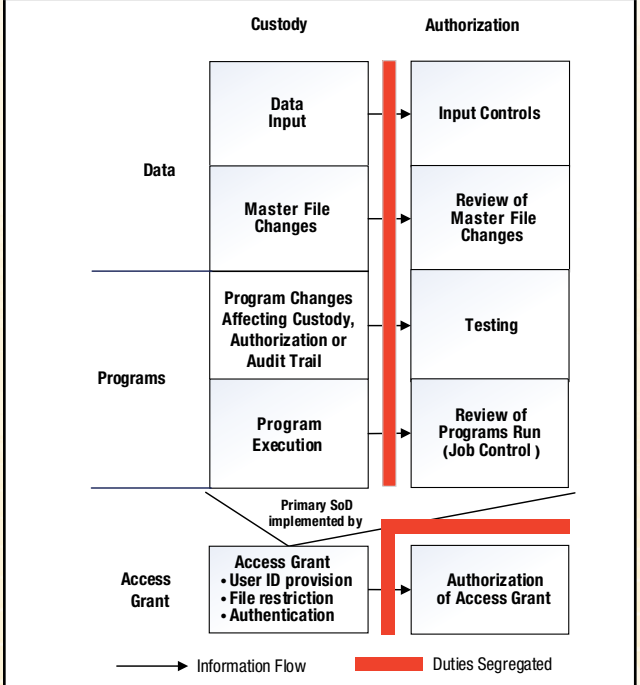
The introduction of IT to support a business process presents additional considerations in implementing SoD. The data associated with records-based assets and the recording of custody and authorization duties become susceptible to manipulation and loss in new ways because of the unique nature of IT-based processes. First, transaction and master file data must be input into the computer system, introducing the possibility of error. Second, these data are processed by software that will have programming errors arising from their development and maintenance or their operational execution. These data or programming errors could result in the loss of a valid transaction, an erroneous transaction or element of a transaction (e.g., an incorrect price is applied), an erroneous record of the transaction (e.g., a clerk records a lesser quantity than was actually shipped), or erroneous authorization of the transaction (e.g., an exception report omits a transaction having an inappropriate price).

These added data and programming risk require new segregations for IT-supported processes to achieve a level of SoD on par with that depicted in **figure 1** for manual processes. Just as with physical assets, paper-records-based assets require the ability to perform custody and authorization duties. Records of performance of these duties are protected by access restrictions in manual processes to achieve primary SoD. IT-based data and the programs that modify them must also be subject to access restrictions. In manual processes, access control is physical, implemented through policies restricting access to assets, records and authorization capability, which are enforced by all employees associated with the process, including some who are independent of custody and authorization tasks. In IT-supported processes, access control is primarily virtual and inconspicuous, enforced by software mechanisms administered by IT specialists at the application, database and operating-system layers. This means extra steps must be taken with IT-supported processes to ensure that access restrictions enabling SoD are articulated fully and implemented effectively.

The approach presented in **figure 2** has two key elements:

1. It treats each of the four primary IT activities (data input, master file changes, program changes and program execution) as manifestations of the custody duty, which requires independent authorization to prevent or detect and report inappropriate transactions. For example, input of sales order data must be subject to controls to reduce the incidence of keying errors affecting pricing, quantities and other fields. Master file changes must be reviewed to ensure that they are not temporarily changed to inappropriate values for a transaction (e.g., a vendor's name and mailing address are modified before a check run so that a check is made out to an unauthorized supplier) and then changed back afterward. Similarly, all program development changes must be independently tested, and there must be adequate preventive and detective controls to ensure that only appropriate programs, such as scheduling programs and review of operations logs, have been run.

Figure 2—Primary SoD of IT-related Duties in an IT-supported Process



Source: Adapted from Kobelsky, K; "A Conceptual Model for Segregation of Duties: Integration Theory and Practice for Manual and IT-based Processes," *International Journal of Accounting Information Systems*, Forthcoming.

2. It recognizes that limiting access to data and programs provides the foundation for segregating these duties (e.g., preventing a user who changes master files from authorizing these same changes). As a result, all access grants at the application, database, operating-system and network levels must be subject to independent authorization. The access-granting duty also includes tasks that facilitate access control, such as the implementation of encryption. The access grant authorizer should not perform any other custody or authorization duties because, if he/she does and the access granter erroneously gives the access grant authorizer access to a segregated duty (e.g., a custody duty that he/she authorizes), the access grant authorizer may be tempted to not report the error because it allows him/her to misappropriate assets.[12]

It is important to note what the model does not segregate. First, data and programming-related duties can be combined. The same employee could input data, make master file changes, write and maintain programs, and be the computer operator, as long as a second independent person (perhaps his/her supervisor) performs input controls; approves master file, program and program schedule changes; and reviews the log of programs run in production. As with non-IT duties, these controls can prevent fraudulent transactions if input controls and approvals are required before changes can be implemented. Further, with the exception of authorization of access grants, the duties described in **figure 2** do not need to be segregated from end-user custody and authorization tasks, so long as each end-user custody task is independently authorized. This is contrary to the commonly recommended practice of segregating the IT functions (i.e., development, testing and operations) from user departments and data entry from program changes.[13]

Second, the access-granting duty can be combined with any of the custody or authorization duties, including program execution, so long as an independent third person authorizes access grants. This also is contrary to some recommendations calling for segregating the database administrator (DBA) function from user departments and the IT security function from the rest of the IT function.[14] In the model, only the authorization of access grants as performed at all layers, including physical, application, database, operating system and network, and not the access grant function itself, must be separated from all other duties. This is necessary so that the authorizer of access grants does not authorize changes to his/her own access levels, which would compromise his/her independence. This could be implemented as a preventive control by having authorization required prior to the access grant's implementation or as a detective control by having authorization obtained afterward. This means the minimum number of employees necessary to achieve a primary level of SoD in an IT-supported process is three.

This three-way segregation model allows segregations that are quite different from the traditional four-way segregation of development, testing, operations and access control. These may be more efficient and more feasible for small organizations. Since the segregation within each row in **figure 2** is evaluated independently, to enhance efficiency, the two IT employees could exchange duties within any row. For example, the model would also allow one employee to input data, change programs, and review master file changes and operations logs associated with a second employee. A second employee could make master file changes, run programs, review the input and program changes made by the first employee, and grant access to users. These access grants would need to be reviewed and authorized by a third person. Given the small amount of time

required to perform this task in smaller firms, the access grant authorization could be performed by a trusted security expert outside the organization. The only limitation to exchanging duties relates to testing programs that perform input controls for, or keep an audit trail of, data input or master file changes. In this case, testing will be compromised if it is performed by the same person who has a data-related duty because he/she will be less likely to report program errors that reduce controls over inappropriate data input or master file changes.

Like traditional approaches, the model requires the IT system to provide reliable logs of programs run and changes to data, programs and access grants. These logs should not be subject to modification by any user without leaving a trail of that modification (e.g., use of a write once, read many [WORM] device).

CONCLUSION

A central element in the governance of internal control of organizations is the adoption of a conceptual approach for evaluating segregation of duties that is rigorous, yet flexible and effective in practice. The proposed model challenges convention and allows organizations, particularly small ones, to implement a basic level of SoD more efficiently and effectively.

ENDNOTES

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, 2013, *www.coso.org/IC.htm*

[2] Public Company Accounting Oversight Board (PCAOB), Auditing Standard No. 5, "An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements," 2007, *http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx*

[3] American Institute of Certified Public Accountants, Audit and Attest Standards: AU Section 314.126 B15, 2006, *http://aicpa.org/*

[4] Stone, N.; "Simplifying Segregation of Duties," *Internal Auditor*, April, 2009, *www.theiia.org/intAuditor/itaudit/2009-articles/simplifying-segregation-of-duties/*

[5] Adolphson, M.; J. Greis; "A Risk-based Approach to SoD, Partnering IT and the Business to Meet the Challenges of Global Regulatory Compliance," *ISACA Journal*, vol. 5, 2009

[6] Hare, J.; "Beyond Segregation of Duties: IT Audit's Role in Assessing User Access Control Risk," *ISACA Journal*, vol. 5, 2009

[7] ISACA, *CISA Review Manual 2005*, USA, 2004, chapter 2, p. 88-91

[8] ISACA, "Best Practices to Resolve Segregation of Duties Conflicts in Any ERP Environment," 2012, *www.isaca.org/Groups/Professional-English/it-audit-guidelines/GroupDocuments/SOD*

[9] Gramling, A.; D. Hermanson; H. Hermanson; Z. Ye; "Addressing Problems With the Segregation of Duties in Smaller Companies," *CPA Journal*, July 2010, p. 30-34

[10] Kobelsky, K.; "A Conceptual Model for Segregation of Duties: Integrating Theory and Practice for Manual and IT-based Processes," *International Journal of Accounting Information Systems*, forthcoming

[11] Protiviti, "Enhancing Sarbanes-Oxley Compliance Cost-Effectiveness," *FS Insights*, vol. 2, no.5, July 2007. The segregation of custody and authorization can operate in a preventive or detective manner. If the authorization duty occurs simultaneously with the custody duty before the latter can be completed, so that the transaction can be stopped before a loss occurs, it is preventive (e.g., reconciliation of batch control data before batch input is accepted for processing). If the authorization occurs after a loss might occur, it is detective (e.g., checking prices on orders after they are accepted by salespeople). Preventive controls reduce the likelihood of perpetration of errors, while detective controls reduce the likelihood of concealment of errors. In practice, firms often find that a preventive approach is more cost-effective.

[12] It is possible that the access granter could make the error of simultaneously giving the access grant authorizer access to custody and authorization duties, which would compromise the effectiveness of the authorization. An alternative approach to ensure that authorization of access grants is handled appropriately would be to have all access grant changes for the access grant authorizer's user ID reviewed by a third person. This would allow the access grant authorizer to perform other custody or authorization duties, keeping the total number of employees required for SoD to three. This alternative is not illustrated in **figure 2** for simplicity of presentation.

[13] Singleton, T.; "What Every IT Auditor Should Know About Proper Segregation of Incompatible IT Activities," *ISACA Journal*, vol. 6, 2012

[14] *Ibid*.

Feature

Law and Best Practices for a Sarbanes-Oxley Systems Review

Frederick G. Mackaden, CISA, CMA, PMP, is an enterprise resource planning (ERP) specialist supporting finance, sales, purchasing and manufacturing modules. He has more than a decade of experience in the ERP consulting environment and more than two and a half decades of experience. He is one of the contributors and reviewers of *A Guide to the Project Management Body of Knowledge, 5th Edition.*

Any organization would like to have an optimal approach to a Sarbanes-Oxley Act review, whether it is the process used or the Sarbanes-Oxley review team's composition. What is the recommended best process to review the internal controls in the core enterprise resource planning (ERP) business application? And what about the team composition? Drawn from a varied background, the team should be able to implement an internal control system commensurate with the size and nature of the organization. But who indeed should constitute this team and what should be their associated skill sets? This is a conundrum that many organizations face as they expand around the globe.

A LEGAL BACKGROUND ON SARBANES-OXLEY

"In the turn of the twenty-first century, several high-profile corporate scandals shook public trust. Insider trading, fraudulent financial records, and other deceitful incidents caused investors to question the integrity of the stock markets and their listed companies.[1] Investors began to move toward more conservative investments and abandon the stock market. Publicly listed companies swiftly began to lose their market value.

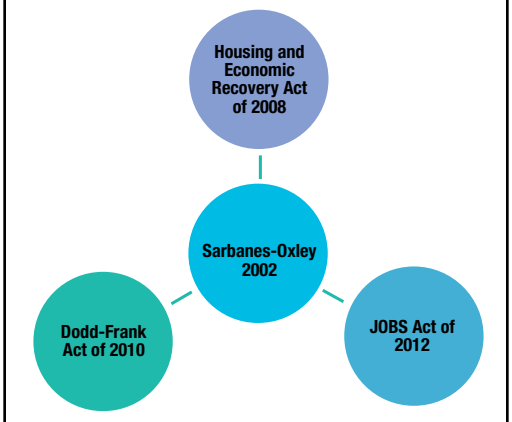
The issues at stake were highlighted by Alan Greenspan in his autobiographical *The Age of Turbulence*, in which he further mentions that the "ultimate control of American corporations by their shareholders is essential to our market capitalist system.[2] Corporate leaders had become a Platonic "wise elite"[3] with "absolute power."[4]

It is, therefore, to reassert the control on corporations that the act, authored by US Senator Paul Sarbanes and US Congressman Michael Oxley, "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes" was enacted on 30 July 2002. Sections 103, 302 and 404[5] govern the legal dimensions under which the information systems (IS) audit is conducted for Sarbanes-Oxley, as internal control in the modern corporation is implemented through information systems.

Section 404 (a) (1) notes, "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting." And, section 404 (a) (2) requires "an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."[6]

In recent years, several amendments have been made to the legislation. These amendments attempt to ensure that the legislation is in step with the needs of economic activity and the fact that some companies may be unable to afford Sarbanes-Oxley provisions in exceptional circumstances (**figure 1**).

Figure 1—Amendments to Sarbanes-Oxley



Source: Frederick G. Mackaden. Reprinted with permission.

The US Housing and Economic Recovery Act of 2008 has no effect on section 404 of Sarbanes-Oxley; the Dodd-Frank Act of 2010 includes exemption to nonaccelerated filers from section 404 (b); and the JOBS Act of 2012 exempts emerging growth companies from section 404 (b).[7]

A QUEST FOR AN EFFECTIVE PROCESS AND TEAM COMPOSITION

The recommended process (in summary) for the annual Sarbanes-Oxley analytic review is (where not expressly indicated, the tasks are expected to be done by the audit manager in association with the ERP specialist):

1. Initiate the review process:
   - Get the charter from the head of finance or head of organization in regard to the annual Sarbanes-Oxley review commencement for the fiscal year.
   - Identify stakeholders affected by the Sarbanes-Oxley annual review.
2. Plan the review process:
   - Create a Sarbanes-Oxley review plan, scope and schedule.
   - Make a list of the stakeholders involved in the review.
   - Make a Responsible, Accountable, Consulted and Informed (RACI) chart of the stakeholders involved in the review,
   - Plan risk management:[8]
     – Make a risk management plan.
     – Identify risk and create a risk register.
     – Perform qualitative risk analysis, as applicable, using risk probability and impact assessment, probability and impact matrix, risk data quality assessment, risk categorization, risk urgency assessment, and expert judgment.
     – Perform quantitative risk analysis, as applicable—data gathering and representation techniques, quantitative risk analysis and modeling techniques, and expert judgment.
     – Plan risk responses—strategies for negative risk or threats, strategies for positive risk or opportunities, contingent response strategies, and expert judgment.
3. Execute the review process:
   - Generate (completed by the security officer) the spreadsheet with the current user population using the ERP system(s), with the associated environments, menu masking, programs, business unit and function key securities to which the users have access. The human resources (HR) specialist provides the review team with the job descriptions currently on file.
   - Perform an analytical programmatic review (**figure 2**) (performed by the review team), and send the spreadsheet draft for discussion.
   - Complete iterative deliberations between the review team and the security officer.
   - Generate the pre-final spreadsheet (generated by the review team).
   - Implement pre-final recommendations (completed by the security officer).
4. Monitor and control the review process:
   - Control the review schedule.
   - Manage rollbacks:
     – Receive requests for rollbacks.
     – Review rollbacks for risk.
     – Perform discussions on rollbacks with user teams.
     – Approve rollbacks, if found justified.
     – Implement (by the security officer) approved rollbacks.
   - Control risk—risk reassessment, risk audits, variance and trend analysis, technical performance measurement, reserve analysis and meetings.[9]
5. Close the Sarbanes-Oxley annual review project:
   - Complete reporting and attestation of the Sarbanes-Oxley annual review for the fiscal year. File the final spreadsheet.
   - Note and file the lessons learned in the review.
   - Update job descriptions of users (completed by the HR specialist).
   - Update the risk register.

THE ANALYTICAL PROGRAMMATIC REVIEW

At first a risk assessment may be done identifying program areas as high, medium or low risk. If there is a stiff time deadline, the focus is on high- and medium-risk areas. High-risk areas are those relating to revenue and cost. Medium-risk areas are those relating to selling, general and administrative overheads. Other income and deductions are low risk. For risk management, the processes recommended by the Project Management Institute (PMI) could be adopted.

First, the environments being used by the ERP application need to be identified and the methods of promoting configurations from one environment to another need to be checked. Especially of concern are the interfaces to the production or live environment. Second, the list of menu masking ("a method of securing entire menus or individual selections on a menu by a user"[10]) is examined on a need-to-have basis. Third, the programmatic (action code—concerned with Add, Change and Delete to a table) accesses are subject to scrutiny on a need-to-have or need-to-know basis. Fourth, business unit security (legal entities or business units being accessed) needs to be scrutinized once again on a need-to-have or need-to-know basis. Business unit security is a "passive security mechanism. If you do nothing, there will be no business unit security."[11] With regard to business unit and legal entity security, the need-to-have or need-to-know element should be considered as the user may or may not need to know what is being done by another legal entity. Sometimes this would also mean that new user groups or responsibilities (always ensure that users are linked to a user group/responsibility with the

Figure 2—User Types and Clearly Conflicting Roles

Type of User	User Role															
	Doing Final Financial Report For Legal Entity	Doing General Ledger Journal Entries	Doing Finance Sales Invoices	Doing Cash Applications	Doing Finance Purchase Invoices	Doing Cash or Bank Payments	Doing Sales Invoices	Creating or Amending the Customer Master	Updating of the Price Master	Creating Vendor Master With Bank Accounts	Doing Purchase Orders	Doing Purchase Receipts	Doing Purchase Receipt Reversals	Processing Work Orders	Updating Cost Tables	Doing Shipments to Customers
Finance: Accounts receivable user			x	x												
Finance: Accounts payable user					x	x										
Finance: Reporting specialist	x	x														
Vendor set-ups: Address book administrator						x				x						
Customer set-ups: Address book administrator			x	x			x	x								x
Sales order management: Sales order administrator				x			x				x					x
Sales order management: Price administrator							x		x							
Purchase order management: Purchase order administrator						x					x	x	x			
Manufacturing: Work order administrator							x							x		x
Manufacturing: Cost accountant		x											x		x	

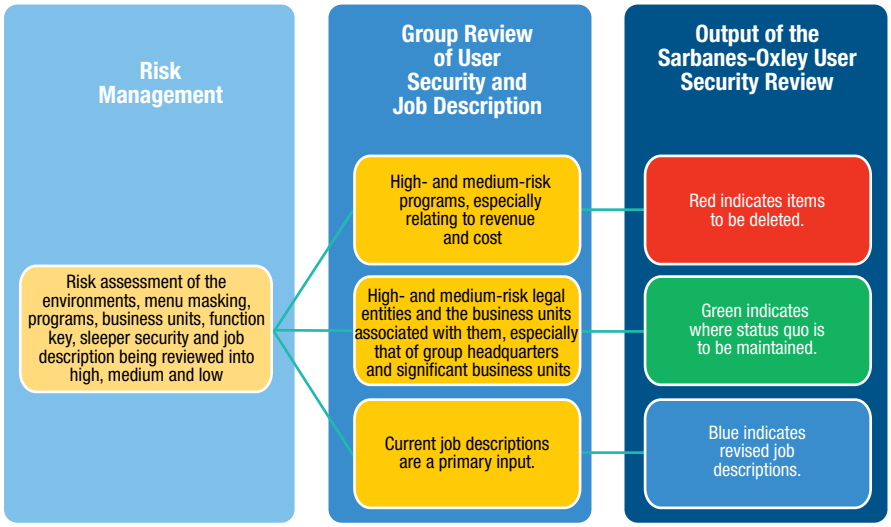
Source: Frederick G. Mackaden. Reprinted with permission.

requisite security) would be spawned as the user's roles and responsibilities may be exclusive enough to warrant this. At times, therefore, inquiry-only access may be granted and may be enough for the user to perform day-to-day tasks. Fifth, function-key security ("allows one to set up security on function keys and/or options by forms or user"[12] and can be used for reports and programmatic security) is examined—once again, on a need-to-have basis. Sixth, a list of unattended night operations (sleeper) jobs and people with access must be examined on a need-to-have basis. Also, the sleeper jobs for the entity need to be checked thoroughly. Finally, a list of functional users who have performed transactions and system adjustments (system specialist) should be corroborated with the user list from the security officer and placed under the microscope especially for material transactions.

Some examples of appropriate role-based security are to ensure separation of manufacturing users involved in work orders and sales order administrators involved in invoicing; separate accounts receivable users handling sales invoices from those handling cash applications; and separate accounts payable users entering vendor invoices from those processing payments. A risk-based focus is always an imperative so that one does not get lost in the woods with trivialities. A laser-shape focus, especially while analyzing high-risk areas (such as programs relating to revenue and costs), helps the perspective a great deal. Those requiring compensating controls could be, for example, when revenue-side programmatic accesses overlap with expense or cost-side accesses—such as in the case of drop ship orders (when the vendor ships directly to the customer) when a sales order administrator generates a purchase order back to back. Always bear in mind that section 404 of Sarbanes-Oxley ultimately drives all this with its objective of having an adequate internal control system structure in place (**figure 3**).

Then the most important thing to consider for section 404 is to examine the trial balance generated by the ERP system and reconcile it to the numbers in the financial reporting software. Usually these are separate software in large corporations. Besides, given that the financial reporting software ultimately provides the numbers in the annual report and is available in the public domain, this is a key area. The controls associated with this are critical and need to be a mandatory target for access controls and internal controls to ensure accuracy of

Figure 3—The Applications Programs Associated With the ERP in Use



Source: Frederick G. Mackaden. Reprinted with permission.

the numbers. Besides, people responsible for the financial reporting should not have access to do manual journal entries (**figure 2**). Users doing cash or bank reconciliation should not be involved in the operational aspects, doing cash or bank receipt applications and cash or bank payments. And the payroll administrator should not have access to make payroll payments in the ERP's HR suite.

THE PRIMARY SARBANES-OXLEY REVIEW TEAM AND THE ANALYTICAL REVIEW

The primary review team needs an internal audit manager, an HR specialist, a finance specialist, an ERP specialist and an ERP security officer. For the purpose of explanation, call this team Team Composition A. The internal audit manager serves as the facilitator for the discussions. The HR specialist brings the job descriptions as of that fiscal year. The security spreadsheet from the ERP security officer details the security roles each person has on the ERP application. The ERP specialist contributes what each program does and its functionality. The team then works through this and the output is a color-coded spreadsheet following the stop-light approach (**figure 3**). Red indicates access that needs to be removed. Amber indicates items that need further thought and iterative discussions with the ERP security officers (they have an in-depth knowledge of the ERP security system). Green indicates those users who can maintain *status quo*. Next on the agenda is a preimplementation review meeting. The output of this meeting is that the recommendations become dual color as red means that accesses needed removal and green means that *status quo* could be maintained until the next review.

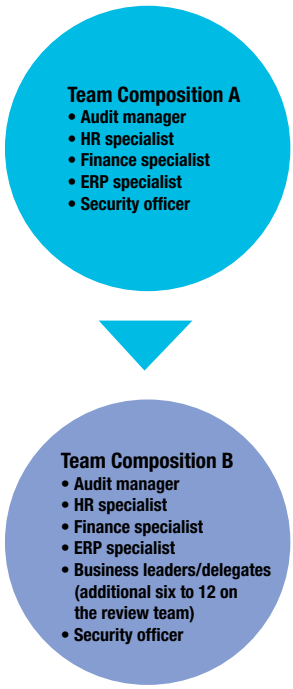
There is a need to budget for business down time during the period in which the security officer implements the recommendations. Strong requests to roll back some of the recommendations may be the order of the day. Users may, for example, voice strong arguments for access that the review team thought unnecessary.

Over the years, the team members achieve a rhythm in their work; go through the "forming, storming, norming, performing phases";[13] and actively challenge each other, if required, without conflict. But specialization does not easily keep in step with business growth. While suitable for an organization of fewer than 1,000 employees, growth beyond that would need a different team composition, much like Team Composition B (**figure 4**).

THE FINAL FRONTIER SARBANES-OXLEY REVIEW TEAM

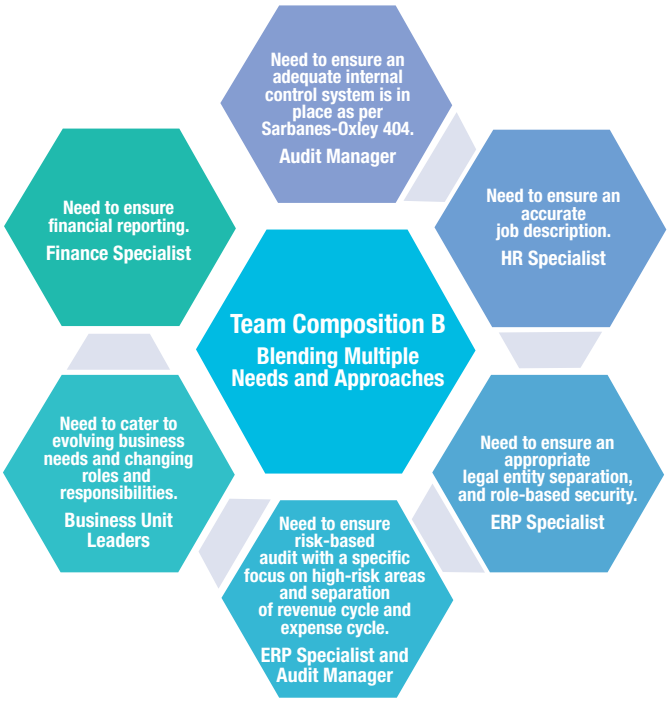
The team members involved in Team Composition A would not know the shifting sands of time in terms of the users' current roles and responsibilities as the business roared ahead. This is where the business leaders (executive-level management) bring in their expertise in terms of the needs of the business and how that translates in terms of roles and responsibilities for various users of the ERP systems. Moreover, the business leaders are

Figure 4—Recommended Sarbanes-Oxley Review Team Compositions and Team Evolution



Source: Frederick G. Mackaden. Reprinted with permission.

Figure 5—Team Composition B Functions



Source: Frederick G. Mackaden. Reprinted with permission.

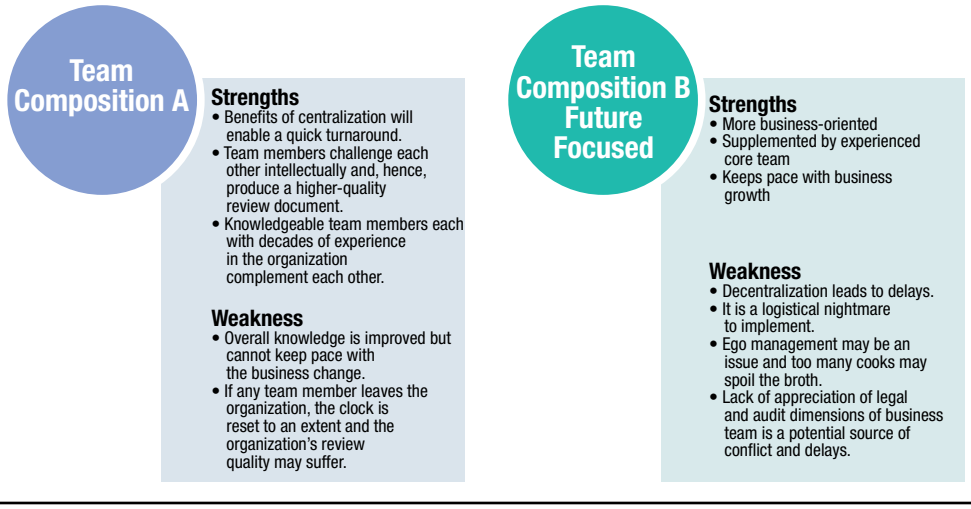
the data owners for operational areas of the business. They are responsible for the sales-order processing, purchase-order processing and work-order processing. For finance, the relevant business unit finance controller or director becomes the data owner. This is how the futuristic Team Composition B (**figure 5**) evolves when business unit leaders or their knowledgeable delegates join the review team.

Multiple points of view may coalesce as shown in **figure 5**. The security team would also engage in training business unit leaders and acting as the final sounding board and implementers of the annual review—this time, hopefully, without any rollbacks. Team Composition B may run into problems, especially as decentralization brings delays and with the difficulty of educating business leaders (for more strengths and weaknesses, refer to **figure 6**). But the central Team Composition A would also need to help educate and develop the new business-savvy team members. This also conforms to the idea that such "knowledge is not only valuable in itself but can contribute to the wise government (of the corporation) and reform."[14] Rollback requests would be extremely minimal as the business takes responsibility for annual reviews. Another future area for consideration would be the possible automation of the process, where possible.

OTHER BASIC AREAS TO BE REVIEWED

The other areas that also need to be considered, in addition to application access and associated controls, are physical access and its associated controls and network access and its associated controls. With regard to physical access, the best access is through dead-man doors because of their inherent ability to prevent tailgating. As applications are hosted on a server, the access to the server would be only for people authorized through swipe cards and passwords. If wireless is used, the unauthorized access is checked through a firewall so that war driving is prevented. For applications, basic login is through a user ID and password. The password needs to have an expiry date not greater than 90 days, and unused user identities would need to be disabled after a period of 30 working days (assuming some users may take long holidays). When a user leaves the organization, network access must be disabled prior to departure and the physical entry access card must be returned to the organization.

Figure 6—Strengths and Weaknesses of Sarbanes-Oxley Team Compositions



Source: Frederick G. Mackaden. Reprinted with permission.

CONCLUSION

A Sarbanes-Oxley review is not a simple task, and over time the complexity may increase exponentially in proportion to the length, breadth and depth of the business. It involves multiple departments and leads to revisions to job descriptions for the users concerned.

Following the initial analysis of the business, it is imperative to create a roles and user profiles matrix (**figure 2**) to identify the conflicting roles that need to be a focus for the Sarbanes-Oxley audit. Areas supporting the application also need to be checked for appropriateness for supporting the internal control structure. In this spirit lies the need to have "adequate internal control structure and procedures."[15]

A methodical approach, especially one with a project management approach, helps enhance the credibility and efficacy of the review. Furthermore, an approach with experienced team members ensures that the Sarbanes-Oxley audit is not "asking the ignorant to use the incomprehensible to decide the unknowable."[16] It evolves over time and the team can make recommendations that may involve a few rollbacks. Users and their managers understand that the process for rollbacks is not always simple. But the flip side is inaction. "Inaction….in the present means deep trouble in the future. Here…lies the threat to capitalism. It is what causes men who know that that things are going quite wrong to say that things are fundamentally sound."[17]

ENDNOTES

1 Anand, S; *Essentials of Sarbanes-Oxley*, John Wiley and Sons, 2007
2 Greenspan, A.; *The Age of Turbulence*, Penguin Books, 2008
3 Stevenson, L.; *Seven Theories of Human Nature*, Oxford University Press, 1974
4 *Ibid*, p. 31
5 Congress, Sarbanes-Oxley Act of 2002, USA, 2002
6 *Ibid*.
7 Howe, J. S.; *The Sarbanes-Oxley Act at 10*, Ernst and Young LLP, 2012
8 Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition*, 2013
9 *Ibid*.
10 JD Edwards & Company, "Technical Foundation Release A7.3," *http://docs.oracle.com/cd/E40228_01/technical/a73_tech_foundation.pdf*
11 *Ibid*.
12 *Ibid*.
13 *Op cit*, Project Management Institute
14 *Op cit*, Stevenson, p. 34
15 *Op cit*, Sarbanes-Oxley
16 Zobel, H. B.; "'The Jury on Trial' in American Heritage," July-August 1995, in N. Sherrin, *Oxford Dictionary of Humerous Quotations*, Oxford University Press, 2008, p. 184
17 Galbraith, J. K.; *The Great Crash 1929*, Penguin Books, 1975

Feature

Conducting IS Due Diligence in a Structured Model Within a Short Period of Time

Bostjan Delak, Ph.D., CISA, CIS, is a senior consultant for information systems (IS) advisory and audit at ITAD Audit and Consulting Ltd., Slovenia. Over the last few years, Delak has conducted more than 40 IS audits. From 1998 to 2012, Delak delivered more than 65 IS due diligences in 15 countries across central and eastern Europe.

Marko Bajec, Ph.D., is an associate professor at the Faculty of Computer and Information Science, University of Ljubljana, Slovenia. Bajec has received several awards and recognitions for his achievements in transferring knowledge to the IT industry. Since 2009, Bajec has been the head of the laboratory for data technologies, where he manages research in the fields of data integration, analysis and visualization.

While companies today are more or less effective and efficient when using information and communication technology (ICT), with the ever-growing impact of information systems (IS) on the daily business support of organizations, the IS governance of an organization has become very important, if not vital. Due diligence is one method of getting the necessary knowledge of existing IS. Other means include IS reviews, IS audits, IS certification and other IS analysis.

The term "due diligence" usually refers to a specific activity during the merger and acquisition process. There are four types of IS due diligence: initial, general, vendor and technology. Initial IS due diligence protects investors and shareholders from making any wrong decisions or underestimating their resources before acquiring the target organization. General IS due diligence is used upon the request of stakeholders or an organization's top management to get the status of an important part of IS or to get the complete status of IS. When an organization decides to outsource some or all IS processing activities, vendor IS due diligence should be performed.[1] Technology IS due diligence is performed on prospective technology investments.

It is critical to follow a structured framework in IS due diligence activities;[2, 3, 4] experience shows that most companies do not.

Despite an in-depth review of existing literature, no research that would identify and describe weaknesses of individual approaches could be found. The Information Technology Assessment Due Diligence Framework (ITADD framework) developers from Red McCombs Business School of the University of Texas at Austin (USA) "found that no conceptual framework or specific tool for evaluating the IT environment of companies being acquired is readily available."[5]

The following framework for IS due diligence delivery, the Framework for Information System Due Diligence (FISDD), has been developed and validated in response to this need, specifically to evaluate the following areas with the goal of analyzing risk and commercial opportunities:[6]

- IT organization and flexibility
- Network design, application and information architecture
- Data centers, premises and facilities
- Contract and regulatory requirements
- Business process integration
- IT tools and methodologies

IS DUE DILIGENCE

IS due diligence may be referred to as general or operational when it is used upon the request of stakeholders or an organization's top management to get the status of an important part of IS or a complete status of IS in the organization in line with its objectives (e.g., vision, strategy, tactical plans). Such an exercise may be carried out when a new chief executive officer (CEO) or chief information officer (CIO) is hired and would like to get an independent review of the organization's IS.

While an organization may decide to outsource some or all of its IS processing activities, vendor IS due diligence[7] should be performed prior to the IS outsourcing and afterward on an annual basis to mitigate risk related to IS and data exposure.

Technology due diligence, "the process by which alternative technologies and technology services are vetted,"[8] is performed on prospective technology investments. Thus, the more technology due diligence is understood, the better technology leverage is understood.[9]

FRAMEWORK DESCRIPTION

From 1998 to 2006, the team that later developed FISDD conducted more than 40 general and more than 25 initial IS due diligence engagements in central and eastern Europe. When the team started conducting due diligence assessments in practice, the information on approaches was limited. Over the years, the team became acquainted with a number of

specific approaches, determined each approach's strength and weakness, and discovered additional subareas to these approaches. Unfortunately, the team found that there was no comprehensive approach that could be of assistance for a quick IS due diligence; this was later confirmed by the study of ITADD framework papers.

The FISDD was created in a similar manner as the ITADD framework; it started in the late 20th century with a simple questionnaire requesting a listing of IS assets. In time, it was integrated with relevant portions of information obtained in, for example, ITIL, international standards (e.g., ISO/IEC 9000, ISO/IEC 27000, ISO/IEC 20000), audit techniques, COBIT®, the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control—Integrated Framework*, and other publications.

The resulting framework for IS due diligence delivery synthesizes these other frameworks and includes upgrades for areas that did not cater to a rapid IS due diligence (e.g., detailed process description, list of required documents, questionnaires). The FISDD also incorporates a decision model, based on the experiences of the framework developers.

The FISDD includes four phases (**figure 1**):

1. Preparation
2. Realization/onsite review
3. Analysis
4. Decision

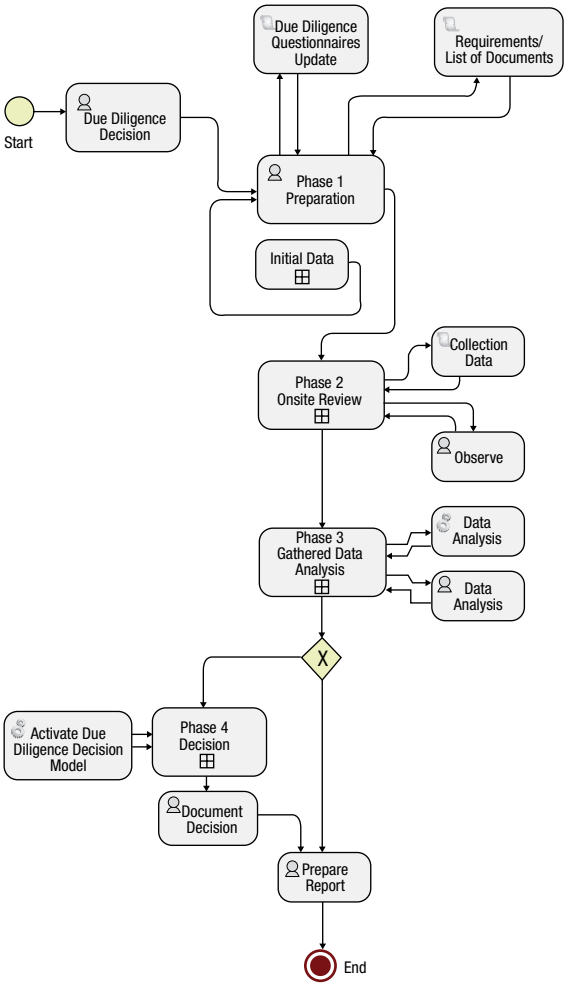
Each phase involves specific activities and subprocesses. The FISDD, because of its structured and well-documented guided approach (a sample list of requested documents, several questionnaires, samples of reports) and a better and formally specified process, allows for the IS due diligence process to be conducted in a relatively short period of time.

TIME REQUIRED FOR IS DUE DILIGENCE

The time frame for each phase may vary depending on the size of the observed organization, its location(s) and available documentation.

The FISDD allows the IS due diligence process to be conducted in a relatively short period of time. **Figure 2** shows the time required to complete IS due diligence and the time for onsite review, depending on the size of the observed organization.

Figure 1—Framework for IS Due Diligence



DECISION MODEL

The FISDD is not a completely new method to be put alongside the others, but an attempt to create a broad

Figure 2—Total and Onsite Review IS Due Diligence Time Frames

Type	Size of the Observed Organization	Minimum Number of Days*	Maximum Number of Days*	Onsite Staff/Days (up to)
A	Up to 150 employees, one major location, and up to three other locations	13	17	5
B	Between 150 and 350 employees, one major location, and up to five other locations	18	22	7
C	Between 350 and 750 employees, two to four major locations, and five to 15 other locations	25	29	9
D	Between 750 and 2,000 employees, three to five major locations, and 15-30 other locations	30	35	11
E	Between 2,000 and 3,500 employees, five to seven major locations, and 30-50 other locations	36	44	15
F	Between 3,500 and 6,000 employees, seven to 10 major locations, and 50-75 other locations	49	61	21
G	Between 6,000 and 10,000 employees, 10 to 15 major locations, and 75-100 other locations	69	85	29
H	More than 10,000 employees, more than 15 major locations and more than 100 other locations	88	112	36

* Indicates gross time. If more than one IS specialist is involved in delivery of IS due diligence, the period is shorter. For example, if three IS specialists work on due diligence, the activity will take between 30 and 38 days in total for the largest observed organization, with an onsite review of a maximum of 12 days; whereas, in the smallest observed organization, the total time required ranges from around six to seven days, with onsite review a maximum of two-and-a-half days.

synthesis method using the existing methods, approaches and frameworks to make due diligence goals easier and quicker to achieve with a simple, but comprehensive decision model.

The most important part of FISDD for IS due diligence is the decision model. The model needs several inputs, some of which must be defined by the stakeholders or their representatives from the investment company. This is undertaken during the first phase of due diligence by confirmation of the due diligence parameters and their weights. This means that for each parameter, a predefined due diligence value factor (factors A-G in **figure 3**) and a maximum value range (max. A-G in **figure 3**) must be defined before due diligence activities are started.

Through the analysis phase, different outcomes are calculated and they represent valuable inputs to the decision model.

RESPONSIBILITIES OF MANAGERS AND OTHER SPECIALISTS

IS due diligence involves several obligations and responsibilities. According to the FISDD methodology, the profiles presented in **figures 4** to **7** are required to participate in different types of IS due diligence.

For initial and vendor IS due diligence, a Responsible, Accountable, Consulted and Informed (RACI) matrix for the organization initiating the due diligence activities is presented in **figure 4**.

For the observed organization—either for the initial IS due diligence for potential acquisition or for vendor IS due diligence in case of potential vendor/outsourcing service provider—the activities to be carried out are presented in **figure 5**.

Figure 6 presents activities to be carried out for general IS due diligence.

The last RACI matrix, in **figure 7**, presents the activities to be carried out for technology IS due diligence.

CASE STUDIES

The FISDD was evaluated by an observational method while conducting IS due diligences in financial industry organizations in various countries of central Europe (Bosnia and Herzegovina, Bulgaria, Kosovo, and the Russian Federation) in addition to one nonfinancial organization (Slovenia) (**figure 8**).

When conducting these IS due diligences, all of the framework's predefined processes, activities, procedures, questionnaires, templates and its decision model were used.

Figure 3—FISDD Decision Model Table						
		Weight		Defined Range	Questionnaire and Analysis Outcomes	Decision
#	Description	Sign	Pre-DD Defined Value Factor	Maximum		Calculation
1	IT current asset value	A	Factor A	Max. A	Analysis Process Outcome A	Calculation A
2	IT investments for next five years	B	Factor B	Max. B	Analysis Process Outcome B	Calculation B
3	IT costs for next five years	C	Factor C	Max. C	Analysis Process Outcome C	Calculation C
4	Investor's human resources requirements	D	Factor D	Max. D	Analysis Process Outcome D	Calculation D
5	IT strengths and weaknesses maximum deviation	E	Factor E	Max. E	Analysis Process Outcome E	Calculation E
6	IT risk degree	F	Factor F	Max. F	Analysis Process Outcome F	Calculation F
7	Product diversity degree	G	Factor G	Max. G	Analysis Process Outcome G	Calculation G
	TOTAL		**100**			**Decision Outcome**

Figure 4—RACI Matrix for Initial and Vendor IS Due Diligence—Initiating Organization									
Activity	Board	Chief Executive Officer	Chief Financial Officer	Chief Technology Officer	Chief Information Officer	Chief Risk Officer	Chief Operations Officer	IS Due Diligence Team Leader/ Manager	IS Due Diligence Team
Make decision for activating IS due diligence.	A	R	R	R	R	R	R	I	
Prepare for IS due diligence/ parameters.		A	R	R	R	C	C	I	
Conduct IS due diligence onsite.		I	I	C	C	I	C	A	R
Analyze gathered data.								A	R
Prepare the report.								A	R
Present the report to the board and stakeholders.	R	R	C	C	C	C	C	A	I
Decide to continue/not continue.	A	R	R	R	C	C	C		

Figure 5—RACI Matrix for Initial and Vendor IS Due Diligence—Observed Organization

Activity		Chief Executive Officer	Chief Financial Officer	Chief Operations Officer	Business Process Owners	Project Management Office	Privacy Officer	Compliance	Human Resources Manager	Audit Manager	Chief Information Security Officer	Chief Information Officer	Head Architect	Head of Development	Head of IT Operations	Database Administrator	LAN/WAN Administrator	Developer	System Administrator	Help Desk Team	Other IT Personnel	IS Due Diligence Team Leader/Manager	IS Due Diligence Team
Prepare for IS due diligence.		C	C	A	I	I	I	I	I	C	I	I	I	I	I	I	I	I	I	I	I	I	
Conduct IS due diligence onsite.	Interviews with IT											R	C	C	C	C	C	C	C	C	C	A	R
	Interviews with end user	C	C	R	C	C	C	C	C	C	C											A	R
	Visiting IT premises						I			C	C	I		I	R		I	I	I	I	I	A	R

Figure 6—RACI Matrix for General IS Due Diligence

Activity		Chief Executive Officer	Chief Financial Officer	Chief Operations Officer	Business Process Owners	Project Management Office	Privacy Officer	Compliance	Human Resources Manager	Audit Manager	Chief Information Security Officer	Chief Information Officer	Head Architect	Head of Development	Head of IT Operations	Database Administrator	LAN/WAN Administrator	Developer	System Administrator	Help Desk Team	Other IT Personnel	IS Due Diligence Team Leader/Manager	IS Due Diligence Team
Make decision for activating IS due diligence.		A	I	R				C	I	C		R										C	
Prepare for IS due diligence.							C	I		C	C	R	R	R	R	R	C	C	C	C	C	A	R
Conduct due diligence.	Interviews with IT											R	C	C	C	C	C	C	C	C	C	A	R
	Interviews with end user	C	C	R	C	C	C	C	C	C	C											A	R
	Visiting IT premises						I			C	C	I		I	R		I	I	I	I	I	A	R
Analyze gathered data.		I		I								I										A	R
Prepare the report.		I		I								I										A	R
Present the report to the board.		A	R	C	I	I	C	I	C	C	C	R	C	C	C	I	I		I			R	I

Figure 7—RACI Matrix for Technology IS Due Diligence

Activity	Chief Executive Officer	Chief Financial Officer	Chief Technology Officer	Chief Operations Officer	Chief Risk Officer	Business Process Owners	Project Management Office	Privacy Officer	Compliance	Audit Manager	Chief Information Security Officer	Chief Information Officer	Head Architect	Head of Development	Head of IT Operations	Database Administrator	LAN/WAN Administrator	Other IT Personnel	IS Due Diligence Team Leader/Manager	IS Due Diligence Team
Make decision for activating IS due diligence.	A	C	R	C	C	C						C							I	
Prepare for IS due diligence.	I	I	A	R	I	C													R	I
Conduct IS due diligence.	I	I	R	C	C	C	C	C	C	C	C	C	C	I	I	I	I	I	A	R
Analyze gathered data.			R									I							A	R
Prepare the report.			I									I							A	R
Present the report to the board.	R	C	A	R	C	C	C	C		I		C							R	I

Figure 8—FISDD Case Studies						
Case	Country	Due Diligence Type	Total Time (Staff/Days)	Onsite time (Staff/Days)	Decision Model Output	IS Manager Feedback
Bank A	Kosovo	Initial	12	5	0.56	Positive
Bank B	Russian Federation	Initial	9	4	0.20	Positive
Bank C	Bulgaria	General	7	3	Not applicable/recommendations	Positive
Bank D	Bosnia and Herzegovina	Initial	11	5	0.40	Positive
Organization E	Slovenia	General	13	6	Not applicable/recommendations	Positive

Initial IS due diligence and general IS due diligence types were carried out.

The purpose of the case studies was to formally verify the validity of the approach and its results. The case studies took place between 2007 and 2012.

The case studies confirmed that the framework allows for rapid IS due diligence delivery and the integrated decision model provides short, but precise answers. Based on the feedback from the organizations' IS managers, the case studies confirmed that the due diligence activities did not disturb their daily operations more than an external IS audit. The fulfilled framework questionnaire—the FISDD IS status—provided complete and current IS documentation for daily operations and future IS external audits.

CONCLUSION

The IS due diligence process is very similar to the general IS audit process. Due to its inherent complexity, however, it requires a framework for delivery. The FISDD is not a completely new method to be placed alongside others. It is a comprehensive synthesis method based on the developers' extensive personal experience in the field of initial and general IS due diligence and the integration of existing methods, approaches and frameworks that have proven effective in specific domains of application (e.g., information security, value of IT).

The framework offers a detailed description of the IS due diligence process, clearly defining the procedures for each phase of review, the tools (questionnaires) and the report templates. Using the FISDD, these activities can be performed more easily and in a more structured manner. The FISDD's questionnaires provide a wide spectrum of data to be collected and analyzed, and the report templates guide the due diligence performer and enable an efficient presentation of the findings.

Compared to other approaches, the FISDD represents a complete framework that can be used in due diligence activities in a short period of time. The integrated decision model, a novelty compared with other approaches, provides short but exact answers that can then be used for further activities.

REFERENCES

Delak, B.; M. Bajec; "Framework for the Delivery of Information System Due Diligence," *Information System Management*, vol. 30, no. 2, 2013, p. 137-149

Gattiker, U.; "Merger and Acquisition-Effective Information Security Depends on Security Metrics," *Information Systems Control Journal*, vol. 5, 2007, p. 51-56

ENDNOTES

[1] Bayuk, J.; "Vendor Due Diligence," *ISACA Journal*, 2009, vol. 3, p. 34-38, *www.isaca.org/archives*

[2] *Ibid*.

[3] Bhatia, M.; "IT Merger Due Diligence—A Blueprint," *Information Systems Control Journal*, 2007, vol. 1, p. 46-49, *www.isaca.org/archives*

[4] Sundberg, B., *et al*; "A Framework for Conducting IT Due Diligence in Mergers and Acquisitions," *Information Systems Control Journal*, 2006, vol. 6, *www.isaca.org/jonline*

[5] Baublits, T.; H-J. Lee; G. Stanis; B. Sundberg; Z-D. Tan; "Development of an IT Assessment Program for Acquisition," Final report of the student project in the IT Audit and Security Course, Red McCombs Business School, University of Texas at Austin, USA, 2005

[6] *Op cit*, Bhatia

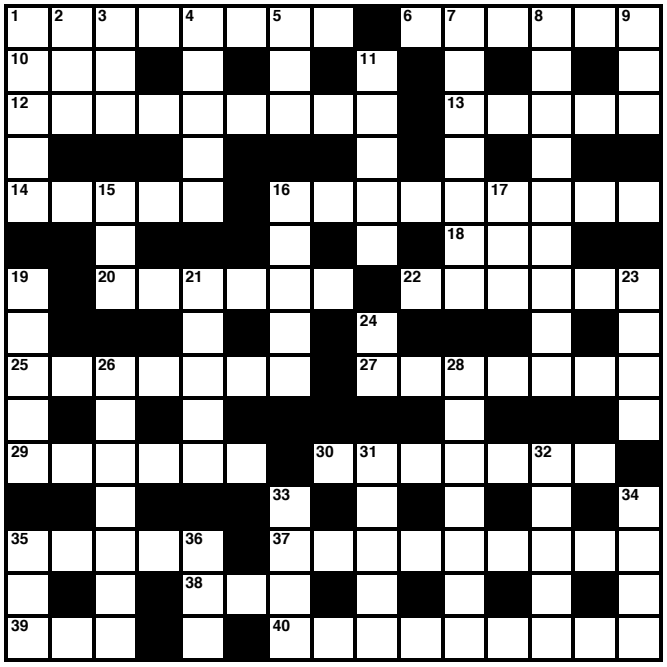
[7] *Op cit*, Bayuk

[8] Andriole, J. S.; "Mining for Digital Gold: Technology Due Diligence for CIOs," *Communication of the Association for Information Systems*, 2007, p. 371-381

[9] Andriole, S. J.; "Technology Due Diligence: Best Practices for Chief Information Officers, Venture Capitalists, and Technology Vendors," *Information Science Reference*, USA, 2008

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1 Make less severe, as in results of network penetration.
6 Immobilized, unable to act effectively
10 Expert
12 Language that should not be used outside of the IT group (2 words)
13 Irrational numbers
14 Excel components
16 Mutually beneficial
18 Fail, usually by misestimating a situation
20 See 1 down.
22 Pled one's case
25 Service offered to companies to test their security preparedness (goes with 26 down)
27 Vitally important
29 Security as a Service, abbr.
30 Short set of commands to correct a bug in a computer program, often related to security deficiencies
35 ISACA certification
37 Copy, as in backing up a system
38 Catch
39 Fix, in a dishonest way
40 Impermanent

DOWN

1 It provides an effective solution to a previously unsolvable problem. (goes with 20 across)
2 Make winning certain
3 Golfer's prop
4 Shocked responses
5 Link (to)
7 Exposing the organization to more danger
8 Model of security architecture that goes beyond perimeter protection and limits data access within a system (2 words)
9 Disapprovals
11 To deal with carelessly, not do a thorough job
15 Testing environment
16 User interface for access to an operating system's services
17 E-mail address ending
19 Powers
21 Makes a file or other piece of data inaccessible
23 Computer giant that started in a garage
24 Type of address, technically
26 See 25 across.
28 People or companies that have suffered from hacking attacks, e.g.
31 Early testing stage
32 Wipe out completely
33 Worry over
34 Conquer
35 Vehicle
36 Cybersecurity Nexus, abbr.

(Answers on page 58)

CPE Quiz

Prepared by Sally Chan,
CGEIT, ACIS, CMA

Take the quiz online:

Quiz #155

Based on Volume 2, 2014—The IS Audit Transformation

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

TRUE OR FALSE

ROSS ARTICLE

1. Organizations should employ an integrated solution to data and system availability in such a way that an organization's information portfolio is protected in a consolidated, consistent fashion, with no data element left behind.

2. The scope of Disaster Recovery as a Service (DRaaS) does not include testing of the recovery of all data and applications.

RAVAL ARTICLE

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

4. Soft volunteerism is sourced in mandatory volunteerism and is disingenuous communication that seeks to create the impression that one is volunteering when that really is not the case.

5. In searching for an appropriate threshold for consent in privacy, Ian Kerr and colleagues excluded the requirement of principal-agent relationship.

SINGLETON ARTICLE

6. Symantec's 2013 *Internet Security Threat Report* says that data breach is a fairly common occurrence among companies of all sizes. *PC World* says that 50 percent of all targeted malicious attacks in 2012 were aimed at entities with fewer than 2,500 employees, and the largest growth area was seen among entities with fewer than 250 employees (31 percent of all attacks).

7. Although it is impossible to prevent all data breach attacks, the courts have taken a stance on reasonable protection. The metric for that reasonableness is best practice in cybersecurity to protect against a data breach.

SUER, CULLENS AND BRANCATO ARTICLE

8. IT's primary goal is business services delivery.

9. IT leaders must recognize that they are in the IT business, not the business of their firm.

10. The request-to-fulfill value stream is concerned with the quality of the requirements process, the predictability of programs and projects, the end-to-end quality delivered, the change process, and the use and measurement of performance against service agreements.

11. The IT value chain viewpoint, which focuses on the data linkages across the service life cycle, complements the COBIT® viewpoint of governance and management.

COOKE ARTICLE

12. Commercial security tools available to audit Oracle databases are practical for consultancies performing external reviews as they are given permission to install or run tools that require full database administrator (DBA) privileges.

13. A username installed with the same password on different Oracle databases will have the same password hash. Default passwords pose a real and common risk to Oracle database installations.

OLAKUNIE ARTICLE

14. The US Securities and Exchange Commission CF Disclosure Guidance mandates that companies report the material risk associated with specific data breaches or other cyberincidents.

15. Third-party insurance risk exposure includes reputation loss and cyberextortion, whereas first-party insurance risk exposure is about the cost of legal damages, crisis service cost and fines.

16. The auditing of cyberinsurance policies can be divided into two major components: (1) condition precedent to the cyberinsurance policy and (2) condition concurrent with the cyberinsurance policy.

WHITE ARTICLE

17. The COSO 2013 framework now includes internal reporting (in addition to external) and nonfinancial reporting (in addition to financial) and the introduction and integration of control principles.

18. The 2013 framework defines an IC deficiency as a shortcoming in a component or embedded principle that reduces the likelihood of an organization achieving its objectives.

ISACA Journal
CPE Quiz
Based on Volume 2—The IS Audit Transformation

Quiz #155 Answer Form

(Please print or type)

Name _____

_____

Address_____

_____

_____

CISA, CISM, CGEIT or CRISC #_____

Quiz #155

True or False

ROSS ARTICLE

1. _____
2. _____

RAVAL ARTICLE

3. _____
4. _____
5. _____

SINGLETON ARTICLE

6. _____
7. _____

SUER, CULLENS AND BRANCATO ARTICLE

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

COOKE ARTICLE

12. _____
13. _____

OLAKUNIE ARTICLE

14. _____
15. _____
16. _____

WHITE ARTICLE

17. _____
18. _____

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

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

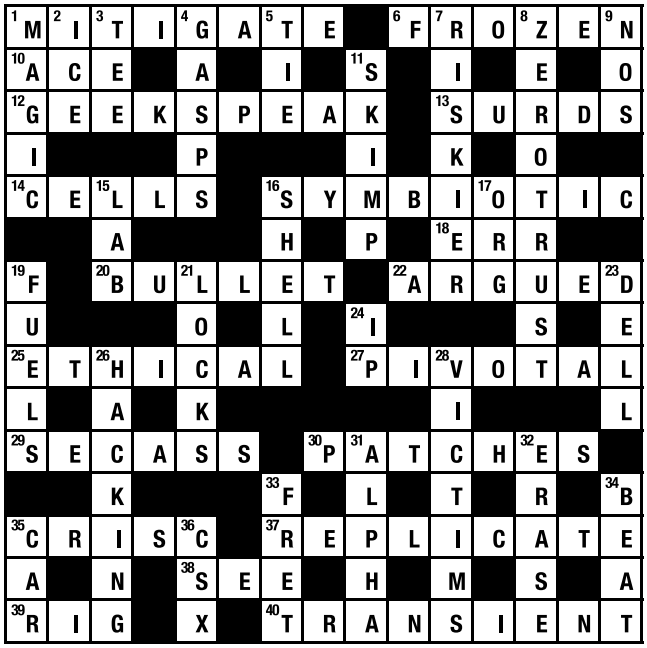
Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

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

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

Answers—Crossword by Myles Mellor

See page 56 for the puzzle.



ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

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

IS audit and assurance standards define mandatory requirements for IS auditing. They report and inform:

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

ITAF™, 3rd Edition (www.isaca.org/itaf) provides a framework for multiple levels of guidance:

- **IS Audit and Assurance Standards**
  - The standards are divided into three categories:
  - General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
  - Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care
  - Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated
- **IS Audit and Assurance**
  The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorisation as the standards (also divided into three categories):
  - General guidelines (2000 series)
  - Performance guidelines (2200 series)
  - Reporting guidelines (2400 series)
- **IS Audit and Assurance Tools and Techniques**
  - These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programmes, reference books, and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf*

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

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

IS Audit and Assurance Standards

The titles of issued standards documents are listed as follows:

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

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

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

Please note that the new guidelines are effective 1 September 2014.

General
2001 Audit Charter
2002 Organisational Independence
2003 Professional Independence
2004 Reasonable Expectation
2005 Due Professional Care
2006 Proficiency
2007 Assertions
2008 Criteria

Performance
2201 Engagement Planning
2202 Risk Assessment in Planning
2203 Performance and Supervision
2204 Materiality
2205 Evidence
2206 Using the Work of other Experts
2207 Irregularity and Illegal Acts
2208 Sampling

Reporting
2401 Reporting
2402 Follow-up Activities

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

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

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

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

Controls and Assurance in the Cloud: Using COBIT 5*

Complimentary eBook available to Members only.
Available in print – **CB5CA** and eBook **WCB5CA**
Member: $35.00 Nonmember: $60.00

Too Big to Ignore: The Business Case for Big Data

Available in print – **102WTB**
Member: $50.00 Nonmember: $60.00

Thomas On Data Breach: A Practical Guide to Handling Data Breach Notifications Worldwide, 2014 Ed.

Available in print – **1WPT**
Member: $199.00 Nonmember: $209.00

Networking A Beginner's Guide 6th Ed

Available in print – **37MCNB**
Member: $45.00 Nonmember: $55.00

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk

Available in print – **33MCIR**
Member: $60.00 Nonmember: $70.00

FEATURED BOOKS

Responding to Targeted Cyberattacks*

Complimentary eBook available to Members only.
Available in print – **RTC** and eBook **WRTC**
Member: $35.00 Nonmember: $59.00

COBIT 5 for Risk*

Available in print – **CB5RK** and eBook **WCB5RK**
Print – Member: $35.00 Nonmember: $80.00
eBook – Member: $35.00 Nonmember: $75.00

CGEIT Review Manual 2014*

Available in print only – **CGM14**
Member: $85.00 Nonmember: $115.00

Transforming Cybersecurity: Using COBIT 5*

Complimentary eBook available to Members only.
Available in print – **CB5TC** and eBook **WCB5TC**
Member : $35.00 Nonmember: $60.00

100 Things You should Know About Authorizations in SAP

Available in print – **3SAPP**
Member: $60.00 Nonmember: $70.00

Carry On: Sound Advice from Schneier on Security

Available in print – **103WCO**
Member: $30.00 Nonmember: $40.00

* 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

New/Featured Books

NEW BOOKS

Controls and Assurance in the Cloud: Using COBIT 5

by ISACA

This book provides practical guidance for enterprises using or considering using cloud computing. It identifies related risk and controls, and provides a governance and control framework based on COBIT 5, and an audit program using *COBIT 5 for Assurance*. This information can assist enterprises in assessing the risk and potential value of cloud investments and determine whether the risk is within the acceptable level. In addition, it provides a list of available publications and resources that can help determine if cloud computing is the appropriate solution for data and processes in scope.
2014, 266 pages

Complimentary eBook available to Members only.
Available in print – **CB5CA** and eBook **WCB5CA**
Member: $35.00 Nonmember: $60.00

Too Big to Ignore: The Business Case for Big Data

by Phil Simon

It's time to start thinking big. In *Too Big to Ignore*, recognized technology expert and award-winning author Phi Simon explores an unassailably important trend: Big Data, the massive amounts, new types, and multifaceted sources of information streaming at us faster than ever. Never before have we seen data with the volume, velocity, and variety of today. Big Data is no temporary blip of fad. In fact, it is only going to intensify in the coming years, and its ramifications for the future of business are impossible to overstate. Too Big to Ignore explains why Big Data is a big deal.
2013, 256 pages

Available in print – **102WTB**
Member: $50.00 Nonmember: $60.00

Thomas On Data Breach: A Practical Guide to Handling Data Breach Notifications Worldwide, 2014 Ed.

by Liisa Thomas

The book will help you understand breach notification requirements so you can have a clear plan in place before the breach occurs.

As the nation—and the world - debate issues about data breach laws, this guide gives you a comprehensive overview of where we are right now, and how to best prepare for the future. It will also aid you in assessing specific data breach questions, such as What are our legal obligations? Do we have to notify under various data breach notification laws? Whom do we notify? How quickly? What should be included in the notice? What is our potential exposure after the notice goes out? And finally Did we do all that we could have to prevent the attack?

Available in print – **1WPT**
Member: $199.00 Nonmember: $209.00

Networking A Beginner's Guide 6th Ed

by Bruce Hallberg

Current, essential IT networking skills--made easy!

Thoroughly revised to cover the latest technologies, this practical resource provides you with a solid foundation in networking fundamentals. *Networking: A Beginner's Guide, Sixth Edition* discusses wired and wireless network design, configuration, hardware, protocols, security, backup, recovery, and virtualization. You'll also get step-by-step instructions for installing, configuring, and managing Windows Server 2012, Exchange Server 2013, Oracle Linux, and Apache. This is the perfect book for anyone starting a networking career or in need of an easy-to-follow refresher.
2013, 416 pages

Available in print – **37MCNB**
Member: $45.00 Nonmember: $55.00

New/Featured Books

NEW BOOKS

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk

by N.K. McCarthy, Matthew Todd, Jeff Klaben

Reinforce your organization's security posture using the expert information contained in this tactical guide. *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk* shows you how to build and manage successful response plans for the cyber incidents that have become inevitable for organizations of any size. Find out why these plans work. Learn the step-by-step process for developing and managing plans built to address the wide range of issues organizations face in times of crisis. July 2012, 240 pages

Available in print – **33MCIR**
Member: $60.00 Nonmember: $70.00

Responding to Targeted Cyberattacks

by ISACA

A Breach WILL Eventually Occur!
Is your enterprise prepared? The threat environment had radically changed over the last decade. Most enterprises have not kept pace and lack the necessary fundamentals required to prepare and plan against cyberattacks.

To successfully expel attackers, the enterprise must be able to:

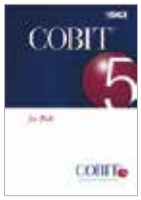
- Conduct an investigation
- Feed threat intelligence into a detailed remediation/eradication plan
- Execute the remediation/eradication plan

This publication covers a few of the basic concepts that will help answer the key questions posed by a new outlook that a breach WILL eventually occur. 2013, 90 pages

Complimentary eBook available to Members only.
Available in print – **RTC** and eBook **WRTC**
Member: $35.00 Nonmember: $59.00

FEATURED BOOKS

COBIT 5 for Risk



by ISACA

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

Available in print – **CB5RK** and eBook **WCB5RK**
Print – Member: $35.00 Nonmember: $80.00
eBook – Member: $35.00 Nonmember: $75.00

CGEIT Review Manual 2014

by ISACA

The *CGEIT Review Manual 2014* is designed to help individuals prepare for the CGEIT exam and understand the responsibilities of those who implement or manage the governance of enterprise IT (GEIT) or have significant advisory or assurance responsibilities in regards to GEIT. It is a detailed reference guide that has been developed and reviewed by subject matter experts actively involved in governance of enterprise IT worldwide. 2013, 182 pages

Available in print – **CGM14**
Member: $85.00 Nonmember: $115.00

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

New/Featured Books

FEATURED BOOKS

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. 2013, 190 pages

Complimentary eBook available to Members only.
Available in print – **CB5TC** and eBook **WCB5TC**

Member : $35.00 Nonmember: $60.00

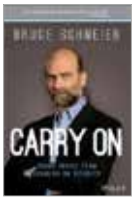
100 Things You should Know About Authorizations in SAP

by Massimo Manara and Andrea Cavarelli

Work smarter with authorizations! Have you ever had an unauthorized user access something in your system that you could have sworn was off limits? Here you go: SAP PRESS equips you with "100 Things" that unlock the secrets of managing your security and authorizations in SAP.
The tips are grouped together based on the area of authorizations they cover, such as development security, Profile Generator, upgrades, and more. They have been carefully selected to provide a collection of the best, most useful, and rarest information. An invaluable resource to support you in your SAP administration duties!
2012, 346 pages

Available in print – **3SAPP**
Member: $60.00 Nonmember: $70.00

Carry On: Sound Advice from Schneier on Security



by Bruce Schneier

Up-to-the-minute observations from a world-famous security expert

Bruce Schneier is known worldwide as the foremost authority and commentator on every security issue from cyber-terrorism to airport surveillance. This groundbreaking book features more than 160 commentaries on recent events including the Boston Marathon bombing, the NSA's ubiquitous surveillance programs, Chinese cyber-attacks, the privacy of cloud computing, and how to hack the Papal election. Timely as an Internet news report and always insightful, Schneier explains, debunks, and draws lessons from current events that are valuable for security experts and ordinary citizens alike. 2013,384 pages

Available in print – **103WCO**
Member: $30.00 Nonmember: $40.00

The future of technology is more secure than ever.

Intel® Security combines the expertise of McAfee® with the performance and trust of Intel to deliver secure computing to consumers and businesses worldwide. We believe that as technology becomes more deeply integrated into life, security must be more deeply integrated into technology. Because when everyone has the confidence to use technology to its full potential they can achieve their full potential. Visit intelsecurity.com. McAfee is now part of Intel Security.

KEEP YOUR CAREER ON TRACK

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

INFORMATION ASSURANCE PROGRAMS

GRADUATE CERTIFICATE

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

MASTER'S DEGREE

- Two year program
- Specialize in cyber security or policy management

The curriculum is modeled on the guidelines and recommendations provided by:

- The Committee on National Security Systems (CNSS) 4000 training standards
- The $(ISC)^2$ Ten Domains of Knowledge
- ISACA

Classes can be taken on campus or completely online.

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

COMMITTEE ON NATIONAL SECURITY SYSTEMS
CNSS
SYSTEMS SECURITY FOR THE 21st CENTURY

BEST COLLEGES
U.S.News & WORLD REPORT
REGIONAL UNIVERSITIES WEST
2014

REGIS UNIVERSITY
School of Computer & Information Sciences

LEARN MORE

www.informationassurance.regis.edu/ISACA
877.820.0581