VOLUME 4, 2018

ISACA Journal

ECONOMICS OF TECHNOLOGY

THE POWER OF IT INVESTMENT RISK QUANTIFICATION AND VISUALIZATION

INTEGRATING KRIs AND KPIs FOR EFFECTIVE TECHNOLOGY RISK MANAGEMENT

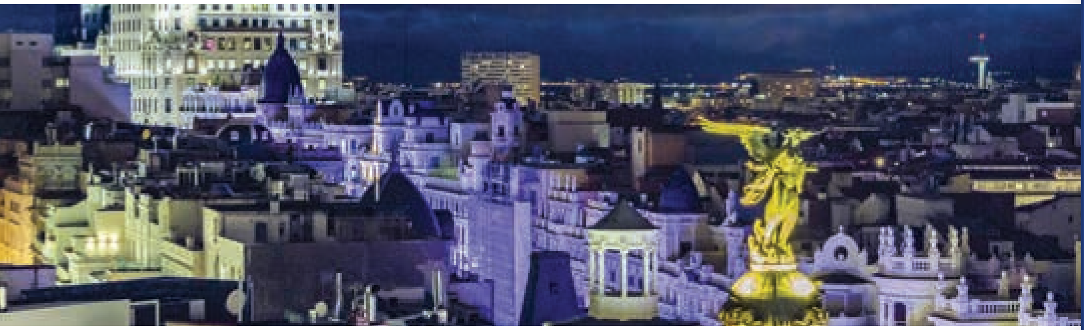
THE PROMISES AND JEOPARDIES OF BLOCKCHAIN TECHNOLOGY

ISACA.ORG

2018 International Basic Compliance & Ethics ACADEMIES

FROM THE SOCIETY OF CORPORATE COMPLIANCE & ETHICS®

24-27 SEPTEMBER
MADRID, SPAIN



The Society of Corporate Compliance and Ethics International Basic Compliance & Ethics Academies® provide three and a half days of classroom-style training in the fundamentals of compliance and ethics management. Learn everything from understanding risk, and setting policies, to training and investigations.

Topics addressed at an academy include:

- Standards, policies, and procedures
- Compliance and ethics program administration
- Communications, education, and training
- Monitoring, auditing, and internal reporting systems
- Response and investigation, discipline and incentives
- Anti-Corruption and Bribery
- Trade Sanctions
- Risk assessment

corporatecompliance.org/academies

Questions: lizza.catalano@corporatecompliance.org

INTERNATIONAL ACADEMIES
OFFERED IN 2018

SÃO PAULO, BRAZIL
20–23 AUGUST

RIO DE JANEIRO, BRAZIL
26–29 NOVEMBER

10,900+ COMPLIANCE PROFESSIONALS HOLD A COMPLIANCE CERTIFICATION BOARD (CCB)® CREDENTIAL

REGISTER EARLY TO RESERVE YOUR SPACE

ACADEMIES ARE LIMITED TO 75 PARTICIPANTS

SCCE™
Society of Corporate Compliance and Ethics

ISACA Journal

FEATURES

PLUS

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

Read more from these *Journal* authors...

Journal authors are now blogging at *www.isaca.org/journal/blog*. Visit the *ISACA Journal* blog, Practically Speaking, to gain practical knowledge from colleagues and to participate in the growing ISACA® community.

Online-Exclusive Features

Do not miss out on the *Journal*'s online-exclusive content. With new content weekly through feature articles and blogs, the *Journal* is more than a static print publication. Use your unique member login credentials to access these articles at *www.isaca.org/journal*.

Online Features
The following is a sample of the upcoming features planned for July and August 2018.

The Downstream Effects of Cyberextortion
Tony Martin-Vegue, CISM, CISSP

Data Spill Lessons From the Oil Industry
Sridhar Govardhan, CISA, CISM, SABSA

Addressing the Challenges in IT Audits by Supreme Audit Institutions
Shourjo Chatterjee, CIA

Discuss topics in the ISACA® Knowledge Center: *www.isaca.org/knowledgecenter*
Follow ISACA on Twitter: *http://twitter.com/isacanews*; Hashtag: #ISACA
Follow ISACA on LinkedIn: *www.linkedin.com/company/isaca*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISACA®

1700 E. Golf Road,
Suite 400
Schaumburg, Illinois
60173 USA
Telephone +1.847.660.5505
Fax +1.847.253.1755
www.isaca.org

I Left My Security in the Office

For many people, information technology has changed the very meaning of work. The classic locus of work is the office, a place where people gathered to perform a variety of tasks with a common purpose. Office workers saw their colleagues more than they saw their spouses; they dressed well; they came and went at relatively regular times so they could catch their trains or avoid the traffic.

Mobile Work

Now I, and many people like me, do not *go* to work. We have laptop computers, cell phones, a printer and Internet connectivity at our homes. Our “office” is where we live. We are in touch with many of our colleagues on a daily basis, but see them only rarely. We are mobile workers, able to do our jobs anywhere as long as we have the technical tools of our trade.

I submit that changing the definition of work necessitates a corresponding redefinition of security over the information with which we work.

I can hear a serious objection to my premise here: Many people do not work in an office, but in a factory, a hospital, a laboratory, a store. Their work is tied to a place and they cannot work anywhere else. True, no one can make steel at home. Among the many manifestations of the changes technology has wrought is that we have created two classes of workers: information workers, whose world is broad, without boundaries or clocks, and place-bound workers who are far more limited in their freedom of movement or in alternatives for getting through disruptions such as heavy snowfalls. This bifurcation has already had major economic, social and political consequences that I will not go into here. This is, after all, the *ISACA® Journal*, not *The New Republic*. Here I will address just the implications for information security.

Physical Security

One of the tenets of information security has been the physical protection of data centers, defined as “where data are.” The prevention of unauthorized physical access, damage and interference to the organization’s information and information processing facilities is one of the key objectives stated in ISO 27002.[1] However, with worker mobility, even if data reside in a room with limited access and other preventive controls, they are accessible everywhere. This raises the stakes for the physical security of information resources; a data center cannot be stolen, but a laptop computer certainly can be.

Consider just a few of the headings in the relevant chapter of ISO/IEC 27002:

- Physical security *perimeter*
- Physical *entry* controls
- Securing *offices, rooms and facilities*
- Protecting against *external* and environmental threats
- Working in secure *areas*[2]

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2Jdm75x

Steven J. Ross, CISA, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal’s* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

The entire reference for physical security is place. Keeping in mind that the ISO/IEC 27002 standard, definitive in the information security field, was published in 2013, we can see how rapidly the environment in which information is used has changed.[3] I would rest easier if hard-drive encryption and two-factor authentication were universally implemented, but that is not the case. Perhaps a later version of the standard will recognize that data are not where the servers are, but where the users are.

Data Leakage Prevention

Not that long ago, somebody[4] wrote:

> *There is no single answer to the problem of data leakage.... [I]f personnel are issued laptop computers and virtual private network (VPN) access capabilities, it may be assumed that they are expected to be mobile, work remotely and take their data with them. So at what point are data considered to be leaked? Are they leaked when they leave an organization's premises?*

The statement is still relevant, but with more immediacy today. For many information workers, issuance of laptop computers with VPN capabilities need not be preceded with "if." The conditional has become assumptive. Information is not "leaked" when a worker is off-premises. The person may rarely, if ever, work *on*-premises. If the frontier between contained and leaked is not the office building, is it the organization-issued personal computer? What then of that person's smartphone or the flash drive on which he or she stores backups?

There is an implicit, but unwarranted, expectation that an authorized user will not betray the trust placed in him or her, either intentionally or inadvertently. Even if that were a reliable control, what meaning does trust have in an era in which data sharing is promoted as an ideal? The boundaries of trust must be encoded in policy that, it is hoped, will lead to behavior. Maybe so, if the definition of "trust" is clear. Clarity of the policy will (or, perhaps, may) motivate staff to follow the rules.[5] But trust parameters are a weak substitute for secure perimeters.

Business Continuity Management

The effect of workers' mobility on business continuity management is so extreme that the plans written even a few years ago may no longer make sense. Most business continuity plans written in the past 25 years have consisted of a search for and transition to designated alternate workplaces. Hence, there is a commercial industry of office space for contingent use (aka hot sites) and many organizations maintain empty, but well-equipped, office space, just in case.

"THE EFFECT OF WORKERS' MOBILITY ON BUSINESS CONTINUITY MANAGEMENT IS SO EXTREME THAT THE PLANS WRITTEN EVEN A FEW YEARS AGO MAY NO LONGER MAKE SENSE."

These provisions make little sense when the extent of a business interruption is the length of time it takes workers to get home—or even less time if people work at their homes on a routine basis. For those few transactions for which minutes are of the essence, coffee shops beckon. If an organization has migrated its data center away—far away—from the building where its work is done, then having workers toil at home is possibly a benefit—at worst, an inconvenience—and not a disaster at all.

Data Center Recovery

The same consideration, but in reverse, applies to data center recovery planning.[6] The ability for people to work remotely is entirely dependent on the availability of information systems centrally. Information workers enter data into systems, manipulate the data and use them for various purposes. That is their job. So, no systems, no jobs, neither in the office nor at home. Increasingly, IT managers recognize this and maintain two or more data centers sufficiently far from each other so that the same event cannot incapacitate both.

There is another, perhaps deeper, implication of the technical enablement of worker mobility (and here I may stray into sociology after all). It is hardly an original observation that information technology is changing society, its cultures and mores, and is doing so at a dizzying and dislocating pace. For this discussion, it has changed the nature of work, of the office, of colleagues and of management. Why should information security be immune from the forces technology has unleashed in our workaday lives? We have to embrace these societal changes because there is no other alternative. We security professionals need only remember how different things were a decade ago to get some idea of how different they will be five years hence.

Endnotes

[1] International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 27002:2013 *Information technology—Security techniques—Code of practice for information security controls*, p. 30, *https://www.iso.org/standard/54533.html*

[2] *Ibid*., p. 31-33, author's italicization

[3] Yes, "Security of equipment and assets off-premises" is addressed, deep in the chapter and almost as an afterthought. The "premises," evidently, are where the data center resides.

[4] Oh, right, that was me in 2009. Ross, S.; "Data Plumbing?" *ISACA® Journal*, vol. 6, 2009.

[5] *Ibid*.

[6] Aka IT disaster recovery planning

SEE WHAT'S NEXT, NOW
EARN ADDITIONAL CONTINUING PROFESSIONAL EDUCATION (CPE) HOURS ON YOUR SCHEDULE
CPE ON DEMAND
www.isaca.org/OnDemand-jv4
ISACA®

Building Tomorrow's Leaders, Today

Rob Clyde, CISM

Is chair of ISACA's board of directors, executive chair of the board of directors for White Cloud Security (trusted app list enforcement), and independent board director for Titus (leader in data protection, categorization and classification). He is the managing director of Clyde Consulting LLC, which provides board and executive advisory services to cybersecurity software companies. He serves as an executive advisor to HyTrust (multicloud workload security) and BullGuard Software (consumer and smart home cybersecurity). Prior to becoming chair of ISACA's Board of Directors, he served as vice-chair, chaired the board-level ISACA Finance Committee, and served as a member of ISACA's Strategic Advisory Council, Conference and Education Board and the IT Governance Institute (ITGI) Advisory Panel. Previously, he was chief executive officer of Adaptive Computing, which provides workload management software for some of the world's largest cloud, high-performance computing and big data environments. Prior to founding Clyde Consulting, he was chief technology officer at Symantec and a cofounder of Axent Technologies. Clyde is a frequent speaker at ISACA events, cybersecurity conferences and for the US National Association of Corporate Directors (NACD). He is an NACD Board Leadership Fellow. He also serves on the industry advisory council for the Management Information Systems (MIS) Department of Utah State University (USA).

Q: You have served and currently serve on a number of organization boards and as an executive advisor to some cybersecurity companies. What in your past experience has best prepared you for the role of ISACA board chair?

A: Currently, I work with several different organizations as an executive advisor to the chief executive officer (CEO) or as a board director. As a board director, I carry out the fiduciary, governance and strategic leadership responsibilities that are inherent in that role. I consider myself a team member of each of my clients. I work closely with the CEO, board directors, other executives and staff. In the case of ISACA, I provide a similar service as a board director and chair, but *pro bono*.

I really enjoy this because I have the privilege of simultaneously being on the teams of several great organizations and the satisfaction of making a significant difference to their success. My executive advice may cover any area of the business, including governance, strategy, organization positioning and messaging, product strategy, product road maps, improving development velocity and quality, mentoring leaders, helping to identify inventions and file patents, sales, support, professional services, organization structure, and mergers and acquisitions.

A long list of experiences has prepared me for this role. Here are a few highlights: initially built my technical skills as a programmer writing information security products, since led development and product teams, led business units, served as the chief technology officer (CTO) for Symantec, and as a CEO. Through ISACA I was able to hone my cybersecurity skills and better understand audit and risk functions by attending and speaking at ISACA events at both the international and chapter level.

What may be less obvious are the failures and adversity I faced that helped build character and understanding. For instance, early in my career, one of my software products crashed all of the systems for a well-known sports league during a proof of concept and I was kicked out of the building and asked to never return. I did not give up and continued trying to improve the product.

Later, out of that company, I cofounded Axent Technologies, which focused on enterprise information security. It grew exponentially and was ultimately taken public and purchased by Symantec. During this time, my wife was struggling with cancer and eventually passed away before we sold the company. While her illness and passing were incredibly traumatic for me and my children, learning how to deal with adversity and loss gave me more empathy for others and an ability to focus on what is truly important and not sweat the little stuff.

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

A: Ransomware attacks continue to increase rapidly. In 2018, we are seeing more targeted ransomware attacks with higher ransom demands. Not just Windows systems are being targeted, but also Linux systems, Mac systems, smartphones and IoT devices.

To deal more effectively with this risk, organizations should consider bolstering their current approach by adding next-generation white-listing tools that allow only trusted code to run. Organizations can choose how tightly to lock down that list.

Privacy also remains at risk, as made evident by the GDPR, which describes many beneficial actions such as discovering, categorizing and encrypting personal data.

Lack of sufficient cybersecurity practitioners poses a risk that organizations may not be able to execute well on their security strategies and effectively detect and respond to incidents. Dealing with the cyberskills gap is a challenge that leaders must navigate.

Q: You have extensive experience in executive leadership. How do you see the role of executives changing to meet the challenges of information security?

A: Meeting the challenges of cybersecurity will require strong leadership including from the board, the CEO and the C-suite. In fact, organizations do not just need cybersecurity, they need cyberresilience, which includes the need for security, but also high availability, scalability, and the ability to allow an organization to keep running in the face of attack or disaster.

The role of executives relative to this is changing as organizations view cybersecurity and resilience as not just issues to be delegated to chief information officers (CIOs) and chief information security officers (CISOs), but as fundamental to the health and growth of the business. The CEO must provide leadership and make cyberresilience, including security, something that is planned, tracked and regularly discussed at executive meetings and at the board level.

Q: What do you think are the most effective ways to address the cybersecurity skills gap?

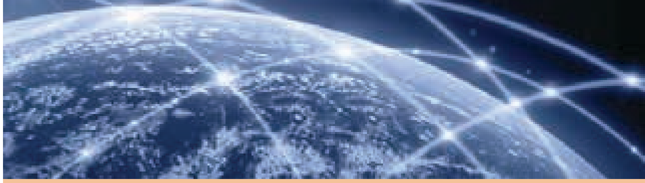
A: Today, most organizations try to hire talent from other organizations. This is difficult and there are not enough cybersecurity professionals available to fill all open positions. To deal with this in the near term, organizations should consider cross-training existing employees or new hires in adjacent areas such as network or systems administration. This can include having them train for and pass appropriate certifications to demonstrate their knowledge and skill. Organizations should drop requirements for a four-year college degree and consider applicants who have been trained at technical schools, in the military or have otherwise demonstrated aptitude. They can use intern programs as a way to mentor and encourage future candidates to gain experience in the field.

In the longer term, we need to work with students from the moment they enter secondary school and at the technical school, college and university levels to encourage more students to go into technical fields such as cybersecurity. We also need to encourage and support more women entering the field. Today, women make up only about 11 percent of the cybersecurity workforce (according to the Executive Women's Forum). I am an enthusiastic supporter of ISACA's SheLeadsTech program as a way to do this. In addition, ISACA's State of Cybersecurity 2018 Report clearly showed that having a diversity program dramatically closes the perception gap between women and men as to equal advancement opportunities in the cybersecurity field.

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

A. I started my work in programming and cybersecurity before certifications ever existed. So, by the time certifications appeared on the scene, I was fortunate enough to be well established in the field. Nevertheless, I was one of the very first to receive ISACA's Certified Information Security Manager® (CISM®) certification and have been vigilant to continue my education and keep it current. It is important to me to continually learn and the goal of earning continuing professional education hours (CPEs) to maintain a certification helps me to do that.

The Certified Information Systems Auditor® (CISA®) certification has become a requirement for most IT audit positions. I also think that performance-based certifications such as ISACA's CSX Practitioner (CSXP) are the way of the future for cybersecurity since employers are looking for candidates who can demonstrate hands-on experience.



1 **What is your favorite blog/online content?**
ISACA's *The Nexus* (of course).

2 **What is on your desk right now?**
Nothing, except my notebook and iPad. I believe in being entirely paperless and do everything electronically. I am encouraging ISACA and its members to go paperless as well. I travel frequently and, since my office contents are electronic, I take my desk with me wherever I go.

3 **What are your goals for 2018?**

- Make ISACA even more relevant and valuable to our members, profession, industry and enterprises, including continuing to innovate with our training, certifications, the CSX platform and new CMMI Cybermaturity Platform.
- Provide strong board leadership demonstrated by great governance, execution oversight and strategic plans.
- Develop and execute on a plan for an ISACA charitable foundation.
- Listen, learn and act.

4 **What is your number-one piece of advice for technology professionals?**
Participate. Volunteer—starting with your ISACA chapter and then at the international level. Look for opportunities to contribute. When you do this, you will grow much faster as a professional, gain valuable skills and insights, build your network, and feel like you are making a difference.

5 **What's your favorite benefit of your ISACA membership?**
Networking. I thoroughly enjoy interacting with ISACA members at various events and chapters all over the world. ISACA is more than just a professional association, it is a global family.

6 **What do you do when you are not at work?**
After losing my first wife, I married a wonderful woman, Becky. We just celebrated our 19th anniversary and together have six children and 17 grandchildren. So, my favorite thing to do is spend time with my wife, children and grandchildren. This often includes boating, fishing and swimming, which we love to do.

Add Value to What Is Valued

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (*www.isaca.org/journal*), find the article and click on the Comments link to share your thoughts.

https://bit.ly/2kRkc8g

I was raised by my mother, a single parent, in relative poverty. This meant that she would sometimes come home with a new shirt or a pair of jeans for me and declare what great value they were! I must admit, at the time I could not see the value. My only thought was that I had to go outside onto the mean streets of the north side of Dublin, Ireland, in those clothes! The point of this anecdote? To demonstrate that value means different things to different people, depending on their perspective.

This is also true in business. Enterprises have many stakeholders, and "creating value" means different—and sometimes conflicting—things to each of them.[1] Bearing this in mind, how can we leverage IT audit to create value?

Defining Value

Internal audit does not define value for the enterprise. That is a function of governance. The governance system should consider all stakeholders when making benefit, risk and resource assessment decisions. For each decision, the following questions can and should be asked: For whom are the benefits? Who bears the risk? What resources are required?[2] In other words, value creation means realizing benefits at an optimal resource cost while optimizing risk (**figure 1**).[3]

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA committees and is a current member of ISACA's CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke supported the update of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for ISACA's CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.

The Goals Cascade

Stakeholder needs can be related to enterprise goals by using, for example, the balanced scorecard (BSC).[4] These, in turn, are cascaded to IT-related goals using the IT balanced scorecard (IT BSC). Finally, IT-related goals are cascaded to enabler goals (**figure 2**).[5] Enablers are factors that, individually and collectively, influence whether something will work.[6]

If enablers influence whether something will work, and this can be traced back to stakeholder needs, then it follows that auditing these enablers to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met[7] will add value.

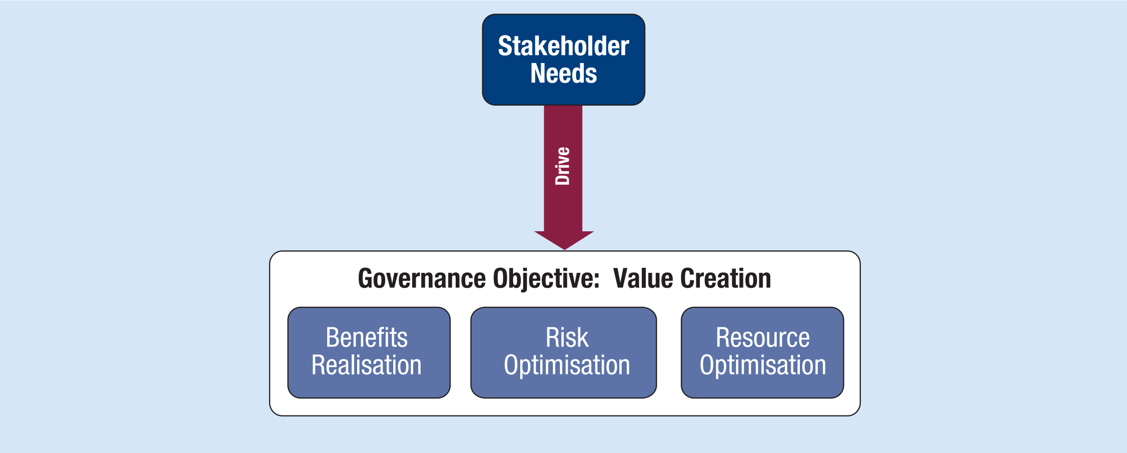
There is, of course, a potential problem here: What if one's enterprise has not adopted COBIT® 5? What if (quite likely) there is no goals cascade? The good news is that there is a solution—one can work in reverse. If the enterprise's IT processes are mapped to the COBIT 5 process reference model,[8] the resulting COBIT 5 processes can be used to determine the IT-related goals.[9] These, in turn, can be used to determine the enterprise goals.[10] For example, business continuity would map to COBIT process Deliver, Service and Support (DSS) DSS04 *Manage continuity*. This maps to IT goal ITG07 *Delivery of service in line with business requirements*, that, in turn, maps to enterprise goal EG07 *Business service continuity and availability*. Note that this will result in generic IT and enterprise goals that can and should be adjusted by senior business and IT managers. The enterprise should then decide which of these adds the most value.

Enablers

The COBIT 5 framework describes seven categories of enablers (**figure 3**):[11]

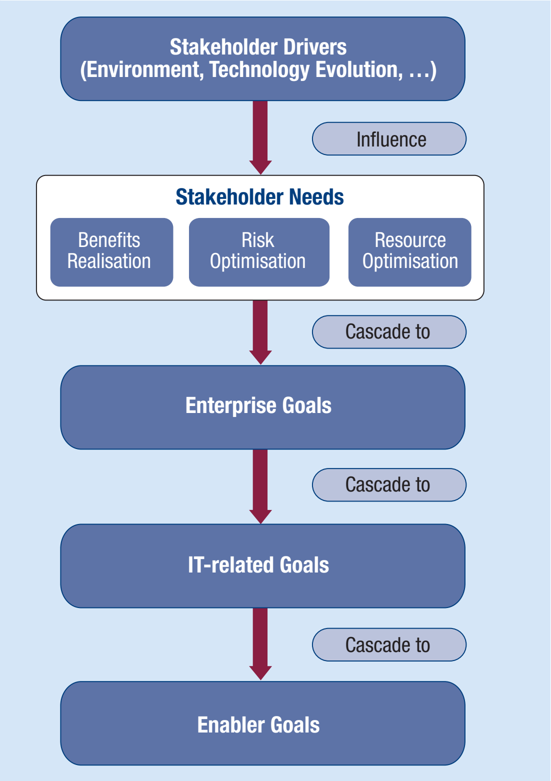
- Principles, Policies and Frameworks are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- Processes describe an organized set of practices and activities to achieve certain objectives and

Figure 1—The Governance Objective: Value Creation



Source: ISACA, COBIT® 5, USA, 2012. Reprinted with permission.

Figure 2—COBIT 5 Goals Cascade



Source: ISACA, *COBIT® 5 for Assurance*, USA, 2013. Reprinted with permission.

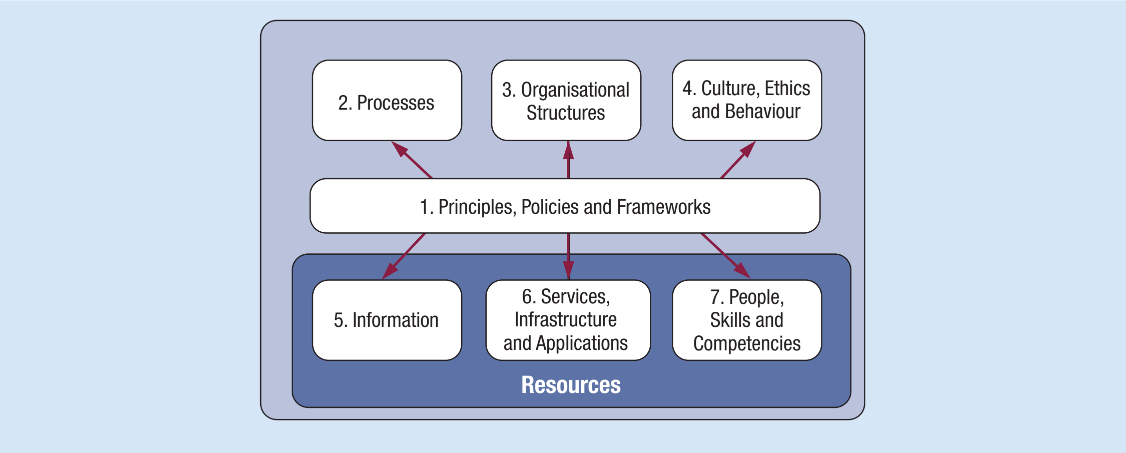
produce a set of outputs in support of achieving overall IT-related goals.

- Organizational Structures are the key decision-making entities in an enterprise.
- Culture, Ethics and Behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
- Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- Services, Infrastructure and Applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- People, Skills and Competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

Auditing the Enablers

At this stage, those who have read previous IS Audit Basics columns[12, 13, 14] are likely expecting the introduction of the ISACA® white paper on creating audit programs[15] and, indeed, this would work. However, in my opinion, the audit approach suggested in the white paper is best suited to enabler six, that is, auditing a discrete piece of infrastructure or technology or an individual application. This is because the approach is purely risk-based, which typically results in the audit objective being described in a control context. For example, in the paper on creating audit programs, the example given for an audit objective is "to determine whether program

Figure 3—COBIT 5 Enterprise Enablers


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

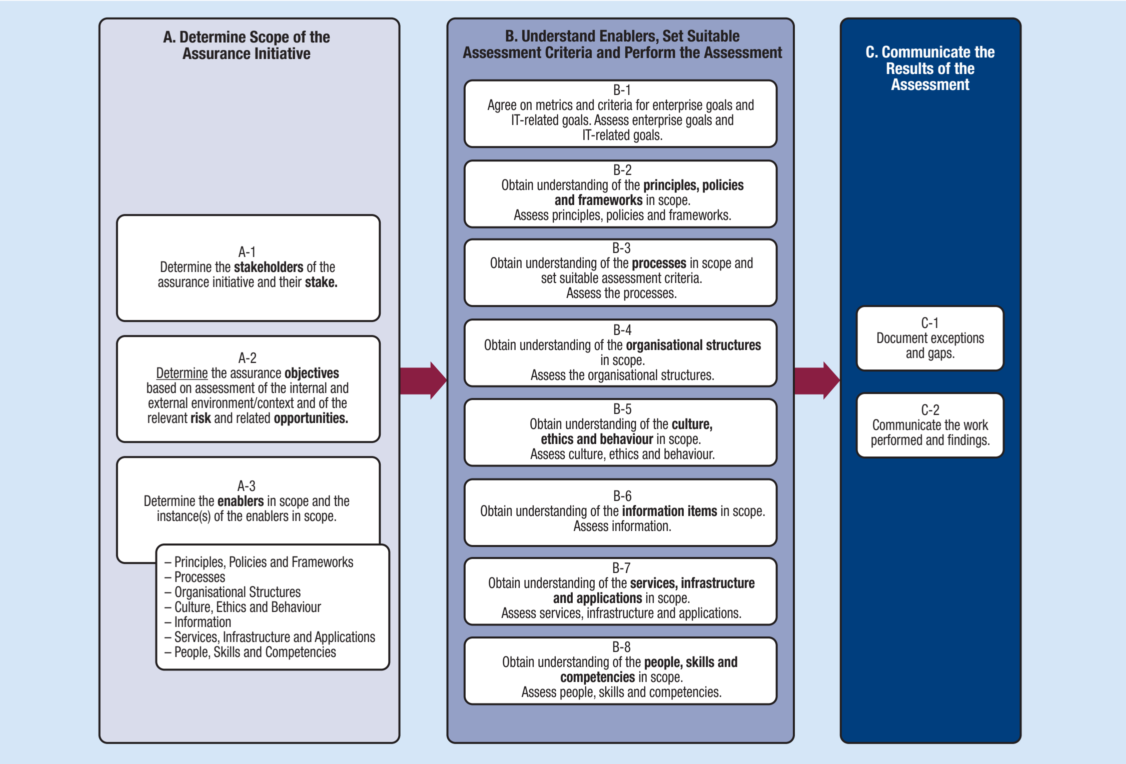
Source: ISACA, *COBIT® 5 for Assurance*, USA, 2013. Reprinted with permission.

source code changes occur in a well-defined and controlled environment."[16]

To meet all stakeholder needs, the assurance engagement should consider all three value objective components: delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.[17] To meet these objectives, I recommend the adoption of the generic COBIT 5-based assurance engagement approach (**figure 4**).[18]

This approach is aligned with generally accepted auditing standards and practices, including the

Figure 4—Generic COBIT 5-Based Assurance Engagement Approach


A. Determine Scope of the Assurance Initiative
A-1 Determine the stakeholders of the assurance initiative and their stake.
A-2 Determine the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities.
A-3 Determine the enablers in scope and the instance(s) of the enablers in scope.
– Principles, Policies and Frameworks
– Processes
– Organisational Structures
– Culture, Ethics and Behaviour
– Information
– Services, Infrastructure and Applications
– People, Skills and Competencies
B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment
B-1 Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.
B-2 Obtain understanding of the principles, policies and frameworks in scope. Assess principles, policies and frameworks.
B-3 Obtain understanding of the processes in scope and set suitable assessment criteria. Assess the processes.
B-4 Obtain understanding of the organisational structures in scope. Assess the organisational structures.
B-5 Obtain understanding of the culture, ethics and behaviour in scope. Assess culture, ethics and behaviour.
B-6 Obtain understanding of the information items in scope. Assess information.
B-7 Obtain understanding of the services, infrastructure and applications in scope. Assess services, infrastructure and applications.
B-8 Obtain understanding of the people, skills and competencies in scope. Assess people, skills and competencies.
C. Communicate the Results of the Assessment
C-1 Document exceptions and gaps.
C-2 Communicate the work performed and findings.

Source: ISACA, *COBIT® 5 for Assurance*, USA, 2013. Reprinted with permission.

phases defined in the creating audit programs document, specifically:[19]

- **Phase A**—Planning and scoping the assurance engagement (planning)
- **Phase B**—Understanding the subject matter, setting suitable assessment criteria and performing the actual assessment (fieldwork/ documentation)
- **Phase C**—Communicating the results of the assessment (reporting/follow-up)

Furthermore, it references the COBIT 5 goals cascade to ensure that detailed objectives of the assurance engagement can be put into the enterprise and IT context, and, concurrently, it enables linkage of the assurance objectives to enterprise and IT risk and benefits.[20]

In addition to this process being described in detail in *COBIT® 5 for Assurance*,[21] ISACA has used the approach to develop audit/assurance programs for 34 of the 37 COBIT 5 processes.[22] Where these are used to audit horizontally[23]—that is, the same process across several different applications—the assurance engagements can not only create, but also demonstrate the link to enterprise value.

Conclusion

In May 2016, Dublin had the honor of hosting EuroCACS.[24] I met some ISACA colleagues in a social setting (incidentally, I was wearing a new shirt and jeans bought especially for the occasion!) prior to the evening reception. The conversation turned to COBIT and a comment was made about how COBIT® 4.1 was "better" than COBIT 5 as it could just be "picked up and used." I had completed COBIT 5 Foundation[25] training at the end of 2015 and so felt comfortable enough to answer.

COBIT 5, as opposed to COBIT 4.1, addresses all stakeholders' needs: benefits realization, risk optimization and resource optimization. By following the goals cascade or, where this is not in place, mapping upward to generic goals, enablers that truly add value to the enterprise, including processes, can be added to the audit universe. The approach also ensures that the objectives and results of the assurance engagement can be put into an enterprise and IT context. This, ultimately, allows audit to add value to what is valued.

Endnotes

1 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/pages/default.aspx*
2 *Ibid*., p.17
3 *Ibid*.
4 Kaplan, R. S.; D. P. Norton; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard University Press, USA, 1996
5 *Op cit* COBIT 5, p. 17. The goals cascade is covered in greater detail in COBIT 5.
6 *Ibid*., p. 27
7 ISACA Glossary, Audit, *www.isaca.org/Glossary*
8 *Op cit* COBIT 5, figure 16, p. 33
9 ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, figure 18, p. 227-229, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*. Map between the IT processes and IT-related goals.
10 *Ibid*., figure 17, p. 226. Map between the IT-related goals and enterprise goals.
11 *Op cit* COBIT 5, p. 27
12 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *www.isaca.org/archives*
13 Cooke, I.; "Auditing Mobile Devices," *ISACA Journal*, vol. 6, 2017, *www.isaca.org/archives*
14 Cooke, I.; "Auditing Data Privacy," *ISACA Journal*, vol. 3, 2018, *www.isaca.org/archives*
15 ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF*
16 *Op cit* ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, p. 8

[17] ISACA, *COBIT® 5 for Assurance*, USA, 2013, p. 59, *www.isaca.org/COBIT/Pages/Assurance-product-page.aspx*

[18] *Ibid.*, p. 55-82

[19] *Op cit* ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*

[20] *Op cit* ISACA, *COBIT 5 for Assurance*, p. 56

[21] *Ibid.*, Section 2B, Assessment Perspective: Providing Assurance Over a Subject Matter, p. 53

[22] ISACA, COBIT® 5 Process Audit/Assurance Programs, *www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/Pages/Audit-Assurance-Programs.aspx#cobit5app*

[23] Cooke, I.; "Innovation in the IT Audit Process," *ISACA Journal*, vol. 2, 2018, *https://www.isaca.org/archives*

[24] European Computer Audit, Control and Security Conference, *https://www.isaca.org/ecommerce/Pages/european-cacs-europe.aspx*

[25] I would like to take this opportunity to publicly thank the gentleman in question, Everett Breakey, CISA, CRISC, CISM, CGEIT, of the ISACA Ireland Chapter, who has made it his mission to bring COBIT 5 training to the population of Ireland.

The Power of IT Investment Risk Quantification and Visualization

IT Portfolio Management

Is it worth the incremental effort to determine IT financial investment risk as part of the IT investment business case? Long, long ago (at least, in IT terms), an IT Portfolio Management Model was developed and introduced to corporate clients by a large IT company.[1] Developed in August 2003, the purpose of the model was to help clients make better decisions about investments in their IT portfolios in the context of both their burgeoning legacy IT costs and their need for IT innovation.

The IT Portfolio Management Model was based on the principles of financial portfolio management, specifically, the relationship between investment risk and investment return as per the so-called risk-return tradeoff. The tradeoff is that higher investment returns can be had only by taking on higher investment risk.[2]

The model also used a modified form of the Boston Consulting Group's (BCG) matrix concept of stars, cash cows, dogs and question marks to help identify the IT investments that would most likely make a sound financial contribution to the organization. The 40-year-old BCG tool is still in use today.[3]

This article explores that 15-year-old IT Portfolio Management Model and contrasts it with ISACA's IT-enabled investment portfolio management paradigm.[4] Where the IT Portfolio Management Model explicitly considered IT financial investment risk and returns, ISACA's IT portfolio management paradigm explicitly considers IT returns and the IT investment mix, where "mix" represents the proportion of the IT portfolio that is invested in, for example, transactional, informational, transformational (strategic) and infrastructural information technology.[5]

Risk of Failure and the Expected Variability of Returns of an IT Investment

Assuming sound alignment between business and IT, knowing what the risk of failure and expected variability of financial returns of an IT investment could feasibly cause stakeholders to rethink how it would be deployed, how it would be resourced, and the nature of process development required to ensure repeatability and consistency.

This is because commitments will have been made to the chief executive officer (CEO) and/or the board of directors (BoD) about the capabilities of the new investment to help realize the organization's strategic and financial objectives, with the chief information officer (CIO) noting that IT project failure would compromise those objectives, possibly with considerable reputational risk to the organization.

Monte Carlo simulation techniques help users visualize IT investment variability and the risk of failure. For example, **figure 1** shows a prospective IT investment with an assessed mean expected return of about US $290,000, a standard deviation

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2slmGcl

Guy Pearce, CGEIT
Has served on boards in banking, financial services, retail and not-for-profits over the last decade. He also served as chief executive officer of a multinational retail credit business, where he led the organization to profitability after the 2008 global financial crisis. He has published numerous articles on data and IT, and today consults on corporate governance, IT governance and data governance.

of about US $200,000, and a ±30 percent probability that the project will produce negative financial returns (financial failure). Metrics like these are useful because they help define the organization’s IT investment risk appetite, which guides decisions about whether a new IT investment should be approved.

> “THIS NEW MODEL, HOWEVER, TAKES THE BUSINESS CASE A STEP FURTHER, BY QUANTIFYING THE FINANCIAL RISKINESS OF THE INVESTMENT TO PROVIDE INTERESTING INSIGHTS INTO THE MAKE-UP OF THE IT PORTFOLIO.”

Figure 1 plots all expected returns from an IT project, showing a high probability of negative returns (the shaded area) and considerable variability of those returns (the width of the distribution).

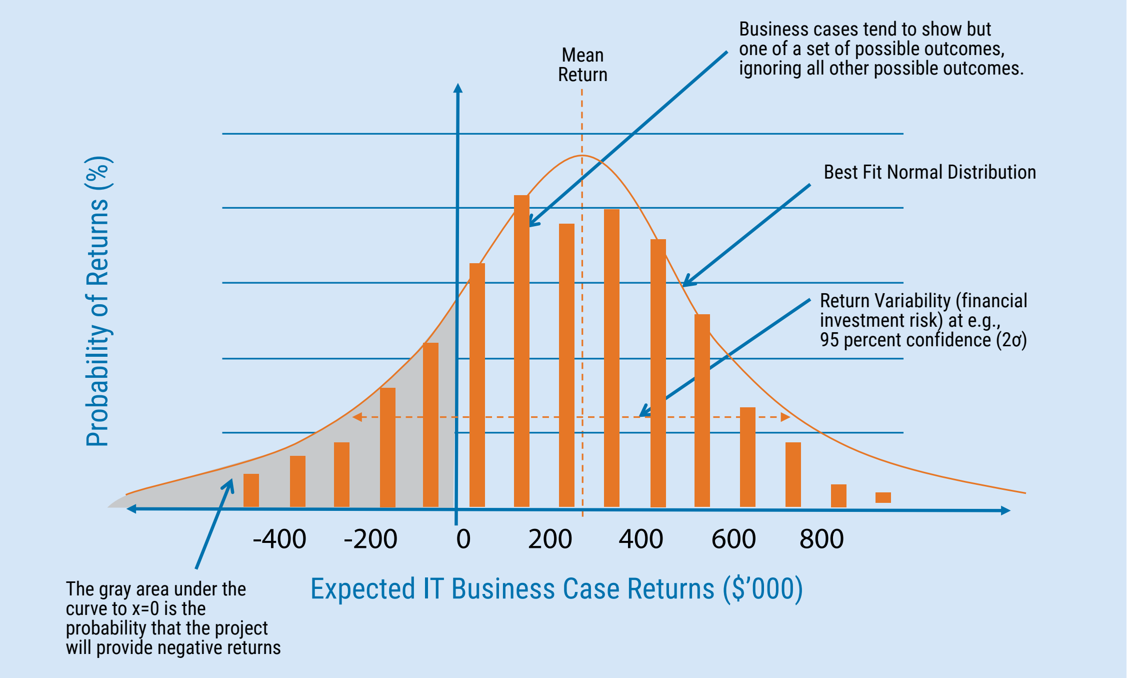
With some reporting that most IT projects fail,[6, 7] what probability of failure would an organization be willing to accept? Is it preferable to go into an IT deployment assuming it will be successful or should more up-front planning be mandatory? IT investment risk analysis helps provide a context for the answers to these questions.

There Are Business Cases and There Are Business Cases

Good IT governance demands a rigorous business case[8] and, in both portfolio models, the benefits of the IT investment are actually captured by the business case. Without an approved business case, the governance task of benefits tracking becomes nearly impossible.

This IT Portfolio Management Model, however, takes the business case a step further, by quantifying the financial riskiness of the investment to provide interesting insights into the make-up of the IT portfolio. In general, while business cases may be supported by a qualitative risk assessment, they generally are not supported by an assessment of the financial risk of the investment.

Figure 1—A Plot of “All” Possible Expected Returns for an IT Project



The simplest way to determine investment risk is to use sensitivity analysis, which determines the percentage change in benefits as a result of a 1 percent change in an input variable, such as staffing costs. The impact of all key input variables is determined in this way and their impact on expected benefits is ranked to find the inputs that have the greatest impact on the business case, and for which risk responses may be needed. A downside of sensitivity analysis is that only one variable is considered at a time.

More sophisticated methods of determining investment risk—modeling the variability of all variables simultaneously—involve probabilistic methods, of which the most popular is Monte Carlo simulation.[9] The technique is noted in the *CGEIT® Review Manual* in the Risk Optimization domain.

Essentially, Monte Carlo simulation substitutes variables in the business case with relevant probability distributions to model uncertainty. In a process involving many thousands of iterations, it selects a set of random values from each distribution for use in the business case, for each iteration, where the outcome of each iteration defines one possible business case outcome. On completion, all the outcomes are plotted in a distribution for analysis, as in **figure 1**.

Monte Carlo methods enable one to say, with a given degree of confidence, that the benefits of an IT investment are likely to fall within a certain range, rather than being expressed as a single value, as would be provided by a traditional business case; the chance of an IT investment returning the exact figure given by a traditional business case is remote, at best.

Plotting the IT Business Cases

In an organization that subscribes to the principles of good IT governance, business cases would exist for the most important IT projects in the portfolio and, in the case illustrated in **figure 1**, the riskiness of the expected returns would be determined too. When plotted, the plot may look similar to **figure 2**.

Based on the risk-reward tradeoff, one would expect an upward sloping trend line with sufficient data points, as indicated in **figure 2**. The closer the IT investments are to the trend line, the more they perform as expected. The farther the IT investments are from this line (the investments highlighted by a darker plot), the more likely the risk-return profiles could be corrected involuntarily (by the market in the case of area B) or voluntarily (by risk response or a focus on realizing benefits).

The vertical axis plots the expected return from the IT investment, while the horizontal axis plots the riskiness of those returns, measured by the standard deviation of returns divided by the mean return (information from the simulation output in **figure 1**). The organization's IT investment risk appetite is shown, being the acceptable variability of returns.

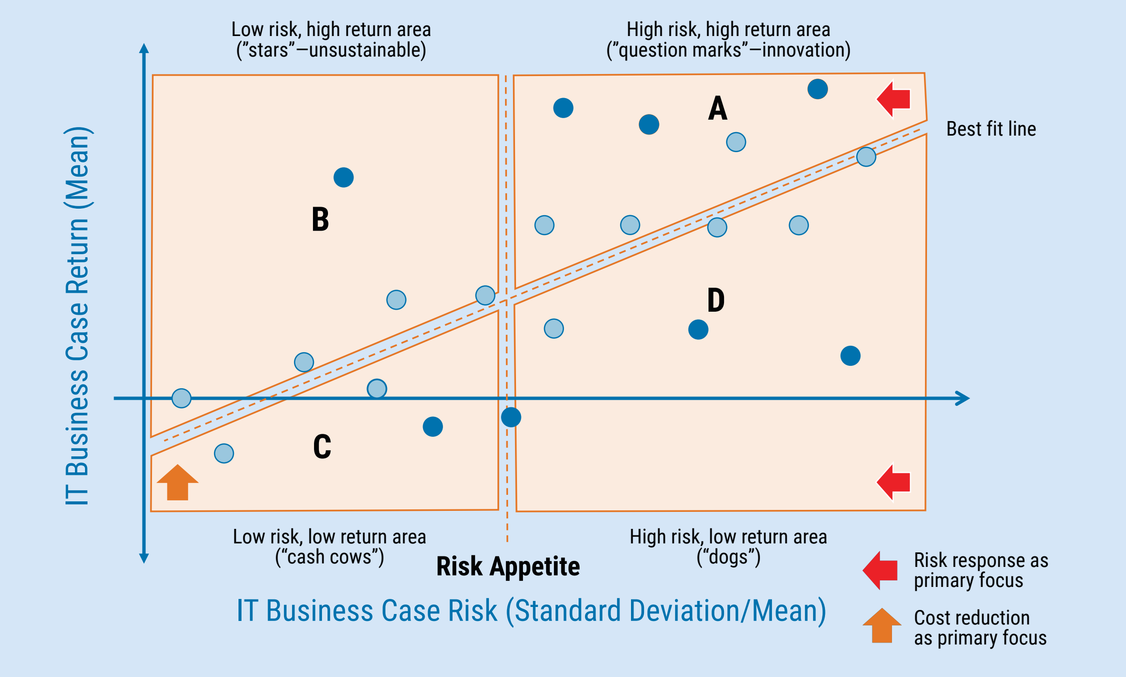
> “ESSENTIALLY, MONTE CARLO SIMULATION SUBSTITUTES VARIABLES IN THE BUSINESS CASE WITH RELEVANT PROBABILITY DISTRIBUTIONS TO MODEL UNCERTAINTY.”

Interpreting the Graph

The intersection between the trend line and the risk appetite line conceptually divides the graph in **figure 2** into four areas:

1. **Area A, Question Marks**—Most investments classified as innovative would be found in this area. Innovative or transformational IT promises high returns, but the riskiness associated with it is seldom articulated, least of all by the technology vendors. The point is that half of these investments will fail,[10] which makes them high-risk with a high probability of failure. The strategic focus should be on risk reduction.
2. **Area B, Stars**—These are interesting investments because they provide higher returns than they should for the risk they bear. Assuming the assessment of risk and return is valid (e.g., all investment costs are appropriately accounted for, and statements of benefit are supported by an action plan that demonstrably drives the benefits claims), such cases can occur when a

Figure 2—A Plot of a Portfolio of IT Projects by Risk



competitive position is leveraged. The position is, however, not sustainable, because competitors will ultimately find ways to compete in this highly profitable area. A new business intelligence (BI) or customer relations management (CRM) (informational) system in an industry where BI or CRM is unfamiliar could result in this situation.

3. **Area C, Cash Cows**—Since these IT investments provide lesser returns than expected for the risk they bear, are they the dogs of the IT investment portfolio? Not necessarily; transactional IT and infrastructural IT are the backbone of any business success and they illustrate cases where margins could be low (transactions) or where most of the benefits of an IT investment are difficult, if not impossible, to quantify (infrastructure).

   The throughputs in these investments can be considerable, and variability in their performance is low due to considerations such as high-availability IT. Cost management is essential for managing this area, because any incremental reduction in costs increases the returns of those investments.

4. **Area D, Dogs**—This is probably the least desirable area on the graph, as the IT investments here provide low returns but bear high risk. Besides a risk focus, these investments should be reviewed through a strategic alignment lens and a cost-cutting lens.

> “INNOVATIVE OR TRANSFORMATIONAL IT PROMISES HIGH RETURNS, BUT THE RISKINESS ASSOCIATED WITH IT IS SELDOM ARTICULATED, LEAST OF ALL BY THE TECHNOLOGY VENDORS.”

Limitations

The IT Portfolio Management Model has limitations; for example, its use demands a certain level of governance of enterprise IT (GEIT) maturity. Some other limitations are:

- Not all IT investments have benefits that are quantifiable. Innovative investments (area A) should be governed by an appropriate business case.
- Calculating investment risk could be complex for some.
- The model is but one abstraction of reality. There are others.
- The estimated risk-return frontier and the risk appetite are different for different companies, realizing that some IT investment business cases would be needed for the organization to make reasonable assessments of both.

It should be noted that the benefits and risk articulated in the business case are based on assumptions that should be qualified. Qualified assumptions provide a perspective of the conditions under which the business case will be a reasonable reflection of reality.

Without qualified assumptions, the benefits-tracking process could be embarrassing for the business case team, especially if the gap between reality and the business case is significant. Without socializing these assumptions, there is little leverage for when the time comes to explain why the technology did not deliver the claimed benefits.

Comparison With ISACA's IT Investment Portfolio Management Paradigm

One part of determining whether the incremental effort required to produce this IT Portfolio Management Model is worth it depends on how mature the GEIT practice is in the business case and benefits realization domains. Both models depend on credible business cases. **Figure 3** summarizes the differences between ISACA's IT investment portfolio management paradigm and the IT Portfolio Management Model.

Figure 3—Summary of the Key Differences Between the Two Approaches

	ISACA IT Investment Portfolio Management Paradigm	IT Portfolio Management Model
Relative time to build the portfolio	Less	More
Relative ease of calculation	Easier	More difficult
Relative data requirements	Less	More
Shows investment returns	Yes	Yes
Shows investment risk	No	Yes
Portfolio mix	Explicit	Implicit (strategic alignment assumption)
Provides investment strategy direction	By means of the mix criterion	By means of areas A, B, C and D in **figure 2**)
Defined investment risk appetite	Indirectly via the CGEIT risk domain	Yes

In Practice

The Office of the Auditor General (OAG) of Canada refers to an artifact called an IT Portfolio Risk Profile, finding that:

> *(IT) Risk management is critical where high-priority portfolio components depend on each other, where the cost of portfolio component failure is significant, or when risks from one portfolio component raise the risks to another portfolio component.*[11]

The cost of portfolio component failure (rather than of portfolio failure) concerns the implications of an individual IT investment failing to deliver. Since the OAG report also speaks of IT playing "a key part in the Agency's ability to achieve its strategic

> “THE COST OF PORTFOLIO COMPONENT FAILURE (RATHER THAN OF PORTFOLIO FAILURE) CONCERNS THE IMPLICATIONS OF AN INDIVIDUAL IT INVESTMENT FAILING TO DELIVER.”

objectives,”[12] it indicates that strategic alignment is an important construct for the agency and failure of high-priority components will have negative implications for performance.

Conclusion

Financial risk is an important part of portfolio management at the level of individual IT investments. This article proposes a means to increase the visibility of individual IT component financial risk in the interests of mitigating the negative implications of IT failure on strategic performance.

Potentially augmenting ISACA’s IT investment portfolio management paradigm, the visualization of financial risk and understanding what kinds of responses are required to increase success of IT in the different areas, as in **figure 2**, are useful in the context of helping to ensure that the strategic objectives of the organization are achieved.

Strategically, determining financial IT investment risk provides invaluable visual insights in the context of IT portfolio management, even though it may take a little more effort to produce.

Endnotes

[1] As a management consultant for this large IT company at the time, the author developed the model in question. A recent study of ISACA’s *CGEIT® Review Manual* gave the author reason to revisit his 15-year-old IT Portfolio Management Model and even to contrast it with ISACA’s IT investment portfolio management paradigm.

[2] Nasdaq, “Risk-Return Tradeoff,” definition, *www.nasdaq.com/investing/glossary/r/risk-return-trade-off*

[3] Reeves, M.; S. Moose; T. Venema; “BCG Classics Revisited: The Growth Share Matrix,” Boston Consulting Group, 4 June 2014, *www.bcg.com/publications/2014/growth-share-matrix-bcg-classics-revisited.aspx*

[4] ISACA, *CGEIT® Review Manual, 7th Edition*, USA, 2015, p. 95, *https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=CGM7ED*

[5] Massachusetts Institute of Technology (MIT) Center for Information Systems Research, IT Portfolio Management, MIT Sloan School of Management, Cambridge, USA, *https://cisr.mit.edu/research/research-overview/classic-topics/it-portfolio-management/*

[6] Krigsman, M.; “Study: 68 Percent of IT Projects Fail,” *ZDNet*, 14 January 2009, *www.zdnet.com/article/study-68-percent-of-it-projects-fail/*

[7] Ezer, J.; “Why Do So Many I.T. Projects Fail?” *Huffpost*, 10 September 2010, *https://www.huffingtonpost.com/jonathan-ezer/why-do-so-many-it-project_b_712060.html*

[8] *Opcit* ISACA

[9] Sharcnet, “1.5 Probabilistic Design Techniques,” University of Waterloo, Ontario, Canada, *https://www.sharcnet.ca/Software/Ansys/16.2.3/en-us/help/ans_adv/Hlp_G_ADVPDS5.html*

[10] Massachusetts Institute of Technology (MIT) Center for Information Systems Research, Risk-Return Profiles in the IT Portfolio, MIT Sloan School of Management, Cambridge, USA, 2009, *https://cisr.mit.edu/files/2009/12/Topic-Portf_Slide4_lg.PNG*

[11] Office of the Auditor General of Canada, “Report 5—Information Technology Investments—Canada Border Services Agency,” 2015, *www.oag-bvg.gc.ca/internet/English/parl_oag_201504_05_e_40351.html#p17*

[12] *Ibid*.

Integrating KRIs and KPIs for Effective Technology Risk Management

Performance evaluation is a key element of any management system and a good governance practice. It involves six key activities: monitoring, measurement, analysis, evaluation, internal audit and management review. Performance evaluation of an organization's risk management system ensures the risk management process remains continually relevant to the organization's business strategies and objectives. Organizations should adopt a metrics program to formally carry out performance evaluation. An effective metrics program helps in measuring security and risk management from a governance perspective.[1]

Simply stated, metrics are measurable indicators of performance. The two key metrics that are used are key risk indicators (KRIs) and key performance indicators (KPIs). *COBIT® 5 for Risk* defines KRIs as metrics capable of showing that the enterprise is, or has a high probability of being, subject to a risk that exceeds the defined risk appetite.[2] They are critical to the measurement and monitoring of risk and performance optimization. These metrics help in effectively reporting the risk management performance results (risk communication) to stakeholders and enable management in taking informed risk management decisions. While KPIs focus on business performance, KRIs focus on risk management performance.

This article highlights how a risk metrics program can be used to integrate KRIs and KPIs for effective technology risk management.

Risk Metrics Program

An effective risk metrics program yields several benefits, including:

- Enabling regular review of risk trends and better visibility of technology risk and vulnerabilities
- Enabling increased accountability and improved technology risk management effectiveness
- Assisting in management review and providing decision indicators for continual improvement of technology risk management
- Providing inputs for prioritizing resource allocation decisions
- Assisting in streamlining risk communications
- Contributing to overall cost savings and increased risk management efficiency

The key steps in the risk metrics program are:

- Selection and development of metrics
- Collection of metrics data
- Analysis of metrics data
- Reporting of metrics results

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2sOsp0D

Rama Lingeswara Satyanarayana Tammineedi, CISA, CRISC, CBCP, CISSP, MBCI, PMP
Is a consultant to various industries in the area of cyberresilience, covering information security governance, information security policy and procedures, security assessments, operational and information risk management, business continuity management, IT disaster recovery planning, ISO/IEC 27001 implementation, data privacy, and ITIL assessment. He has more than 30 years of IT experience in diverse organizations—business and technology—that enables him to deliver client-focused services and value as a cybersecurity consultant.

Enjoying this article?

- Learn more about, discuss and collaborate on information security management in the Knowledge Center. *www.isaca.org/information-security-management*

The set of risk metrics selected for initial implementation should be based on the organization's current risk management maturity level and should contribute to improvement of high-priority risk management focus areas. The metrics should also cover various categories of stakeholders in the organization. The collection and analysis of metrics data and reporting of metrics results can be automated (see the section of this article titled "Automation—The Role of GRC Tools in a Metrics Program"). The three-lines-of-defense model[3] is suggested to establish risk ownership and ensure accountability.

Risk Ownership and the Three-Lines-of-Defense Model Against Risk

Business managers tend to think that technology risk is owned and managed by IT or the risk function within the organization. *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.[4]

The three-lines-of-defense model can be used as a primary means to structure the roles and responsibilities for risk-related decision-making and control to achieve effective risk governance, management and assurance:

1. **The first line of defense** is the management teams of individual lines of business (LoBs), who are responsible for identifying and managing the risk inherent in the products, services, processes and systems within their LoBs.
2. **The second line of defense** is an independent corporate risk function, responsible for designing the risk management framework; defining roles and responsibilities; and providing oversight, support, monitoring and reporting.
3. **The third line of defense** is the internal audit function and is responsible for an independent review of the organization's risk management controls, processes and systems.

> "LINKING KRIs TO KPIs ALSO HELPS IN GETTING BUSINESS BUY-IN FOR INVESTMENT IN RISK MITIGATION MEASURES."

Figure 1 provides an overview of the roles and responsibilities of the three lines of defense, with example KRIs.

Figure 1—Three Lines of Defense and Their Roles and Responsibilities

Line of Defense	First Line of Defense	Second Line of Defense	Third Line of Defense
Organization Unit	**Lines of Business**	**Risk Function**	**Internal Audit**
Role	Risk owners/managers	Risk governance	Independent assurance
Responsibilities	• Identify and manage risk. • Assess and enhance controls. • Monitor and report the risk profile. • Comply with risk policies and frameworks.	• Assist in determining risk strategies, policies and structures for managing risk. • Provide risk management frameworks. • Define roles and responsibilities. • Provide oversight, support, monitoring and reporting.	• Provide independent and objective assurance on the overall effectiveness of the risk governance and management. • Communicate results of the independent reviews to all stakeholders.
Example KRIs	• Percentage of incidents involving customer personal data	• Lack of succession plan for key roles	• Lack of effective reporting of key risks

The model helps in aligning risk strategy, governance, management and assurance.

Figure 2—Linking KRIs With KPIs

KRI	KPI	Implication/Business Impact
Lack of succession plan for key roles	On-time rollout of service or delivery of project	Lack of backup for identified key roles affects service continuity, leading to compliance issues and possible failure to meet service level agreements (SLAs).
Percentage of incidents involving customer personal data	Adherence to regulations, policy or processes	This indicates a failure to meet compliance obligations and might lead to scrutiny from regulators or media, which can adversely impact the reputation of the organization.
Number of services cancelled or delayed owing to security-related service downtimes	Number of security-related service downtimes	Security incidents impacting critical systems potentially cause service interruption or degradation.
Percentage of business applications/systems not supported by a backup plan	Number of business applications/systems not supported by a backup plan	Lack of data backup for business applications/systems leads to data loss and adversely affects service continuity in case of any interruption.
Number of nonconformities detected in security tests/audits remaining unresolved beyond the planned time frame	Percentage of nonconformities detected in security tests/audits, but not resolved within the time frame planned	Delay in remediating vulnerabilities detected in security tests/audits makes the organization an easy target for malicious attacks.
Number of security incidents attributed to vulnerabilities in third-party systems/employees	Inadequate third-party management	The organization's information can be exposed to risk by third parties with inadequate information security management.
Number of systems without up-to-date patches	Lack of adequate time frame for scheduled downtime of systems	Delay in patching the systems makes the organization an easy target for malicious attacks.
Lack of effective reporting of key risk	Lack of review of risk management processes	In the absence of a review of risk management processes, these processes might continue to be ineffective, resulting in nonidentification of vulnerabilities/risk.

The Need for Linking KRIs to KPIs

Linking KRIs to KPIs enables business managers to appreciate the relationship between risk and business performance, and relevance of KRIs to the organization's business objectives and risk appetite. This helps in cross-functional collaboration and embedding risk considerations into business decisions. Linking KRIs to KPIs also helps in getting business buy-in for investment in risk mitigation measures. **Figure 2** shows some examples of KRIs linked to KPIs and the business impact of the KRIs.

COBIT 5 for Risk and KRIs

COBIT 5 for Risk is a COBIT® 5 professional guide that discusses IT-related risk and provides detailed and practical guidance for risk professionals. Specific to KRIs, it defines KRIs, lists the parameters and criteria for KRI selection, describes the three-lines-of-defense model, lists the benefits KRIs provide to an enterprise, and outlines common challenges encountered during successful implementation of KRIs.

COBIT 5 for Risk lists some possible KRIs for different stakeholders—the chief information officer (CIO), the risk function and the chief executive officer (CEO)/board of directors (BoD). Some of these KRIs are shown in **figure 3**.

Automation—The Role of GRC Tools in a Metrics Program

A governance, risk and compliance (GRC) risk management solution provides an organization with a consolidated view of its risk. The solution allows for risk assessment and gives authorized personnel

Figure 3—Example KRIs From COBIT 5 for Risk

Event Category	CIO	Risk Function	CEO/BoD
Investments/project decision-related events	• Percent of projects on time, on budget • Number and type of deviations from technology infrastructure plan	• Percent of IT projects, reviewed and signed off on by quality assurance (QA); that meet target quality goals and objectives • Percent of projects with benefit defined up-front	• Percent of IT investments exceeding or meeting the predefined business benefit • Percentage of IT expenditures that have direct traceability to the business strategy
Business involvement-related events	• Degree of approval of business owners of the IT strategic/tactical plans	• Frequency of meetings with enterprise leadership involvement where IT's contribution to value is discussed	• Frequency of CIO reporting to or attending executive board meetings at which IT's contribution to enterprise goals is discussed
Security	• Percent of users who do not comply with password standards	• Number and type of suspected and actual access violations	• Number of (security) incidents with business impact
Involuntary staff act: destruction	• Number of service levels impacted by operational incidents • Percent of IT staff who complete annual IT training plan	• Number of incidents caused by deficient user and operational documentation and training • Number of business-critical processes relying on IT not covered by IT continuity plan	• Cost of IT noncompliance, including settlements and fines • Number of noncompliance issues reported to the board or causing public comment or embarrassment

Source: Adapted from ISACA, *COBIT 5 for Risk* (Figure 70: Example KRIs), USA, 2013. Reprinted with permission.

the ability to assign metrics to risk, collect changes in the organization's risk profile, and monitor risk and metrics against targets and tolerance thresholds.

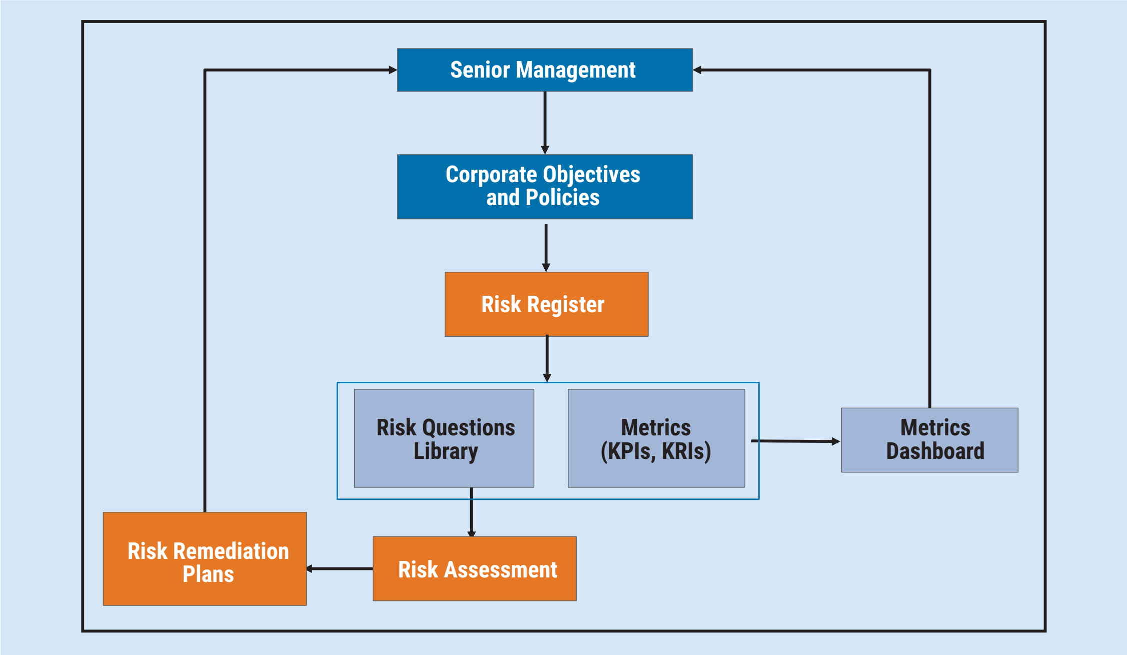
Corporate objectives and policies defined by senior management, together with other authoritative sources and standards, contribute to the development of a risk register. The risk register is used to generate risk assessment questionnaires that are used for conducting risk assessments. Risk assessment results drive the development and implementation of risk remediation or mitigation plans. These plans, as well as the outcomes, are communicated to senior management.

Corporate objectives and the risk register are used to develop the metrics—KPIs and KRIs, respectively. The metrics dashboard or results are communicated to senior management on a regular basis. **Figure 4** provides an overview of a risk metrics automation workflow in a typical GRC solution.

Conclusion

Risk communication is a key element of the risk management process. Communication and consultation with stakeholders are important as they make judgments about risk based on their perceptions of risk.[5] An effective risk metrics program brings objectivity into stakeholders' risk perception by providing a shared language to measure the effectiveness of security and risk mitigation measures within the organization. Integration of KRIs with KPIs helps in strengthening organizations' risk culture by enabling business managers to recognize the business benefits of effective technology risk management.

Figure 4—Overview of Risk Metrics Automation Workflow in a Typical GRC Solution



Endnotes

1 For examples of operational efficiency metrics and metrics in a security balanced scorecard, see Volchkov, A.; "How to Measure Security From a Governance Perspective," *ISACA® Journal*, vol. 5, 2013, *www.isaca.org/archives*

2 ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

3 For a detailed description of the three-lines-of-defense model and its role within the enterprise's wider governance framework, see *COBIT® 5 for Risk*.

4 *Op cit* ISACA

5 For a detailed description of the importance of communication and consultation in risk management, see International Organization for Standardization, ISO 31000:2018, *Risk management—Guidelines.*

Protection From GDPR Penalties With an MFT Strategy

Do you have something to say about this article?

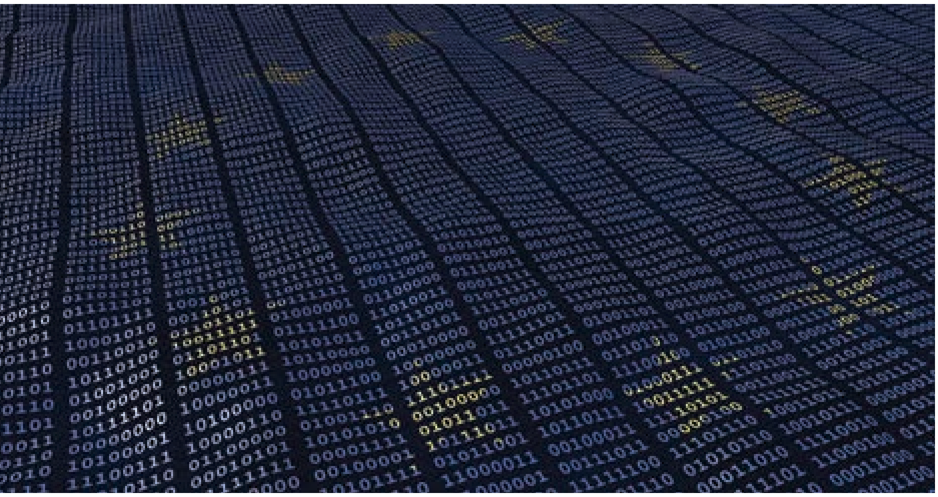
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2sJuwmh

Companies facing the EU's looming General Data Protection Regulation (GDPR) compliance mandate could benefit from a modernized managed file transfer (MFT) solution.

GDPR aims to streamline data protection regulations and strengthen data protection for all individuals affiliated with the European Union. The new mandate applies to any EU company that has an establishment in the European Union, provides goods and services to EU residents, and monitors the behavior of EU residents. What it all comes down to is protecting the rights of an individual's data privacy.

But the GDPR reaches beyond European borders. Any organization, no matter where it operates in the world, selling goods or services to businesses or citizens in EU member countries must comply with GDPR. This applies to any private citizen who simply lives, works or travels through the EU countries—meaning, anyone's personal data can fall within GDPR's scope. Personal data are defined as any information (legal names, bank details, medical information, email addresses, IP addresses, global positioning system [GPS] data and photos among others) related to a natural person or "data subject" that can be used to directly or indirectly identify a person.



Dave Brunswick
Has more than 25 years of experience in technical sales, presales, technology strategy, engineering, product management and product development, including holding senior consulting and architecture roles throughout the managed file transfer software market. He currently serves as vice president of North America presales and solution support for Cleo.

Knowing how GDPR compliance involves a complex combination of on-premise and cloud systems and tools, a robust MFT solution and integration platform are useful for any organization in the business of data movement. MFT supports organizational security by enhancing operational visibility and efficiency, and safeguarding sensitive data is an integral part of this new EU mandate. Outdated file transfer solutions will not deliver the auditing, logging, reporting and automation that will help with compliance.

Impact of GDPR

Missing GDPR's 25 May 2018 compliance deadline will be costly when the UK Information Commissioner's Office (ICO) and other EU agencies start auditing companies. Simply failing a GDPR audit means a fine of 2 percent of an organization's annual global turnover or US $12.3 million (€10 million). Data breaches will cost organizations even more. Breached organizations face a hefty fine of 4 percent of annual global turnover or US $21.2 million (€20 million), whichever amount is higher. And gone are the days that organizations could wait months—even years—without divulging information about compromised data. The window to report breaches is tightening. Once an organization is made aware of a breach, hacks that may pose a risk must be reported to affected individuals and to the data protection authorities within 72 hours.

The fact is, attacks on systems that store personal information, unfortunately, are more and more common in the digital age. This just goes to show that even the most technologically savvy organizations struggle to cover all their bases, leaving them prone to breaches, big or small. But the European Union is trying to raise the bar with GDPR, which aims to streamline the data protection regulations and strengthen protection for all individuals affiliated with the European Union.

Equifax is an example of how hard the GDPR hammer can drop. By now, nearly everyone with a credit report is familiar with the bureau's high-profile data breach.[1] Many people viewed Equifax's fiasco as staggering, egregious and historic. As one of the three major credit reporting agencies in the United States, the Atlanta-based bureau compromised the names, Social Security numbers, home addresses, dates of birth, driver's license numbers and credit card information of nearly 146 million Americans and even 700,000 British citizens.[2]

Arguably, the major concern throughout the credit report breach incident and others like it, such as those targeting Uber and Facebook, has been the lack of immediate transparency, communication and accountability. Equifax's data breach reportedly occurred in mid-May, but it was not discovered by bureau officials until 29 July and was not reported to consumers until 7 September—a 41-day delay before those affected were notified that sensitive personal information had been hacked.

If GDPR had been in effect when Equifax was breached, the credit reporting bureau giant would be facing fines of approximately US $130 million. With that thought in mind, organizations are being forced to think more about digital transformation and adapt new technologies because of a new EU mandate.

Yes, GDPR puts an increased weight of data security on the shoulders of organizations, but that does not mean the majority of organizations that must be compliant are taking necessary action. According to a recent survey,of the nearly 3,000-plus security decision makers in organizations with more than 20 employees in the United States and nine other countries, roughly 30 percent think their organization is GDPR-ready.[3] The report goes on to state that only 26 percent of Europe-based enterprises say they are GDPR-compliant. When it comes down to it, the report says, "the percentage of companies not affected by GDPR is small."[4]

> "AN ADVANCED MFT SOLUTION WILL GO A LONG WAY IN ENSURING THAT ROUTINE BUSINESS-CRITICAL INFORMATION FLOWS ARE NOT RISKING HEFTY NONCOMPLIANCE PENALTIES."

Everything an organization does with data constitutes processing, and virtually every process involves data transfer at some level. MFT is key to ensuring those processes meet GDPR requirements. For industries such as healthcare, supply chain and logistics, financial services, and Software as a Service (SaaS), data transfer is the lifeblood of an organization's operation, keeping in mind that any action on data is technically a processing event, including internal transfers, external transfers, storage, viewing, analyzing, changing, synchronizing and replicating. By deploying a steadfast and secure file transfer system that tracks the who, what, where and when of transactions, organizations have the functionality and documentation required to comply with GDPR and beyond.

MFT Solution for GDPR Compliance

An advanced MFT solution will go a long way in ensuring that routine business-critical information flows are not risking hefty noncompliance penalties. Modernization provides advanced security and the control and governance needed to ensure GDPR-compliant data transfers, and the clear, accurate documentary evidence to prove it.

MFT solutions assist enterprises in the management, control and governance of the data flows that power their business ecosystem. A centralized, reliable, scalable and secure file transfer solution can improve business performance, reduce IT complexity and inefficiencies, support corporate cloud and big data initiatives, and reduce risk associated with GDPR data breaches and noncompliance.

The security and visibility of an MFT solution, combined with a data management strategy, will enable an organization to enforce and facilitate compliance directives. Proper procedures, policies and technologies allow for better control and transparency over data that must be protected—whether in movement or at rest. MFT helps enhance organizational security details through operational visibility and efficiency.

A complete MFT solution securely transports personally identifiable information (PII), payment card industry (PCI) and protected health information (PHI) data to and from organizations that must adhere to GDPR compliance by using encryption of data in motion and at rest, nonrepudiation, data integrity checks, comprehensive transfer logging, and integration with existing security systems.

How can a modern and robust MFT solution enable secure PII, PCI and PHI data transfer compliance for GDPR?

- According to GDPR article 5.1, personal data must be processed to ensure the appropriate security of the personal data. With the right MFT solution in place, a two-tier architecture method secures demilitarized zone (DMZ) streaming while data are secured in transit and at rest: Secure Sockets Layer (SSL), Secure Shell (SSH), Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail Extensions (S/MIME), Extensible Markup Language (XML), Internet Protocol (IP) whitelisting/blacklisting, and US Federal Information Processing Standards (FIPS) 140 -S compliance.
- According to GDPR articles 7 and 8, individuals may give consent to have their personal data collected and/or used when there is no other legal basis to process an individual's information (e.g., vital interest, legitimate interest, contractual obligation), and consent must be separable from other written agreements. GDPR articles 15 and 20 state that EU citizens may request a copy of their data and request a transfer of personal data from organization to organization upon request. That is where an MFT solution can offer nonrepudiation via digital receipts and signatures to ensure the authenticity of a message or document. User authentication is delivered via Lightweight Directory Access Protocol (LDAP) and Active Directory mechanisms.
- According to GDPR article 25, organizations must be able to provide a reasonable level of data protection and privacy. A modern MFT solution has multiple advanced protocols to deliver the flexibility to securely connect a business to all kinds of trading partners (business-to-business [B2B], application-to-application, peer-to-peer). It stores personal data securely by using industry-leading algorithms such as SHA-256 to ensure that personal data are kept secure.
- According to GDPR article 30, records of processing activities must be maintained, including the type of data processed and purpose for which they are used. With MFT, detailed audit trailing and logging centralizes file tracking; filters searchable content; enables dashboards for

Enjoying this article?

- Read *Implementing the General Data Protection Regulation www.isaca.org/implementing-GDPR*

enhanced data tracking; and provides alerts and notifications, even non-event alerting.

- According to GDPR articles 39.1(b) and 39.2, a data protection officer (DPO) must be able to monitor compliance with the GDPR regulation. GDPR article 32 says a controller and processor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. MFT offers delegated administration to distribute supervision capabilities across business units on a centralized browser.

Conclusion

It is up to each organization to determine how it will meet this new EU compliance and avoid mistakes that could be Equifax-like in proportion. GDPR guidelines do not specifically dictate how compliance is done, it just orders what needs to be done, why it needs to be done and when it needs to be done. But accurate management of organizational data cannot happen without the right strategy and tools.

Most likely, the GDPR mandate is just the first wave of what constitutes a global reenvisioning of data security and personal privacy regulation. And, while data integration is not the be-all nor end-all to becoming completely GDPR-compliant, with robust, scalable MFT and B2B solutions in place to centralize and govern all data moving throughout an organization with quick and secure protocols, organizations that must be GDPR-compliant can avoid delaying the inevitable and become a modernized commodity in the continued globalization of data.

> “MOST LIKELY, THE GDPR MANDATE IS JUST THE FIRST WAVE OF WHAT CONSTITUTES A GLOBAL REENVISIONING OF DATA SECURITY AND PERSONAL PRIVACY REGULATION.”

Endnotes

[1] Equifax, “2017 Cybersecurity Incident & Important Consumer Information,” 1 March 2018, *https://www.equifaxsecurity2017.com/*

[2] BBC, “Equifax to be Investigated by FCA Over Data Breach,” 24 October 2017, *www.bbc.com/news/technology-41737241*

[3] Iannopollo, E., *et al*; “The State of GDPR Readiness,” Forrester, 31 January 2018, *https://www.forrester.com/report/The+State+Of+GDPR+Readiness/-/E-RES141679*

[4] *Ibid*.

The Promises and Jeopardies of Blockchain Technology

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (*www.isaca.org/journal*), find the article and click on the Comments link to share your thoughts.

https://bit.ly/2JaFSuB

Disponible également en français

www.isaca.org/currentissue

The idea of the distributed ledger of everything, which burst into the public scene in 2008 with the publication of the fascinating white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*,[1] has transitioned from hype to reality much faster than many experts had predicted. The author of the paper vanished soon after introducing the ingenious cryptographic concept, telling a fellow Bitcoin developer back in 2011 that he had "moved to other things."[2]

The nascent technology, however, which was introduced as a mere 31,000 lines of code,[3] has now clearly grown far beyond its original intent. At the time of this writing, CoinMarketCap, a cryptocurrency market capitalization tracking website, listed 731 coins and 562 tokens, including Marijuanacoin, Cabbage, SatoshiMadness, PonziCoin, Monster Byte and several other absurd names.[4]

Phil Zongo

Is an experienced head of cybersecurity, strategic advisor, author and public speaker based in Sydney, New South Wales, Australia. He is the author of *The Five Anchors of Cyber Resilience*—a contemporary strategy book that absorbs the ambiguity and complexity associated with cyber security and passes on practical guidance to directors, business executives, CISOs and other risk management professionals. Zongo was the 2016-17 recipient of ISACA's Michael Cangemi Best Book/Article Award, a global award that recognizes individuals for major contributions to publications in the field of IS audit, control and/or security. He is also a member of the board of directors of the ISACA Sydney (New South Wales, Australia) Chapter. In 2016, Zongo won the ISACA Sydney Chapter's first-ever Best Governance of the Year award, a recognition for the thought leadership he contributes to the cybersecurity profession. Over the last 14 years, Zongo has advised several business leaders on how to cost-effectively manage business risk in complex transformation programs. Zongo regularly speaks at conferences on disruptive trends, such as cyberresilience, blockchain, artificial intelligence and cloud computing.

Confirming the cryptocurrency mania, a start-up called Brave recently raised US $35 million in approximately 30 seconds during an initial coin offering (ICO) to fund the development of a new web browser.[5] Inspired by traditional initial public offerings (IPOs), ICOs are a novel capital-raising method whereby start-ups grant investors digital tokens in exchange of cryptocurrency, such as Ether or Bitcoin. Ether is the cryptocurrency that powers the Ethereum network—a decentralized platform that runs smart contracts on a blockchain, referred to as the Ethereum Blockchain.[6] But, unlike IPOs, the majority of ICOs are carefully crafted so that they do not classify as financial assets, as doing so will automatically invoke several financial regulation clauses.

This technology that underlies Bitcoin and other virtual currencies, referred to as blockchain, is an open, distributed ledger that enables two unrelated parties to exchange anything of value—such as intellectual property, title deeds or virtual currency—without the need of a central guaranteeing authority, such as a bank.[7] Blockchain transactions are periodically validated and chronologically appended to the previous block using a pair of asymmetric cryptographic keys. Unlike traditional databases, blockchains are distributed across many participants in the network; they do not exist in on centralized repository.[8] Blockchains can be used in both public and private settings.

Blockchain's use cases, however, extend far beyond the realm of cryptocurrencies; this technology is undeniably destined to redefine several industries. The healthcare sector, for instance, fits the bill perfectly. Through its core virtue of decentralized architecture, blockchain is anticipated to supplant archaic, fragmented and heterogenous healthcare systems, thus boosting interoperability of healthcare data.[9] Furthermore, by creating "a common database of health information that doctors and providers could access no matter what electronic medical system they used,"[10] blockchain will provide physicians complete view to sequentially arranged patient records, improving the quality of patient care and lowering healthcare delivery costs.

Another industry prime for blockchain disruption is the complex world of derivatives, swaps and futures trading. Within this sector, the existence of "multiple versions of the truth" results in significant inefficiencies and costs through reconciliations, exception handling and manual interventions.[11] A case in point is the Depository Trust & Clearing Corporation (DTCC), a New York (USA)-based post-trade financial services giant that processes a staggering 100 million clearing and settlement transactions daily, worth trillions of US dollars. The DTCC is executing a blockchain proof of concept to enable it and its clients "to further streamline, automate and reduce the cost of derivatives processing across the industry by eliminating the need for disjointed, redundant processing capabilities and the associated reconciliation costs."[12]

Given the depth, breadth and credibility of this blossoming technology, it is no wonder that a leading thinker has equated blockchain's strategic importance to that of the World Wide Web, saying that, arguably, blockchain "might give us back the Internet, in the way it was supposed to be, more decentralized, more open, more private, more equitable, and more accessible."[13]

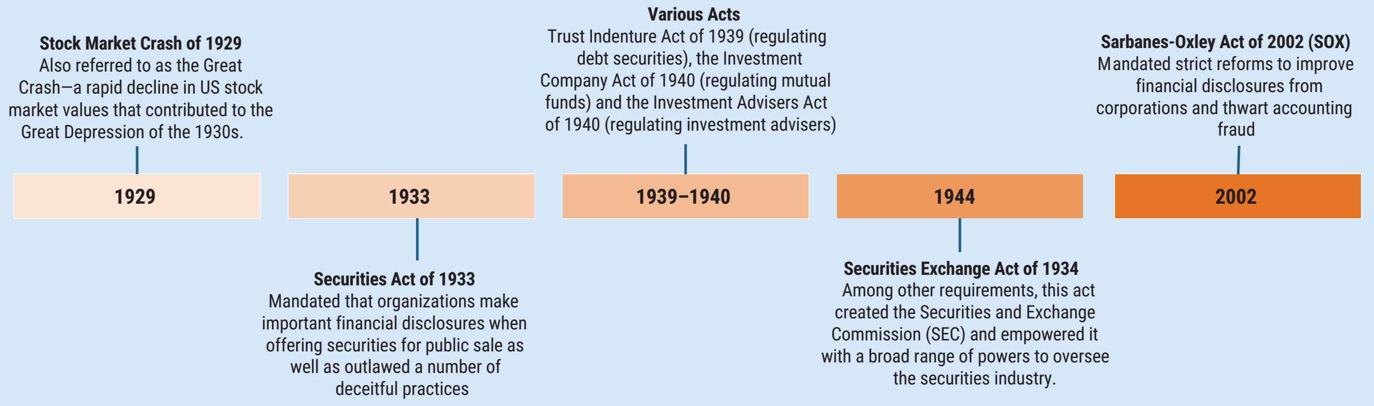
The potential and benefits of this emerging technology are compelling. The distributed ledger of everything, however, also carries complex and hidden risk. Governments, enterprises and civilians can make strategic mistakes by ignoring or discounting blockchain's downsides. The following sections explore in-depth three fundamental challenges enterprises face when adopting blockchain: the absence of clear-cut regulations, security vulnerabilities and interoperability with existing core systems.

> "THE DISTRIBUTED LEDGER OF EVERYTHING, HOWEVER, ALSO CARRIES COMPLEX AND HIDDEN RISK."

The Absence of a Regulatory Framework

To appreciate the significance of this matter, it is worth briefly reflecting on some historical moments that birthed and shaped securities regulations, with focus on the United States (**figure 1**). In the aftermath of the market crash of 1929 and ensuing Great Depression, the US Congress passed the Securities Act of 1933 and The Securities Exchange Act of 1934. These regulations were aimed at restoring the badly dented public trust in financial markets. Among a raft of requirements, the two laws mandated that

Figure 1—Overview of Major Historical Events That Shaped US Securities Regulations



Stock Market Crash of 1929
Also referred to as the Great Crash—a rapid decline in US stock market values that contributed to the Great Depression of the 1930s.

1929

1933

Securities Act of 1933
Mandated that organizations make important financial disclosures when offering securities for public sale as well as outlawed a number of deceitful practices

Various Acts
Trust Indenture Act of 1939 (regulating debt securities), the Investment Company Act of 1940 (regulating mutual funds) and the Investment Advisers Act of 1940 (regulating investment advisers)

1939–1940

1944

Securities Exchange Act of 1934
Among other requirements, this act created the Securities and Exchange Commission (SEC) and empowered it with a broad range of powers to oversee the securities industry.

Sarbanes-Oxley Act of 2002 (SOX)
Mandated strict reforms to improve financial disclosures from corporations and thwart accounting fraud

2002

The aim of this figure is solely to highlight some of the historical moments that gave rise to and shaped US securities regulations. A detailed analysis of the history of securities exchange laws is beyond the scope of this article.

organizations make important financial disclosures when offering securities for public sale and prohibited a wide range of deceitful practices.

In the years that followed, the US government enacted several additional laws to further tighten governance of securities markets and protect investors. These included, but were not limited to, the Trust Indenture Act of 1939 (regulating debt securities), the Investment Company Act of 1940 (regulating mutual funds) and the Investment Advisers Act of 1940 (regulating investment advisers).[14] Approximately 70 years later, in response to Enron, WorldCom and Tyco financial reporting mendacities that bankrupted several investors, George W. Bush, then President of the United States, signed into law the Sarbanes-Oxley Act of 2002 (SOX). Named after the two US senators who sponsored it, SOX mandated strict reforms to improve financial disclosures from corporations and thwart accounting fraud.[15]

Granted, financial regulations have their imperfections. Opponents argue that they engender inefficiencies and drive needless costs, often borne by investors. But, despite occasional letdowns, securities regulations continue to insulate investors from deceitful enterprises, thus buttressing public trust in financial markets and promoting long-term prosperity. The pertinent information mandated by these laws—such as audited financial statements, strategies, risk and governance—enable investors to align their investment strategies with their appetite for risk and personal circumstances.

But until recently, there have been very few global laws to govern digital currencies and ICOs. Regulators are, however, aware of this matter and are starting to act. The responses are disjointed and sporadic. Countries such as China and Hong Kong have outlawed ICOs. Meanwhile, countries such as Australia, Switzerland and the United States have issued guidelines articulating circumstances under which an ICO is deemed a security.[16] The US Securities and Exchange Commission (SEC) has also publicly scolded celebrities who thoughtlessly promoted ICOs via their Twitter accounts. The Central Bank of Nigeria (CBN), one of Africa's largest economies, distanced itself from Bitcoin regulation, stating, "Central bank cannot control or regulate bitcoin. Central bank cannot control or regulate blockchain. Just the same way no one is going to control or regulate the Internet. We don't own it."[17]

Several other jurisdictions are still scrambling to figure out how to respond to this new challenge. The limited examples cited also highlight the divergent nature of regulatory responses. As a result, due to the virtual nature and global reach of ICOs, subscribers all over the world can participate in an ICO, leading to potential conflicts of laws across jurisdictions.[18] This means if investors subscribe in an ICO not registered in their country and things go wrong, local laws will do little to protect them. The patchy global regulatory frameworks have created significant risk for consumers and glaring loopholes for bad guys to exploit. This vacuum is quite troubling, albeit not surprising. The disdain for centralized governance is by design; it is not an omission by cryptocurrency creators. Invented soon after the 2007 global financial crisis, Bitcoin's original intent was to act as a counterforce to central governments, big banks and other political schemes—a concept referred to as cryptoanarchy. What cryptoanarchists did not foresee, however, is that code and cryptography by themselves cannot shield investors from the unavoidable self-dealings, greed and other transgressions of the corporate world. Predictably, three stubborn challenges have emerged.

The Explosion of Ponzi Schemes

First, the regulatory voids and related market confusion have inevitably lured counterfeiters and Ponzi schemers. Through promises of extraordinary returns, predatory and fraudulent enterprises are ensnaring unwitting investors, and then vanish after closing the purported ICO. The unsuspecting investors are often left with very little to no possibility of recovering their hard-earned funds. As Reuters underscored:

> *...the recent flurry of ICOs raising millions of dollars has attracted some dubious business propositions and outright scams, as well as speculators looking to trade the coins for swift gains.*[19]

A chilling example comes from OneCoin, a phony India-based corporation whose claimed blockchain "consisted of little more than a glorified Excel spreadsheet and a fugazi portal that displayed demonstrably fake transactions."[20] In April 2018, Indian financial enforcement officers raided OneCoin, seizing US $2 million and arresting 18 OneCoin representatives in the process. By the time of the raid, OneCoin, which billed itself as "the next Bitcoin," had allegedly siphoned at least US

$350 million in scammed funds through a payment processor in Germany.[21]

Insufficient Data to Benchmark ICO Performance
It is fair to say that a significant portion of startups do not set out to create fraudulent ICOs. In most cases, however, ICOs are established to finance envisioned futures or imaginary ideas. Most of the cryptotokens sold to the public have no track records, no proven products and no assets on their balance sheets. This loophole was also emphasized by the German Federal Financial Supervisory Authority (BaFin), which warned consumers, "Typically, projects financed using ICOs are still in their very early, in most cases experimental, stages and therefore their performance and business models have never been tested."[22]

Without historical performance data or credible cash-flow projections, it is difficult for investors to benchmark ICO valuations. Once the ideas prove unworkable, the ICO project may have lost a significant proportion of the capital, leaving investors with no recourse. These glaring issues caught the attention of Vitalik Buterin, the cofounder of Ethereum and *Bitcoin Magazine*, who declared at the 2017 Ethereum Hackathon in Waterloo, Canada, that 90 percent of ICOs will go under.[23] This was a weighty declaration, as Buterin himself has a significant stake in the game.

Increased Complexity of Smart-Contract-Based Agreements
The majority of ICOs provide white papers and terms and conditions, articulating the underlying philosophy and formal agreement between investors and the ICO issuer, respectively. The agreements stipulated in the ICO terms and conditions are enforced by smart contracts—self-executing programs that automate the transfer of digital assets once the underlying conditions are met, without the need for a central authority. But as with any other software program, there is increased risk that the smart contract "executes prematurely because it misread the circumstances"[24] or the code may not accurately reflect the expectations of the investors. How smart contracts are coded is beyond the comprehension of several investors. Furthermore, code developers may infuse their biases into the code or unintentionally introduce flawed code. Both factors may lead to undesired or unanticipated outcomes, often to the detriment of the investor.[25]

Further compounding this complexity is the wide use of cryptojargon, some of it unfathomable, even by IT experts, such as segwit, altcoins, halving, multsig, proof of stake and an assortment of other complex lingo. Consequently, most investors cannot interpret the encoded rules and do not fully understand the implications of what they are signing and to what they are agreeing. Given these uncertainties, it is not surprising that Warren Buffet, the respected chief executive officer and chairman of Berkshire Hathaway, publicly distanced himself from cryptocurrencies, saying, "I get into enough trouble with the things I think I know something about. Why in the world should I take a long or short position in something I don't know about?"[26]

> “WITHOUT HISTORICAL PERFORMANCE DATA OR CREDIBLE CASH FLOW PROJECTIONS, IT IS DIFFICULT FOR INVESTORS TO BENCHMARK ICO VALUATIONS.”

Closing the Regulatory Loopholes

If an important lesson can be taken from history, it is this: The current irrationality and excesses of the inconsistently regulated cryptocurrency market are somewhat reminiscent of the malpractices that preceded the 2007 financial crisis. As the US government's *Financial Crisis Inquiry Report* admitted, "The crisis was the result of human action and inaction, not of Mother Nature or computer models gone haywire."[27]

The growing list of high-profile embezzlements continues to convey a steady and clear-cut message: Investors are going to take serious losses from their exposures in the ICO markets unless governments intervene. The previous brief narrative on the evolution of the US securities regulation indicates that regulators have historically enacted or tightened laws after consumers have suffered heavy losses. This ought not be the case with cryptocurrencies. Kicking the proverbial can down the road or assuming the cryptocurrency industry will proactively self-police would be naive and constitute turning a blind eye to the original intentions of cryptocurrency inventors, as discussed previously.

Enjoying this article?

- Read *Blockchain Fundamentals. www.isaca.org/*

An outright ban on ICOs may, however, be imprudent. If harnessed correctly, ICOs provide a viable alternative for startups to raise capital to fund strategic projects. As one pundit argued, "…it would be a pity if ICOs vanished as quickly as they appeared due to overregulation, as they might be very useful."[28] On the other hand, issuing veiled rebukes to celebrities represents only form, not substance. Regulators could, for instance, take a cue from Canada's Autorite des marches financiers (AMF), the financial regulator for the Quebec region. In an unprecedented 2017 move, AMF extended its regulatory sandbox to ICOs, exempting specific ICOs from strict securities registration requirements, such as issuing an investor prospectus or registering as securities dealers.[29]

Allowing ICOs to operate in a regulatory sandbox has two distinct advantages:

1. First, it provides the ICO market with a crucial opening in which to mature without stifling its potential.
2. It provides regulators an opportunity to acquaint themselves with opportunities and risk associated with this budding concept, enabling them to develop pragmatic regulations.

> "IF HARNESSED CORRECTLY, ICOS PROVIDE A VIABLE ALTERNATIVE FOR STARTUPS TO RAISE CAPITAL TO FUND STRATEGIC PROJECTS."

It is also important for regulators to enact laws that prohibit pension funds and other pools of public assets from investing in the volatile and uncertain cryptocurrencies or ICOs. If publicly owned funds take significant cryptocurrency exposures and things go awry, the ensuing hazards could badly damage economies. Similarly, boards of directors should explicitly define conditions under which their enterprises can invest in cryptocurrencies or ICOs.

Cybersecurity and Vulnerabilities

While the upsides of digital transformation to enterprises, nations and civilians are unquestionable, each nascent technology also introduces a new set of security vulnerabilities, some with implications that are not yet fully understood. This constant dichotomy continues to underscore the double-edged sword of innovation. Blockchain further complicates cyberrisk, at least in two significant ways.

The DAO Case Study: A Glimpse Into the Myth of Blockchain's Immutability

A fundamental tenet that supposedly differentiates blockchain from traditional applications is its immutability—an assumption that once transactions are appended to the public ledger and digitally time-stamped, they become persistent and irrefutable. Deleting or altering confirmed transactions becomes computationally infeasible. Traditional applications, on the other hand, function differently; their transactions can be modified, deleted or forgotten at will, and doing so requires trivial effort.

The immutability claims by the blockchain faithful have considerable merit. In addition to the vast amounts of power required to reverse transactions, blockchain uses asymmetric keys to encrypt and decrypt content, thus ensuring high levels of authentication and nonrepudiation. Furthermore, Bitcoin, the first and most successful implementation of blockchain, was proficiently designed to fend off potential attacks—so much so that, in 2013, Dan Kaminsky, a heavily credentialed security researcher who previously discovered a pervasive Internet Domain Naming System (DNS) vulnerability, confessed that he had futilely attempted to hack Bitcoin on several occasions.[30]

This widely held belief—that records affixed to blockchains cannot be reversed—is, however, a fairy tale, considering the fate of the Decentralized Autonomous Organization (DAO). The DAO, a now-defunct Ethereum-based application, was founded in 2016 as a for-profit entity that would sell tokens to investors in exchange for cryptocurrency. In return, investors would share potential profits generated by future DAO projects.[31] The DAO was an instant hit, raising more than US $150 million from more than 11,000 fanatics—approximately 15 percent of all Ether in circulation at that time.

But, in May 2016, before the DAO commenced its operations, the dreams and hopes of its investors were shattered. A hacker exploited a DAO coding flaw and drained approximately US $50 million worth of Ether into a replica of the original DAO. The value of Ether plunged. The Ethereum community had three options to resolve the theft: uphold the core principle of immutability and let the attacker walk away with the stolen funds; destroy the stolen Ether in the replica DAO, ensuring the hacker did not profit from it; or, most controversial, rewrite the Ethereum protocol and erase the theft, referred to as a hard fork.

The majority of the Ethereum community voted for a hard fork. The idea of unwinding, erasing or willfully opting out of digitally signed blockchain transactions, however, did not go down well with Ethereum purists. To them, cryptocode was law and the underlying principles of blockchain were sacred. As one expert wrote, "In the raucous arena of blockchain debate, immutability has become a quasi-religious doctrine—a core belief that must not be shaken or questioned."[32]

When compared to several other high-profile breaches, the financial value of the DAO hack paled in comparison. The consequences of the DAO breach and the resultant hard fork, however, rippled well beyond the cryptocurrency community. It prompted the SEC to investigate and issue a public report. It ignited heated debate among blockchain experts. It also incited a revolt from Ethereum fundamentalists, who chose to stick with the unadulterated version of Ethereum, now referred to as Ethereum Classic. The DAO case study provides two vital lessons.

First, the widely acclaimed theory that cryptocode can shield blockchains from human meddling is nothing more than hyperbole. As the DAO saga vividly illustrates, transactions digitally signed on a public blockchain can be manipulated by humans. To idealists, the DAO hard fork—in which two core principles of immutability and decentralized consensus were sacrificed—resembled the financial bailouts that followed the 2007 financial crisis, whereby some banks were deemed "too big to fail."

Second, blockchains have historically been widely touted as "well-protected, reliable and immutable." These supposed virtues, however, are fast becoming blockchain's Achilles' heel. They provide a false sense of invulnerability to enterprises, perpetuating indifferent attitudes toward security. By zooming into all high-profile cryptocurrency hacks, it can easily be concluded that the majority of underlying security issues are not specific to blockchain. They are the same fundamental flaws that have vexed the digital world for decades.

> "THE WIDELY ACCLAIMED THEORY THAT CRYPTOCODE CAN SHIELD BLOCKCHAINS FROM HUMAN MEDDLING IS NOTHING MORE THAN HYPERBOLE."

For instance, in early 2018, cybercriminals stole a staggering US $534 million from Coincheck, a Japan-based cryptocurrency exchange. Apparently, Coincheck's coins were accessible from the Internet, a concept referred to as "hot wallets." Coincheck also lacked multisig, the equivalent of multifactor authentication.[33] Another example comes from Mt. Gox, another Japan-based Bitcoin exchange that was bankrupted in 2014 when thieves siphoned more than US $400 million. Mt. Gox, according to several reports, had poor version control procedures and was a victim of suspected malicious insiders.[34] Using classic phishing scams—such as spoofed websites—crooks have also duped several unsuspecting individuals into divulging private keys to their digital wallets, leading to heavy losses.[35] Blockchain security problems, it turns out, are more human than technical.

Increased Attack Surface as Blockchains Interconnect With Vital Data Sources

Several use cases require blockchains to successfully integrate with existing data repositories. A case in point is smart contracts, which are self-executing digital agreements. Smart contracts, however, "live in a walled garden on the blockchain and can't fetch external data on their own."[36] To address this limitation, several enterprises are deploying smart oracles, specialized middleware applications that enable blockchains to interact with external data sources. Because of the novelty of smart oracles, which are smart contracts of sorts themselves, there are no adequately skilled developers to handle the intricacies of this technology. According research, there were only an estimated 5,000 developers dedicated to writing software for cryptocurrency by mid-2016. That number, the same research asserts, pales in comparison to the 9 million Java developers during the same time.[37] The shortage of experienced and skilled blockchain developers raises the possibility of introducing exploitable bugs or malfunctioning blockchain applications.

> "THE SHORTAGE OF EXPERIENCED AND SKILLED BLOCKCHAIN DEVELOPERS RAISES THE POSSIBILITY OF INTRODUCING EXPLOITABLE BUGS OR MALFUNCTIONING BLOCKCHAIN APPLICATIONS."

Additionally, exposing core systems to newly built blockchains also expands the cyberattack surface. It also introduces several security issues: insecure application programming interfaces (APIs), unencrypted sessions, business logic flaws, insecure endpoints, weak authentication, unprotected encryption keys and others. Blockchain implementations, therefore, demand a careful balance between interoperability and security.

Addressing Cybersecurity Matters

No framework or technology can provide impermeable defenses against cyberthreats. The right set of controls should be dictated by the value and exposure of the underlying assets. With that caveat in mind, here are five key issues enterprises should consider when embracing blockchains:

- Develop a baseline of nonnegotiable security controls and governance procedures to ensure no blockchain projects are opted out of any mandatory controls without stringent sign-offs.
- Implement robust technologies and processes to ensure cryptographic keys are protected from misappropriation or inadvertent loss. Consider storing private keys to digital wallets offline, for example, on removable USB drives, safe deposit boxes, offline hardware wallets or paper wallets. It is, however, important to emphasize that none of these will provide immunity against financial loss. For instance, while paper wallets are insulated from online attacks, they are also vulnerable to other hazards, such as fire or theft. Risk specific to each cold storage option should be carefully assessed, and appropriate mitigations should be implemented.
- Use multisignature (multisig) digital wallets, whereby two or more private keys, stored separately, are required to transfer funds from a specific address.
- Develop detailed security test scenarios and ensure that the effectiveness of each mandatory control is independently validated in a sandbox environment prior to implementation.

Impediments to Transformational Change

As with any other disruptive trend, the rise of blockchain reignites the dynamic interplay between continuity and change. Maneuvering past these constant dualities requires careful balance between innovation and business stability; neither of these two can be managed in isolation. Enterprises that blindly fight change, fail to adapt and hold on to established routines may eventually lose relevance to their customers. This risk looms larger for established players, whose market dominance is still underpinned by legacy systems and processes. According to research, incumbent firms that neglect digital innovations can experience up to 50 percent and 30 percent reduction in revenues and earnings, respectively.[38]

Unavoidably, blockchain renders a wide array of existing decentralized applications obsolete, particularly those that support back-office processes. Adding another layer of intricacy, most of these systems have operated steadily over many years and still underpin strategic revenue lines. Such is the case of the Australian Securities Exchange (ASX), which announced in 2017 plans to replace its Clearing House Electronic Subregister System (CHESS)—implemented in the 1990s—with a distributed ledger solution.[39] Architecture documentation for most of these archaic applications has not been consistently updated as businesses have been transformed and original subject matter experts have either moved on or are now deceased.

Furthermore, an enterprise's culture—"elements of social behavior and meaning that are stable and strongly resist change"[40]—can also present significant inertia to blockchain implementations as employees resist change and stick to their old ways of working. Business routines, mind-sets and norms are shaped and reinforced over years, making them harder to dislodge with the passage of time.

Response

To get past these technological and cultural hindrances to blockchain adoption, best-in-class enterprises set realistic expectations upfront when embracing blockchain. They actively resist the urge to jump into execution mode. Rather, they take measured steps and start their blockchain journey by asking hard questions, such as:

- Has the enterprise conducted an in-depth diagnosis to identify entrenched routines, bureaucracies and deep-seated interests? If yes, has the enterprise devised effective change management strategies to diffuse those cultural obstacles?
- What strategic advantages or areas of core differentiation can be amplified by embracing blockchain technologies?
- Which strategic platforms, if replaced by blockchain, lead to reduced long-term operational cost issues, increased business resilience and more scalable digital environment?
- What expertise is needed to develop required blockchain platforms, dislodge and migrate legacy applications, and interface blockchains with core applications?

Blockchain, which is still in its infancy, promises to tackle several pressing global challenges. For instance, blockchain-based smart contracts are anticipated to facilitate direct, transparent and irreversible transfer of funds from donors to those in dire need, eliminating needless intermediary costs and cutting global poverty.[41] But, if the weighty challenges explored in this article are discounted, they could undermine faith in this important technology. A leading thinker and author agrees: "If we get this wrong, Blockchain technology, which holds so much promise, will be constrained or even crushed."[42]

Endnotes

1 Nakamoto, S.; "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, *https://bitcoin.org/bitcoin.pdf*

2 Davis, J.; "The Crypto-Currency," *The New Yorker*, 10 October 2011, *https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency*

3 *Ibid*.

4 Coinmarketcap.com, "Cryptocurrency Market Capitalizations," *https://coinmarketcap.com/all/views/all/*

5 Russell, J.; "Former Mozilla CEO Raises $35M in Under 30 Seconds for His Browser Startup Brave," Techcrunch, 1 June 2017, *https://techcrunch.com/2017/06/01/brave-ico-35-million-30-seconds-brendan-eich/*

6 US Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," USA, 25 July 2017, *https://www.sec.gov/litigation/investreport/34-81207.pdf*

7 Tapscott, D.; A. Tapscott; *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin Books, United Kingdom, May 2016

8 Church, Z.; "Blockchain Explained," MIT Sloan Management School, Cambridge, USA, 25 May 2017, *http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/*

9 Deloitte, "Blockchain: Opportunities for Health Care," August 2016, *https://www.healthit.gov/sites/default/files/4-37-hhs_blockchain_challenge_deloitte_consulting_llp.pdf*

10 Marr, B.; "This Is Why Blockchains Will Transform Healthcare," *Forbes*, 29 November 2017, *https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/#4288b721ebe3*

11 Dunjic, M.; "Post-Trade Clearing & Settlement Processing Optimization: An Opportunity for Blockchain?," Medici, 3 May 2016, *https://gomedici.com/post-trade-clearing-settlement-processing-optimization-an-opportunity-for-blockchain/*

12 Depository Trust & Clearing Corporation, "DTCC Selects IBM, AXONI and R3 to Develop DTCC's Distributed Ledger Solution for Derivatives Processing," 9 January 2017, *http://www.dtcc.com/news/2017/january/09/dtcc-selects-ibm-axoni-and-r3-to-develop-dtccs-distributed-ledger-solution*

13 Mougayar, W.; *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, Wiley, USA, May 2016

14 US Securities and Exchange Commission, "The Laws That Govern the Securities Industry," USA, *https://www.sec.gov/answers/about-lawsshtml.html*

15 Investopedia, "Sarbanes-Oxley Act Of 2002—SOX," *https://www.investopedia.com/terms/s/sarbanesoxleyact.asp*

16 Clayton, J.; "Statement on Cryptocurrencies and Initial Coin Offerings," US Securities and Exchange Commission, 11 December 2017, *https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11*

17 Helms, K.; "Central Bank of Nigeria Says 'We Can't Stop Bitcoin'," Bitcoin.com, 5 May 2017, *https://news.bitcoin.com/central-bank-of-nigeria-says-we-cant-stop-bitcoin/*

18 Barsan, I.; "Legal Challenges of Initial Coin Offerings (ICO)," *Revue Trimestrielle de Droit Financier (RTDF)*, no. 3, 2017, p. 54-65

19 Irrera, A.; S. Stecklow; B. Hughes Neghaiwi; "Special Report: Backroom Battle Imperils $230 Million Cryptocurrency Venture," *Reuters.com*, 19 October 2017, *https://www.reuters.com/article/us-bitcoin-funding-tezos-specialreport/special-report-backroom-battle-imperils-230-million-cryptocurrency-venture-idUSKBN1CN35K*

20 Morris, D. Z.; "The Rise of Cryptocurrency Ponzi Schemes," *The Atlantic*, 31 May 2017, *https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/*

21 Morris, D. Z.; "The Rise of Cryptocurrency Ponzi Schemes," *The Atlantic*, 31 May 2017, *https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/*

22 German Federal Financial Supervisory Authority (BaFin), "Consumer Warning: The Risks of Initial Coin Offerings," 9 November 2017, *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2017/meldung_171109_ICOs_en.html*

23 Daniell, J.; "Ethereum's Vitalik Buterin On 'Tokens 1.0,'" ETHnews, 23 October 2017, *https://www.ethnews.com/ethereums-vitalik-buterin-on-tokens-10*

24 Hansen, J.D.; L. Rosini; C. L. Reyes; "More Legal Aspects of Smart Contract Applications," Perkins Coie LLP, March 2018, *https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2018/03/Perkins-Coie-LLP-More-Legal-Aspects-of-Smart-Contract-Applications-White-Paper.pdf*

25 *Ibid*.

26 Shen. L.; "Here's Why Warren Buffett Swears He'll Never Invest in Bitcoin," *Fortune*, 10 January 2018, *http://fortune.com/2018/01/10/bitcoin-warren-buffett-cryptocurrency/*

27 Financial Crisis Inquiry Commission, *The Financial Crisis Inquiry Report*, USA, 25 February 2011, *https://www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf*

28 *Op cit* Barsan

29 Trustnodes, "Canada Extends Sandbox to ICOs, Impak Becomes World's First Regulated Token Sale," 20 September 2017, *https://www.trustnodes.com/2017/09/20/canada-extends-sandbox-icos-impak-becomes-worlds-first-regulated-token-sale*

30 Bradbury, D.; "Security Guru Confesses, 'I Couldn't Hack Bitcoin'," Coindesk, 23 April 2013, *https://www.coindesk.com/security-guru-confesses-i-couldnt-hack-bitcoin/*

31 *Op cit* US Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO"

32 Greenspan, G.; "The Blockchain Immutability Myth," Coindesk, 9 May 2017, *https://www.coindesk.com/blockchain-immutability-myth/*

33 Buck, J.; "Coincheck: Stolen $534 Mln NEM Were Stored on Low Security Hot Wallet," *Coin Telegraph*, 26 January 2018, *https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet*

34 McMillan, R.; "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster," *Wired*, 3 March 2014, *https://www.wired.com/2014/03/bitcoin-exchange/*

35 Wieczner, J., "Hackers Stole $50 Million in Cryptocurrency Using 'Poison' Google Ads," *Fortune*, 14 February 2018, *http://fortune.com/2018/02/14/bitcoin-cryptocurrency-blockchain-wallet-hack/*

36 Bjoroy, V. T.; "Zen Blockchain Hopes to Strengthen, Broaden Bitcoin," Venturebeat, 30 September 2017, *https://venturebeat.com/2017/09/30/zen-blockchain-hopes-to-strengthen-broaden-bitcoin/*

37 Mougayar, W.; *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, Wiley, USA, 9 May 2016

38 Bughin, J.; T. Catlin; "What Successful Digital Transformations Have in Common," *Harvard Business Review*, 19 December 2017, *https://hbr.org/2017/12/what-successful-digital-transformations-have-in-common*

39 McLean, A.; "ASX Chooses Blockchain for CHESS Replacement System," ZDNet, 7 December 2017, *www.zdnet.com/article/asx-chooses-blockchain-for-chess-replacement-system/*

40 Rumelt, P.R.; *Good Strategy/Bad Strategy: The Difference and Why It Matters*, Profile Books, United Kingdom, 2011

41 Castilla-Rubio, J.C.; N. Robins; S. Zadek; "Fintech and Sustainable Development: Assessing the Implications," United Nations Environment Programme (UNEP), December 2016, *http://unepinquiry.org/wp-content/uploads/2016/12/Fintech_and_Sustainable_Development_Assessing_the_Implications.pdf*

42 *Op cit* Tapscott and Tapscott

FEATURE

Roles of Three Lines of Defense for Information Security and Governance

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2sLKf4m

Disponible également en français

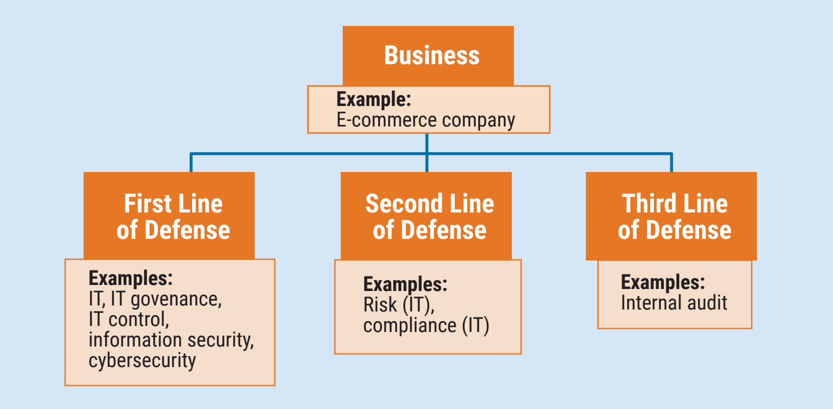
www.isaca.org/currentissue

While the three lines of defense covering assurance, governance, risk, compliance, information security and cybersecurity functions can all be working in one way or another on information security and governance, one can examine the objectives, roles and activities of these functions to explore ways to optimize outputs. Optimized outputs means the combined outputs of the various parties working on information security are maximized, which allows resources to be better deployed with increased productivity by reducing duplication.

Roles and Responsibilities of Various Functions

Organizations aim to achieve their objectives while managing risk within their risk appetites. A good governance structure for managing risk is to establish three lines of defense. Briefly, the first line of defense is the function that owns and manages risk. Within the first line of defense, businesses can set up control functions (e.g., IT control, which reports to the IT department) to facilitate the management of risk. The second line of defense is the independent control function (e.g., IT risk, IT compliance) that oversees risk and monitors the first-line-of-defense controls. It can challenge the effectiveness of controls and management of risk across the organization. The third line of defense is internal audit, which provides independent assurance. **Figure 1** provides examples of the functions under the three lines of defense.

Figure 1—Three Lines of Defense



Various business functions aim to ensure organizations are managing risk within their risk appetites. In particular, IT governance provides the consistency, processes, standards and repeatability needed for effective IT operations while monitoring the budget and compliance with regulatory and/or organization requirements. IT risk management must function as part of the enterprise risk management framework and address various types of risk and the challenges and opportunities the risk presents. It helps focus IT governance, security and privacy investments in the areas most critical to the achievement of organizational objectives. Information security aims to protect data and information systems from inappropriate access, manipulation, modification and destruction, thus ensuring systems/data confidentiality, integrity and availability. Cybersecurity, which includes technology, processes, policies and people, focuses on using business drivers to guide security activities while ensuring that cybersecurity risk factors are included in the organization's risk management processes.[1]

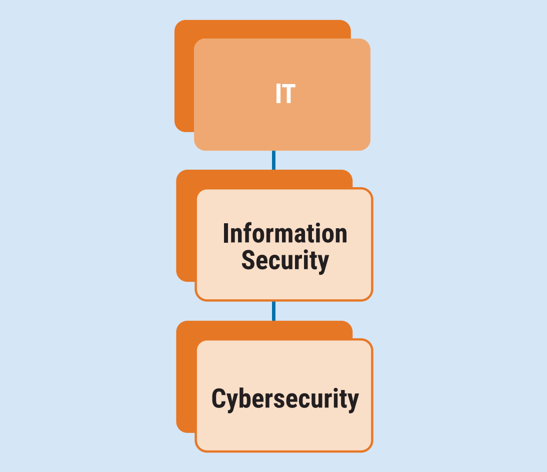
The assurance function is internal audit, whose mission can be defined to enhance and protect organizational value by providing risk-based and objective assurance to evaluate the effectiveness of governance, risk management and control processes.[2]

Amelia Ho, CISA, CISM, CA, CFE, CIA, CISSP, FRM, PMP
Is a senior vice president with Citibank and has more than 20 years of experience in the financial services industry in a number of internal audit, risk management and compliance roles. She has contributed to ISACA as an article author and expert reviewer of ISACA publications. She is the recipient of the 2013 Ted Keys Honorable Mention Award for her article "Emerging Risk Audits" in *Internal Auditor* published by The Institute of Internal Auditors.

Organization Structure of Various Functions

Different teams can be organized in various ways, as shown in **figures 2** and **3**. **Figure 2** illustrates how the IT risk, information security and cybersecurity teams can be organized in a hierarchical way. Under this organizational structure, there is less chance that their tasks/activities are duplicated because cybersecurity is within information security, which means the latter is fully aware of the former's activities and role. **Figure 3**, on the other hand, is an example of IT risk, information security and cybersecurity teams organized in a flat structure, as counterparts of each other. With this kind of organizational structure, there is a higher chance that their activities will overlap because the different teams may not be aware of what each other is doing. For instance, the information security team can be reviewing information security settings and controls over all operating systems, whereas the cybersecurity team can be reviewing web server settings and controls that may cover the same server. Another example may be information security being responsible for disaster recovery planning or service level management, while the cybersecurity team is responsible for addressing denial-of-service (DoS) risk; whereas, disaster recovery and service level management are controls to address DoS risk.

Figure 2—Hierarchical Organization Structure



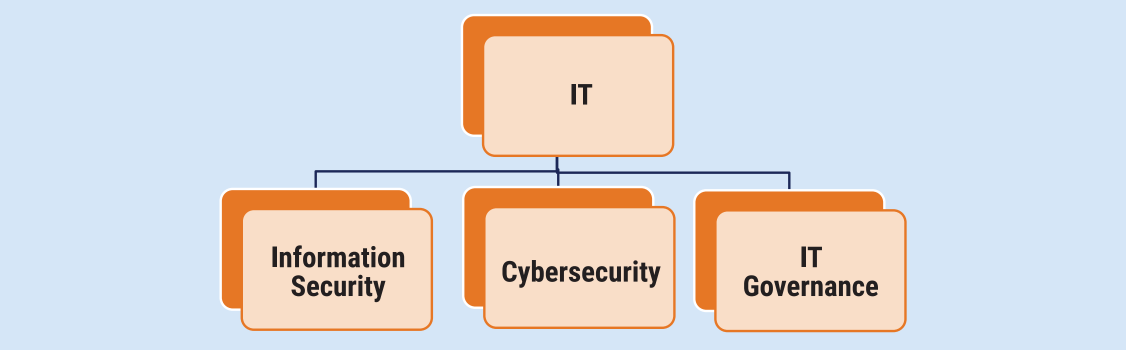
Activities of Various Functions and/or Three Lines of Defense

To achieve the organization's ultimate goal of managing risk (e.g., information and technology risk) within its risk appetite, various business functions and/or the three lines of defense have to perform activities such as information gathering, risk assessment, reviews, analysis, reporting and monitoring of risk that may be common among the three lines. One way to find out these commonalities is through frequent communication, which facilitates information sharing. To facilitate communication and discussion of risk within an organization, different business functions can use the same set of risk categories and taxonomy.

Sharing of Inputs

Various business functions working on IT risk can share useful internal information such as source information (e.g., transaction data), risk information (e.g., trends or statistics such as web application availability percentage) and internal loss data (e.g., IT security incidents including details and/ or nature of incidents). Through the sharing of

Figure 3—Flat Organization Structure



internal information, business functions can fulfill their duties by conducting respective analysis, risk assessment and monitoring, and control review planning (e.g., compliance or audit planning).

Also, information can be shared within the industry through an external loss database, just as ORX stores loss data for the banking and insurance industry. Through the sharing of external risk information, various business functions can be better informed on how to detect and prevent similar risk. For example, in 2016, there was an unauthorized money transfer request through Bangladesh Bank,[3] detected by one of the routing banks that flagged the transaction for further review solely because of the misspelled word "fandation," which resulted in the transfer being stopped.

> “THROUGH THE SHARING OF EXTERNAL RISK INFORMATION, VARIOUS BUSINESS FUNCTIONS CAN BE BETTER INFORMED ON HOW TO DETECT AND PREVENT SIMILAR RISK.”

Information can also be shared within a country. For instance, Cyber Security Information Sharing Partnership (CiSP)[4] of the United Kingdom is a joint industry/government initiative set up to exchange cyberthreat information in real time in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK organizations. Information can also be shared among countries. For instance, there is intercountry sharing such as the Asia Pacific Computer Emergency Response Team (APCERT) to encourage and support cooperation among national CERTs in the Asia Pacific (APAC) region. APCERT maintains a trusted network of computer security experts in the APAC region to improve the region's awareness and competency in relation to computer security incidents.[5]

Sharing of Processing

Besides sharing of inputs, processing can also be shared. Different functions may be using tools to develop monitoring measures for preventive and/or detective purposes. Sharing these tools can reduce duplication of work among various teams. For instance, either the first or second line of defense may be adopting regtech (an application of technology to ensure compliance with the latest requirements from regulators and/or the company) or using machine learning to detect distributed DoS (DDoS) attacks based on detection of similar past patterns of DDoS. Tools developed by the first line can be used by the second line and vice versa. Internal audit can develop automated scripts to perform testing or continuous auditing (e.g., use of bots to go to service providers' websites to check whether the latest system patches or virus signatures are used by the organization), which can also be used by the first or second line of defense for continuous monitoring purposes.

Sharing of Outputs

Results of reviews conducted by one party can be shared. For instance, the first line of defense can conduct a self-check of adherence to the Hong Kong regulators' (Hong Kong Monetary Association) e-banking guidelines for compliance management; the second line of defense can use this self-check for regulatory reporting.

Another example is the governance function. The second and third lines of defense can use the first line's exception reporting and/or third-party (e.g., regulator or external auditor) control review results for identification of systemic issues. The third line can also use the first or second line's control review results for assessing the effectiveness of the first and second lines of defense.

Work of the Assurance Function

While the reviews performed by the assurance function can be similar to those conducted by the first or second lines of defense, only the internal audit department or external service providers can provide the required assurance because they are functionally independent from the business and have reporting lines and a mandate that differs from those of the first and second lines of defense. Hence, audit teams need to conduct certain work to evaluate the effectiveness of governance, risk management and control processes.

There are various reviews that can be conducted by audit teams. If the audit teams conduct re-performance, it is not economical because it duplicates efforts by re-performing a control such as checking extracting sampled emails to identify any unencrypted customers' personally identifiable information (PII) or independently checking the accuracy of processing by the company's application. Even if the audit team re-performs a control, such as application control, for the first year, audit can nonetheless reduce the extensive control re-performance work in a subsequent year (hence saving time and effort while achieving the desired assurance) by performing other tests such as change management controls or a check of the last date of change to see if any change has been applied since the last audit, when the re-performance test was conducted to confirm accurate processing of the company's application.

> “THE AUDIT FUNCTION'S APPROACH TO, AND AMOUNT OF, CONTINUOUS AUDITING DEPENDS ON THE EXTENT TO WHICH MANAGEMENT HAS IMPLEMENTED CONTINUOUS MONITORING6 AND ITS EFFECTIVENESS.”

Audit can also perform continuous auditing to provide assurance on a more timely basis, based on a bigger data population being tested. However, the scope of continuous auditing can potentially be reduced if management has implemented similar and effective continuous monitoring. There is an inverse relationship between the adequacy of management's monitoring and risk management activities and the extent to which auditors must perform detailed testing of controls and assessment of risk. The audit function's approach to, and amount of, continuous auditing depends on the extent to which management has implemented continuous monitoring[6] and its effectiveness.

Economic Allocation of Resources

If a business function lacks the resources to perform the required tasks, it can consider obtaining the resources internally. For instance, IT's Sarbanes-Oxley Act (SOX) testing can be conducted by internal resources such as the internal audit/compliance/risk team, depending on which team has the required resources, as all functions meet the requirements for performing SOX testing.

For regulator-mandated reviews that require an independent party to conduct, an organization can

choose internal resources with adequate skills for fulfilling the requirement because internal resources are usually less costly than external resources. If internal resources do not have the requisite skills/tools (e.g., penetration tests or ethical hacking) and cannot provide the required assurance, then external resources should be hired, irrespective of the relatively higher costs involved.

Conclusion

When examining the roles and objectives of the three lines of defense covering assurance, governance, risk, compliance, information security and cybersecurity, there can be common or overlapped activities. A hierarchical organization structure can reduce the chance of duplicated tasks/activities among functions or teams because each team is more aware of the role and activities of the other teams within the hierarchical structure. Another way to optimize outputs and save resources and costs for the organization is to share inputs, processing and outputs of various business functions and teams (including output of industrywide and countrywide public or nonprofit organizations), which can be used to streamline each function's activities.

The assurance function, however, can be delivered only by independent parties such as the internal audit team and external providers. Internal resources would be less costly than external resources, but the former may not have the required resources to conduct certain tasks. For these cases, external service providers may be required despite the relatively higher costs involved to ensure the required assurance is provided.

Author's Note

Opinions expressed in this article are the author's and do not necessarily represent the views of Citibank.

Endnotes

1 Lainhart, J W.; Z. Fu; C. Ballister; "Holistic IT Governance, Risk Management, Security and Privacy: Needed for Effective Implementation and Continuous Improvement," *ISACA® Journal,* vol. 5, 2016, *https://www.isaca.org/Journal/archives/Pages/default.aspx*

2 The Institute of Internal Auditors, "Supplemental Guidance, Model Internal Audit Activity Charter," 2017, *https://iia.no/wp-content/uploads/2017/04/2017-SG-Model-Internal-Audit-Activity-Charter.pdf*

3 Schwartz, M.; "Bangladesh Bank Hackers Steal $100 Million," Bank Info Security, 10 March 2016, *https://www.bankinfosecurity.com/bangladesh-bank-hacers-steal-100-million-a-8958*

4 National Cyber Security Centre, Cyber Security Information Sharing Partnership, 20 March 2018, *https://www.ncsc.gov.uk/cisp*

5 Asia Pacific Computer Emergency Response Team, *https://www.apcert.org*

6 Coderre, D.; "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment," The Institute of Internal Auditors, 2005, *https://www.iia.nl/SiteFiles/IIA_leden/Praktijkgidsen/GTAG3.pdf*

Getting the Basics of Cybersecurity Right

Security professionals understand and acknowledge that there are a myriad of challenges facing cybersecurity teams today. However, not all challenges are relevant to all organizations at any given time. It is important to understand what the real challenges are for the vast majority of cybersecurity teams and chief information security officers (CISOs) as opposed to the challenges that are faced by the minority of cutting-edge organizations. This article discusses some conclusions about the relevance of challenges based on the author's experience in addition to efforts in the social media realm. These conclusions come from an ongoing exchange of experiences and opinions with peers from various sectors, industries, geographies and organizations of all sizes and maturity levels. As obvious as these conclusions may sound, many articles on cybersecurity seem to be unaware of them. Many articles seem to address high-profile organizations that are far from representative of most organizations. The conclusions discussed herein can be applied to the vast majority of organizations. The points that follow are closer to a written mind map rather than a formally structured framework.

Affording Security Technology

Leaving aside cutting-edge or high-risk-profile organizations, critical service providers and other, similar businesses, the following lessons appear to be true:

- **Organizations buy the technology they can afford**—That is the reality. Technical features are good to know and technological fit into the organization's IT landscape may be a weighing factor, but, at the end of the day, the money available to spend on a firewall, security information and event management (SIEM) system, data loss prevention (DLP) system, or any other security control is, in the vast majority of cases, the single most influential criterion used to make the decision. This is primarily because there should be an inevitable proportionality between the value of the assets the organization intends to protect and the cost of the resources the organization devotes to actually protect them. More than the technology itself, it is likely that the organization's chief restriction is the price it can pay for technology, and that is strictly related to the value of the assets it is protecting (**figure 1**).
- **The vast majority of organizations are not ahead of the market**—They either represent "the market" or are behind the market. So, while certainly there are debates on the limitations of the technology currently available in the market to prevent, protect, detect and respond to cyberattacks, and discussions as to where artificial intelligence will

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

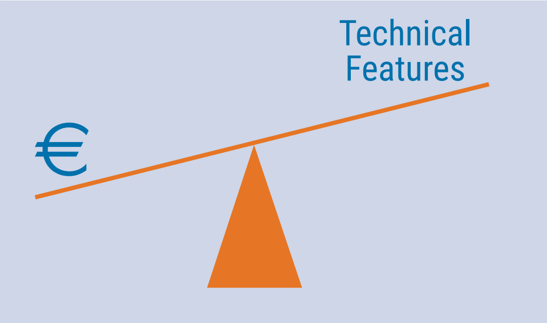
https://bit.ly/2sJvizH

Ramón Serres, CGEIT, CISM, CSX Fundamentals, CCSK, CISSP
Is an industrial engineer with a long career in IT and a passion for information security and risk management. After being a management and e-business consultant in his early years, he has held several management positions in consumer goods and pharmaceuticals. Over the last few years, Serres has successfully led a transformational project in his current company, bringing the information security function to the business and the C-level and pushing the organization to a higher maturity level.

Enjoying this article?

- Read *A Risk-Aware Path to Cybersecurity Resilience and Maturity*. *www.isaca.org/CMMI-Cyber-Capability-Maturity*
- Learn more about, discuss and collaborate on it cybersecurity in the Knowledge Center. *www.isaca.org/cybersecurity-topic*

Figure 1—Cost vs. Technical Features



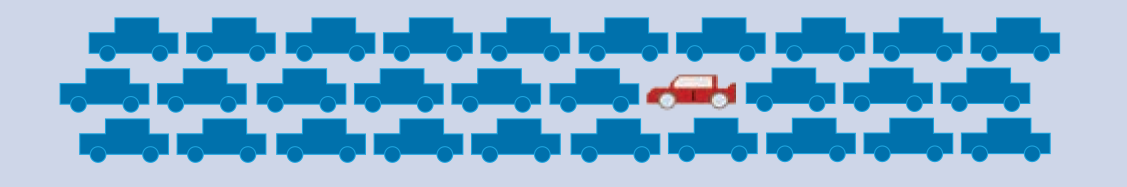
lead, those conversations actually apply to a very limited minority. In global terms, by remaining grounded, it becomes clear that the limitations current technologies may have are likely a problem for a very small minority. Most organizations are not in that elite class. It can be likened to commenting on the possible defects of a McLaren, while the truth is most will actually be driving a Volkswagen. **Figure 2** shows this in further detail.

The majority of organizations can definitely do with the technology that is available. The real challenges remain in the basics around having those technologies in full operation.

- **Senior management lives far away from the frameworks, methodologies, maturity models, standards and other tools of the cybersecurity trade**—ISACA® frameworks and good practices, the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the International Organization for Standardization (ISO) with all its recommended controls, and other relevant standards/guidance are valuable assets indeed, but the bridge between these frameworks and senior management needs to be built. The most common reality is that in virtually all domains, it is not unusual to find, not a big gap, but an ocean of gaps between what good practices recommend and what really happens. Most organizations use a security framework more as an inspiration, guideline or stimulating target, rather than a real objective, unless a stakeholder actually manages to clearly demonstrate the relevance of those frameworks and controls to the particular business and its particular senior management. It is crucial to think thoroughly about the controls to implement and the relevance they have to the business.
- **Organizations know what needs to be done**—Thanks to all the good advice that circulates—even from before the Wannacry attack, but particularly after high-profile breaches that are becoming more frequent—and the beautifully formatted presentations, infographics and other communication tools, organizations know what to do. Most readers have seen dozens of pictures with the key messages: Patch, invest in detection and prevention, gain resilience. What to do is known to most practitioners and organizations. What most do not know is how to do it because there is a major step between the goal (e.g., the systems must be patched) and its realization (e.g., actually patching the systems). The challenge has a lot to do with organization, definition of responsibilities, service level agreements (SLAs), managing people, etc.

In this general context, much of the cybersecurity content that goes around in specialized blogs and magazines could be considered as missing the point, as it would apparently seem that missing extra features in the current technology and getting even more advanced features are the most common problems organizations face when, in fact, they are not.

Figure 2—Is Individual Reality Representative of a Majority or of an Elite Class?



The Real Challenge

Basic cybersecurity recommendations that appear in many sources are fine and sufficient for most organizations, but the challenge remains in how to do it, how to get things done. Organizations struggle to get things done.

Having a third party scan the organization's network to find vulnerabilities; check controls to see which ones are missing; point at the network's, systems' and applications' weaknesses; and interview key stakeholders to complete the picture is relatively easy, particularly on the most technical part, as the available tools are effective.

Translating all those weaknesses and vulnerabilities into a program that makes sense to that particular business is a key challenge. The program will be a set of activities and projects, some of them performed as a sequence, some of them in parallel. Again, this is relatively easy, particularly if there is no particular commitment as to the feasibility of the deadlines.

Building a Simple Model

This leads to a very simplistic model where there is, on the one hand, the implementation and deployment of new solutions, whatever they are (based on technology, people, processes or organization) and, on the other hand, the business as usual, the operations.

The implementation and deployment of new solutions refers to new projects, which can tackle any domain of information security: a new regulatory framework, a new security architecture design, the implementation of a new perimeter firewall, a DLP system, a cloud access security broker (CASB), an identity and access management (IAM) process, a SIEM, etc. Something new. Something the organization did not have previously that now must be implemented and set in operation.

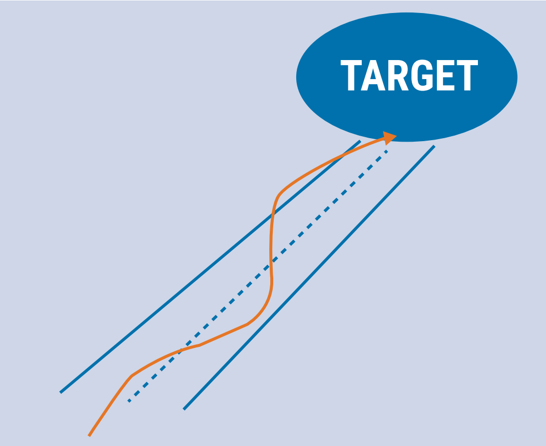
The reference to business as usual points to all security operations: alert monitoring, systems adjustments, policy compliance monitoring, incident response, security reporting, etc. All new systems, projects and solutions end up adding new tasks to the business-as-usual side.

> "BASIC CYBERSECURITY RECOMMENDATIONS THAT APPEAR IN MANY SOURCES ARE FINE AND SUFFICIENT FOR MOST ORGANIZATIONS, BUT THE CHALLENGE REMAINS IN HOW TO DO IT, HOW TO GET THINGS DONE."

Governance

All these projects and business-as-usual activities should be done under a certain direction—knowing why things are being done; knowing that what is being done is good for the organization's goals; and knowing that these activities are consistent with a well-defined direction that has not been laid down as a result of improvisation, but formally by the organization's senior management. This all can be described extensively in processes and concepts, but it all comes down to one single word: governance. As **figure 3** shows, deviations should progress toward the end target.

Figure 3—Deviations Along Project Execution



In addition to the most accurate definitions of the term “governance,” it is important to stress that governance is, among other things, about setting direction. In the course of managing projects and operations, addressing deviations to the plan, handling unplanned obstacles, and making constant decisions, governance is what enables consistency with the set direction and the avoidance of drift.

Governance provides the guidance that is necessary to enable proper decision-making regarding what to do, what to postpone, what risk to accept and what risk factors to mitigate. Too often, when reflecting on why an IT team did this or that, it is easy to come to the conclusion that the decision was made on technical criteria rather than based on risk. Therefore, there has to be an explicit effort to embed risk management in cybersecurity decisions so that decisions are determined by risk over other criteria such as technology. Of course, it must be acknowledged that economic factors compete as equals with risk factors, when it comes to being the basis for cybersecurity decisions.

> “IN ADDITION TO THE MOST ACCURATE DEFINITIONS OF THE TERM “GOVERNANCE,” IT IS IMPORTANT TO STRESS THAT GOVERNANCE IS, AMONG OTHER THINGS, ABOUT SETTING DIRECTION.”

An Operating Model

Once the plan is properly defined, getting activities done on the project level and running security as a business-as-usual activity are matters of defining an operating model. Again, managing it is not really a matter of having cutting-edge technology nor of developing a technology that is ahead of what the market can offer. On the contrary, above all, several disciplines or domains stand out as much more important than the technology itself.

A complete operating model may be sensibly built on ITIL. Nevertheless, for those organizations that cannot afford to go for such a complete model, the following guidance may be useful:

- **People**—Managing security is about managing people: leading a team; organizing people; and conveying clear messages as to the priorities, mission, general criteria and guidance that should steer all decisions in which the leader will not be directly participating. For those decisions that are delegated across teams and service providers, to be consistent, the mission and vision should be clearly stated and effectively communicated. Another thing relating to people is motivation. The leader must keep up the motivation and convey a challenging future that engages a team that will, in many cases, cover a 24/7 service and, in the event of a severe incident, will stay awake long hours doing forensics, hunting threats and monitoring the network at an inch-by-inch level.
- **Processes**—Even at different maturity levels, all organizations need to have clear processes. If the right context and culture are in place to create a perfectly defined organization, then processes, their inputs and outputs, their activities, and their measurement will need to be defined in a formal way. If the organization’s context, culture or size does not fit with a formal definition, then an effort should be made to implement a process-like organization that enables the organization to work as smoothly as possible.
- **Roles and responsibilities fall somewhere in between processes and people**—They define who does what and the more concrete, the better. This is especially important when various teams are involved such as security operations, infrastructure management, enterprise architecture and service management. This becomes not only important, but critical, when various service providers interact with each other. The organization should face the definition of responsibilities at the earliest possible stage. The sooner the potential conflicts are identified, the sooner a solution can be devised, which, in most cases, will be a compromise. Blurred, unclear or informal definitions of roles

and responsibilities are bound to be a problem. And, if the organization has to manage a security incident, which, unfortunately, is likely, an unclear definition of responsibilities will explode.

- **Internal regulatory framework**—That is, the organization's information security policy and related documents, whatever they are: guidelines, standards, baselines, procedures. It is worth dedicating time to creating these documents to suit the organization rather than just downloading a policy from the Internet. The regulatory framework has to be tailored to the organization's particular context, size, culture and, most important, risk map. There are often many stakeholders that have a say in elaborating an information security policy: IT, legal, human resources, information security, even finance. But once it is all written, some time should be devoted to gaining explicit approval and endorsement from senior management. This may take time, some explanation and some minor changes, but it will pay off because a proper regulatory framework will enable further security-project-related decisions that come as a consequence of what is stated in the policy.

Conclusion

Managing cybersecurity or, more specifically, managing cybersecurity risk, is much more than just technology and, in most cases, has nothing to do with having the money to afford state-of-the-art technology.

> "MANAGING CYBERSECURITY OR, MORE SPECIFICALLY, MANAGING CYBERSECURITY RISK, IS MUCH MORE THAN JUST TECHNOLOGY AND, IN MOST CASES, HAS NOTHING TO DO WITH HAVING THE MONEY TO AFFORD STATE-OF-THE-ART TECHNOLOGY."

Managing cybersecurity risk is generally a matter of acquiring affordable technology and, above all, getting the basics right: managing people, processes and organization, and setting up governance and operational models that work. This is easily said but is a big challenge by itself, particularly in larger organizations where several teams and service providers are involved, each of them with a specific service level agreement. The more pieces in the puzzle, the more complex it becomes. And the reality will prove that defining roles and responsibilities, processes and organization will turn out to be more important than what particular technical feature has the last next-generation firewall acquired by the organization.

There is no magic solution, nor a single approach that fits all. Knowing the organization, the particular industry in which it operates, the risk and the resources will result in a better position to develop the right solution.

FEATURE

Data Governance From the Actuary and Risk Management Perspectives

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2Jgt55L

Considering the practices and current and future legislation in Turkey and around the world, the Solvency II framework[1] and new International Financial Reporting Standards (IFRS) regulations[2] (especially IFRS 9 and IFRS 17) are areas where there has been discussion recently from the actuary and risk management perspectives as well as the data dimension. Given that the framework and regulations are data-focused, and the right way to apply them depends on data quality, the importance of data governance can be seen. **Figure 1** summarizes the framework and regulations.

Considering the responsibilities of actuary and risk management functions within the Solvency II framework and IFRS regulations, and risk managers' general job description, the quality of the data used for all calculations, modeling and reporting is very important and critical to outcomes. Since the data used for calculations, modeling and reporting are kept on information systems in all institutions, ensuring data quality is mainly the data owner's job, but the IT department is also responsible because it retains the data.

Figure 1—Solvency II and IFRS 9 and 17

Solvency II	IFRS 9	IFRS 17
This is a regulatory framework that defines the methods related to the capital amount required to be set aside to manage the risk insurance companies assume and risk resulting from the nature of their work.	This is a financial reporting standard that guides the classification and measurement of financial instruments, financial assets and liabilities, and hedge accounting, and their removal from the balance sheet.	This is a financial reporting standard that guides the accounting of insurance and reassurance agreements.

Actuaries and risk managers, the parties who use the data produced by the business functions and employ the data to produce new data, are indirectly responsible for assessing and questioning data quality. Their responsibilities continue as data owners when they create, model and report the data.

Since data are created, processed, kept, reported and archived in a distributed way in information systems (i.e., applications, databases, data warehouses and spreadsheets kept in file servers) and in processes and used for different purposes such as product management, policy production, claims, accounting and legal activities, data governance on a corporate level becomes very important from actuary and risk management perspectives. Because data may be created internally and/or obtained externally, and external stakeholders in the insurance sector are varied and include sector and economic data providers as well as agencies, service organizations and lawyers, the need for ensuring data governance rises.

From the risk management perspective, the need for data governance exists not only in the insurance sector, but also in all sectors affected by IFRS regulations. Complex information systems structures increase the need for data governance. These structures are composed of expert/source systems and accounting/reporting systems, peripheral systems for data management and reporting positioned around these systems, as well as interfaces and integrations ensuring the proper functioning of these systems.

Data governance comprises a holistic management system that describes, coordinates and manages

Mehmet Zeki Önal, CISA, CRISC, CGEIT, CCSA, CRMA
Is a senior manager in Risk Assurance Services at PricewaterhouseCoopers Turkey. He is experienced in assurance and consultancy projects related to IT processes in financial and nonfinancial companies. He has participated in assurance, compliance, review and gap analysis engagements, as well as improvement, optimization, design, transformation, readiness and implementation engagements regarding local and global frameworks, standards and regulations. He has experience in IT governance, IT strategy, IT transformation, IT reorganization, IT cost management and cloud computing risk management. Additionally, he has experience in performance assurance topics such as vendor and system evaluation and selection and third-party assurance.

how data move in the organization, responsibilities and data flows, and all risk and actions related to data. Therefore, data from different sources can be managed in line with the organization's needs on the corporate level, using holistic and coordinated approaches.

Data that must be kept, processed and reported differently to meet the requirements of the Solvency II framework and IFRS regulations must comply with this framework and these regulations. In addition, a robust data governance structure must be created to meet all the organization's business and technological needs related to data.

One of the important frameworks guiding organizations in relation to data governance is the COBIT® 5 framework for the governance and management of enterprise IT (**figure 2**),[3] which aims to manage all IT on a corporate level in a way that adds value.

Figure 2—COBIT 5

COBIT 5
A set of principles, practices and models to set up, operate and manage information and technology structures and processes that comply with organization targets and business requirements.

The COBIT 5 framework guides the building of IT processes and structures at the corporate level in line with good practices. In this framework, data governance is handled across the organization within the framework of these processes and structures. Since data are considered to be important sources in all business and IT functions (as inputs, as parts of the process, and as outputs), IT processes and structures defined within the COBIT 5 framework have been built from this perspective.

The following parts of the COBIT 5 framework are examples of important process descriptions, management practices and activities from the data governance perspective where they mention the importance of data, information and knowledge. These selected processes, practices and activities explain the core objectives or expectations of the COBIT 5 framework from the data governance perspective and the use of data, information and knowledge in IT governance from the effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability perspectives:

"SINCE DATA ARE CONSIDERED TO BE IMPORTANT SOURCES IN ALL BUSINESS AND IT FUNCTIONS (AS INPUTS, AS PARTS OF THE PROCESS, AND AS OUTPUTS), IT PROCESSES AND STRUCTURES DEFINED WITHIN THE COBIT 5 FRAMEWORK HAVE BEEN BUILT FROM THIS PERSPECTIVE."

- **APO01 Manage the IT management framework: APO01.06 Define information (data) and system ownership**—Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners make decisions about classifying information and systems and protecting them in line with this classification.
- **APO03 Manage enterprise architecture**—Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realizing enterprise and IT strategies.
- **APO13 Manage security**—Define, operate and monitor a system for information security management.
- **BAI02 Manage requirements definition**—Identify solutions and analyze requirements before acquisition or creation to ensure that they are in line with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services.
- **BAI03 Manage solutions identification and build**—Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.

Enjoying this article?

- Read *Getting Started With Data Governance Using COBIT® 5.* *www.isaca.org/data-governance-cobit-5*
- Learn more about, discuss and collaborate on information risk management in the Knowledge Center. *www.isaca.org/risk-management*

- **BAI07 Manage change acceptance and transitioning**—Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post-implementation review.
- **DSS01 Manage operations: DSS01.01 Perform operational procedures—activity 3**—Verify that all data expected for processing are received and processed completely, accurately and in a timely manner.
- **DSS04 Manage continuity: DSS04.03 Develop and implement a business continuity response—activity 4**—Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity.
- **DSS04 Manage continuity: DSS04.07 Manage backup arrangements**—Maintain availability of business-critical information.
- **DSS05 Manage security services**—Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy.
- **DSS06 Manage business process controls: DSS06.02 Control the processing of information**—Operate the execution of the business process activities and related controls, based on enterprise risk, to ensure that information processing is valid, complete, accurate, timely and secure (i.e., reflects legitimate and authorized business use).

When these practices, processes and activities mentioned in the COBIT 5 framework are evaluated, the importance and criticality of data quality can be seen in every phase, from planning to acquiring, from building to operating, and from managing to monitoring the IT function that adds value to business processes and the organization. Thus, important steps to be taken in the IT environment are becoming more obvious to ensure data quality. As a result of managing data in line with the data-related requirements defined in the COBIT 5 framework, IT structures will serve for calculating and reporting from the actuary or risk management perspectives in addition to financial reporting in a robust way. Additionally, it is possible to build a data governance structure at the corporate level that will support analytic work. This analytic work will add value to business processes and organization and accomplish various aims.

After building an efficient data governance system, structures such as an information security management system (ISMS)[4] and business continuity management system (BCMS)[5] based on the relevant International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards can be built in a way that meets the organization's needs regarding data security and continuity and is in line with the global standards. Similarly, although the Communiqués on Information Systems Management and Independent Audit published by the Capital Markets Board of Turkey[6, 7] do not require certification of compliance with the mentioned standards, they demonstrate the requirements and the expectations related to these subjects.

In addition to operational requirements and reporting requirements, local and global legislation on data protection, such as Turkish Personal Data Protection Law[8] and the EU General Data Protection Regulation (GDPR),[9] also require the implementation of steps for data governance processes; thus, they accelerate and guide the related processes.

Consequently, data governance is becoming more important from the actuary and risk management perspectives, and the need for organizations to develop an approach that considers legislation and regulations related to this issue has arisen. In this regard, the COBIT 5 framework offers a data governance approach to guide organizations.

Therefore, it is advisable that a data governance structure be built, and data ownership, responsibilities and criteria be determined to meet direct and indirect requirements defined in the Solvency II framework and IFRS regulations in a way that complies with the COBIT 5 framework's data governance requirements and covers all stakeholders. The current data governance approach should be revised accordingly and current data should also be tackled and reorganized under this approach. Meanwhile, other compliance and organization targets must be taken into account and compliance must be ensured at the corporate level.

> “DATA GOVERNANCE IS BECOMING MORE IMPORTANT FROM THE ACTUARY AND RISK MANAGEMENT PERSPECTIVES, AND THE NEED FOR ORGANIZATIONS TO DEVELOP AN APPROACH THAT CONSIDERS LEGISLATION AND REGULATIONS RELATED TO THIS ISSUE HAS ARISEN.”

Endnotes

1 European Insurance and Occupational Pensions Authority, "Solvency II," *eiopa.europa.eu/regulation-supervision/insurance/solvency-ii*

2 International Financial Reporting Standards, List of IFRS Standards, *www.ifrs.org/issued-standards/list-of-standards/*

3 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/cobit/pages/default.aspx*

4 International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements*, 2013, *www.iso.org/standard/54534.html*

5 International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 22301:2012, *Societal security—Business continuity management systems—Requirements*, 2012, *www.iso.org/standard/50038.html*

6 Capital Markets Board of Turkey, Bilgi Sistemleri Yönetimi Tebliği, Turkey, 2018, *mevzuat.spk.gov.tr/*

7 Bilgi Sistemleri Bağımsız Denetim Tebliği, Turkey, 2018, *mevzuat.spk.gov.tr/*

8 Personal Data Protection Agency of Turkey, Personal Data Protection Law, Turkey, 2016, *www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.6698&MevzuatIliski=0&sourceXmlSearch=6698&Tur=1&Tertip=5&No=6698*

9 European Parliament, General Data Protection Regulation, 2016, *gdpr-info.eu/*

Using Audit Tools to Support Strategic Objectives

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2kQRy6U

Organizations that seek excellence tend to maintain a sharp focus on their strategic objectives. Information systems (IS) auditors who wish to add value to their organizations—and surely that is all of them—should do the same.

There are two phases of the audit process where IS auditors can leverage tools to make their work align to and support the organization's strategic objectives.

Planning Phase—Being Alert to Organizational Changes

The planning phase of the IS audit should consider both organizational objectives and engagement-specific issues.[1] The engagement-specific issues relate to systems, applications or processes that support the organization's existing processes as well as new initiatives. In determining whether to assess these matters, IS auditors evaluate the potential increase in risk or the introduction of new risk to the organization. Consideration of risk-based matters is a cornerstone of audit planning, but real value is added when IS auditors are alert to strategic initiatives, then leverage audit planning to ensure continuous alignment of the IS audit function's efforts with the organization's strategic objectives.

Robin Lyons, CISA, CIA
Is a technical research manager in ISACA's Knowledge and Research department. In that role, she contributes thought leadership by generating ideas and deliverables relevant to ISACA's constituents. She partners with Learning Solutions as a subject matter expert on audit and CSX-related projects. She also writes audit programs, narratives and blogs as well as leads projects when any of these functions are co-sourced with external resources. Prior to joining ISACA, Lyons was a Payment Card Industry (PCI) subject matter expert for a Fortune 200 corporation, and the internal audit director for an institution of higher education.

In most instances, IS auditors' direct involvement in organizational progress toward strategic objectives means evaluation outside the scope of a planned audit. Creation of a specific project around the organization's new initiative relies on skills auditors use routinely; however, the approach to the deliverable is different. Unlike an audit, where a report signals the end of an effort, participation in a strategic initiative requires IS auditors to assess and report on a repeat basis. Given the ongoing nature of this work, a supporting tool can prove helpful.

Informal tracking of the project can be done through readily available tools such as Microsoft Word and/or Excel, and that level of tracking may be adequate, depending on the organization. However, because strategic projects generally have higher visibility within the organization, IS auditors should explore tools that better support centralization of project data and reporting. An example of such a tool is open-sourced Eramba *(www.eramba.org/)*.

In addition to modules that document organizational structure, assets and controls, Eramba offers several modules that can be used to track IS auditors' strategic initiative efforts. For example, in Eramba's Risk Management module, there is a business impact analysis component that supports documentation of the revenue associated with each project risk. Going beyond simply identifying a risk (during audit planning) to monitoring and reporting customized, specific information on that risk enables IS auditors to add value to the organization.

Recommendations and Remediation Phase—Understanding and Innovating

Having identified areas of concern during fieldwork, IS auditors can proceed to making recommendations and tracking progress toward resolution (remediation), remaining mindful to maintain independence. ISACA's Information Technology Assurance Framework™ (ITAF™) notes that as long as management retains responsibility for oversight and results of services, the IS auditor's independence should not be impaired.[2] Notwithstanding the need to maintain independence, the recommendation and remediation phase is the IS audit function's opportunity to reinforce its trusted advisory/consultative role to the organization.

> "WHILE INNOVATION DEPENDS STRONGLY ON CULTURE AND MINDSET, IT CAN BE HELPED ALONG WITH THE APPROPRIATE TOOL."

Interacting with most, if not all, groups throughout the organization places IS auditors in the unique position of having a comprehensive view of the organization's people as well as its processes (technological and nontechnological). This insight can, and should, be leveraged to make innovative audit recommendations. "Innovative" is the key word; the recommendations must be progressive and look to the future, even when they are addressing deficiencies that occurred because of past practices. For example, a few years ago, when employees started using personal devices at work and kick-started an *ad hoc* bring-your-own-device (BYOD) approach, some IS auditors recommended that their organizations design and launch policies to prohibit BYOD. A more innovative recommendation examined how employees use mobile devices and determined how the IS audit function could collaborate with the organization to address concerns around securing devices while supporting employees' workstyles.

While innovation depends strongly on culture and mind-set, it can be helped along with the appropriate tool. For example, an exception tracking tool can support the IS audit function's ability to expend resources and time more efficiently, thereby enabling a focus on crafting innovative recommendations.

MantisBT *(www.mantisbt.org/)* may serve that need by allowing users to document the following features for each audit recommendation—category, severity, status and summary—which, in turn, can inform IS auditors' consideration of how each feature can impact the organization's strategic objectives. If the strategic initiative is based on processes, the exception management category can be process-based. If, on the other hand, the strategic objective is driven by business units, the exception management category can be the business unit. Grouping recommendations in this way has several benefits, such as allowing the IS audit function to identify significant trends, such as patterns related to resource constraints or repeated instances of technology underutilization. After identifying the trend, the IS auditors can make recommendations and track them, but the more value-added outcome is the ability to report how these enterprisewide patterns may reflect challenges or barriers that will affect achievement of strategic objectives. This demonstrates the IS auditors' profound understanding of the organization and its goals.

Conclusion

IS auditors have an opportunity and obligation to use the audit phases to add value to their organizations by leveraging audit information to further the achievement of strategic objectives.

Endnotes

1 ISACA, Information Technology Assurance Framework (ITAF), USA, 2003, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx*

2 *Ibid.*

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2JcQc5p

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty member at the National Institute of Bank Management, India.

Q Our organization is considering multiple projects for developing and implementing IT-based solutions. I have checked on various websites, but could not get a detailed list of generic risk scenarios for IT-related projects. Can you help?

A Project management is a specialized area of knowledge about completing work that involves various kinds of resources within the constraints of deliverables, cost and time. Considering the proliferation of IT as an enabler for almost all areas of a business, most organizations initiate IT-related projects at one time or other. To leverage project management techniques to deliver on time and within costs, it is imperative for the organization to have a project and program management framework. (A program is a group of projects with a larger scope and a common objective.) If such a framework is not available, implementing one should be the starting point. A standard framework can be obtained from the *Project Management Body of Knowledge (PMBOK) Guide, Sixth Edition.*[1]

Key aspects of project management are identification of risk and the strategies that could be used to either mitigate or minimize the impact due to risk. ISACA's *COBIT® 5 for Risk*[2] is an excellent resource on how to manage risk. In addition, ISACA® has also published *Risk Scenarios Using COBIT® 5 for Risk*.[3] However, it is important to understand that every organization needs to develop its own scenarios depending upon internal (within the organization) and external (i.e., competition, legal, regulatory) risk factors and the nature of the project deliverables, their time lines and budget.

Listed below are a few sample generic areas of risk associated with IT-related projects that may be useful.

Project Planning and Schedule

Project planning is a key for successful completion of the project. Poor planning is the main reason for project failure. Planning requires understanding of all aspects of the project deliverables and constraints for execution of the project. The following risk factors must be considered while planning a project:

- Resource availability schedules by the project sponsor do not match the project time lines.
- The project plan is prepared considering most optimistic effort estimates.
- The work breakdown structure (WBS) omits some tasks.
- The project plan depends upon specific resources.
- Unrealistic time lines are used.
- Existing technology does not support deliverables.
- Tight time lines create pressure, resulting in reduced productivity.
- The project sponsor arbitrarily changes time lines and resource schedules.
- Staff is not familiar with the new technology required for the project deliverables.

Project Organization and Management

To execute the project plan, the project manager needs management skills to address issues arising out of risk materialization. Risk scenarios include:

- The project sponsor is not appointed by the business, and the project lacks top management support.
- Tasks take longer than pessimistic estimates.
- Resources leave the project halfway.
- Project budget is deferred/reduced.
- Specific technology is proposed that is not available locally.
- Personal issues exist among team members.
- Decision/review by management/sponsor at milestones is slow.
- Expected/mandated infrastructure is not available for testing/deployment.
- A user acceptance test resulted in a lack of acceptance.
- The go-to-market time lines are arbitrarily proposed by management, impacting the quality.
- Changes in requirements make rework necessary.
- There are delays in procurement of infrastructure required for project/testing/implementation.

Outsourcing/Third-Party Issues

Many projects require hiring third-party resources or vendors. The following situations, at the minimum, must be considered:

- The third-party (vendor) selection process does not consider the capability of vendor.
- The quality of supplies from the vendor is very low.
- Selected vendor does not have the appropriately skilled resources.
- Vendor management is out of the purview of the project manager.
- Vendor-supplied tools/hardware/services have a high learning curve or are not user-friendly.
- The contract and service level agreement (SLA) with the third party contain weaknesses such as:
  - Absence of a nondisclosure agreement
  - Undefined service levels or service levels not in line with project time lines
  - Absence of monitoring of the third party.
  - Noninvolvement of legal department, resulting in an unenforceable agreement
- Cost of outsourcing was not considered in budget.

Project Requirements Specifications

Almost all IT-related projects suffer from risk associated with scope creep due to various factors including:

- The requirements and scope have not been frozen and signed-off.
- The requirements specifications are poorly defined, resulting in frequent changes.
- The technical requirements are defined vaguely, resulting in gap in understanding.
- The project requirements specifications are signed off, but the change management process is not defined.
- The security requirements specifications are not defined in scope.

Deliverables and Quality Requirements

The quality of the deliverables depends heavily on the skills and experience of the architects, designers and developers involved in the project. Some of the issues faced when the resources are not up to expected levels are:

- Designs result in error-prone/faulty products requiring rework.
- Poor-quality software requires additional design, testing and implementation efforts.
- The specifications of the user interface are not met.
- Extra functions/modules that are not required are included.
- Response/execution speed/capacity requirements are not considered during design creating issues.
- Compatibility and interface with legacy and other systems require more effort for testing, design and implementation.
- Use of unproven, latest technology results in frequent changes in design and development.
- A requirement for a platform-independent solution takes longer to satisfy stakeholders.
- The final production environment is not available for testing and implementation.
- The testing/production environment is not configured as per policy.
- Deliverable milestones are unrealistic and affecting the quality of the deliverables.

Read more about risk factors of IT-related projects in the expanded HelpSource column which can be found exclusively online *(www.isaca.org/journal/archives/Pages/default.aspx)*.

Conclusion

The risk scenarios listed here are generic and one may use them as guidance. It is not complete list of project-related risk. The project manager needs to develop a list of possible risk scenarios depending upon the associated risk factors.

Endnotes

1 Project Management Institute, *Project Management Body of Knowledge PMBOK Guide, Sixth Edition*, USA, 2017, *https://www.pmi.org/pmbok-guide-standards/foundational/pmbok/sixth-edition*

2 ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/cobit/pages/risk-product-page.aspx*

3 ISACA, *Risk Scenarios Using COBIT® 5 for Risk*, USA, 2014, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Risk-Scenarios-Using-COBIT-5-for-Risk.aspx*

Enjoying this article?

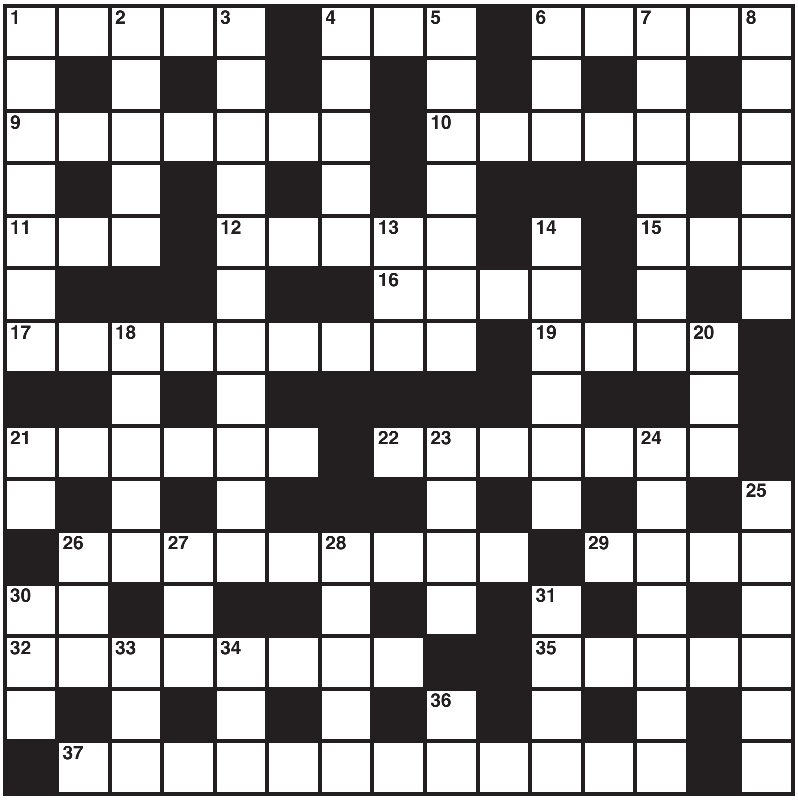
- Learn more about, discuss and collaborate on audit tools and techniques in the Knowledge Center. www.*isaca*.org/it-audit-tools-and-techniques

CROSSWORD PUZZLE

by Myles Mellor
www.themecrosswords.com

ACROSS

1. Incidents of data being allowed to get into unauthorized hands
4. Encrypted network for company employees
6. Estimated worth
9. Internet gateways
10. Very large
11. Prefix for gen or acetylene
12. Makes less arduous
15. List's last letters
16. Increase
17. Court orders of a kind
19. Popular *ISACA® Journal* columnist, Stephen
21. Are stored in
22. Area of IT concern following recent Facebook lapses
26. The SC in BSC
29. Employee in a company's IT system
30. Exercise class (abbr.)
32. Process of restoring lost, deleted or inaccessible data
35. Development stage
37. One word in the title of an area of technical development that is probablistic rather than deterministic



DOWN

1. Easily stolen mobile devices
2. Data structure including a group of elements
3. One with an interest in a company
4. Places in control of, as stocks, funds or property, etc.
5. Unbeatable foe
6. Get-up-and-go
7. Makes less strict, as rules
8. One factor that is often underestimated as a success factor in government and management activities
13. Epoch
14. Determine by reasoning
18. Underlying
20. Infiltrator
21. Memo subject line intro
23. Nearly unique
24. COBIT® 5 Goals ____
25. Instructions
26. Understand
27. Classified sales letters
28. ____ draw graphics
30. Prefix for before
31. Word often used before source
33. Is able to
34. Contend
36. Symbol for silver

Answers on page 58

Take the quiz online.

https://bit.ly/2HjZHd6

CPE QUIZ #179

Based on Volume 2, 2018—Innovation Governance
Value—1 Hour of CISA/CRISC/CISM/CGEIT Continuing Professional Education (CPE) Credit

TRUE OR FALSE

BAYUK ARTICLE

1. Technology risk is recognized as an enterprise risk in the new Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework document, *Enterprise Risk Management—Integrating With Strategy and Performance*.
2. The new ERM framework's components must be established in cascading order (similar to COBIT®) so that one component can provide goals for others. For that reason, the framework requires that continuous operation of risk management activities be carried out in a prescribed sequential order.
3. The processes used to identify, assess, quantify and monitor technology risk can be applied to support the integrity of information used by risk managers in other risk domains.

DAVIS ARTICLE

4. When knowledge is shared, it can positively affect innovation performance. When knowledge is leaked (accidentally), it can negatively affect relationships.
5. Despite indications to the contrary, there is no established linkage between environmental compliance and the development of new, "green" products.
6. Although global competitiveness has increased significantly, development of platforms for IT disruptive advantage and sustainability is still not considered a strategic issue for business leaders.
7. Defender organizations function in two marketplace or product domain types: one stable and the other morphing. In the latter, they tend to behave like prospector organizations.

GHAZNAVI-ZADEH ARTICLE

8. Availability and effectiveness of required controls, monitoring of the controls' operation and integrity, and regular optimization all contribute to calculation of the organization's information security maturity levels.
9. Of the two categories of risk—business risk and operational risk—business risk is the one that takes into account new audit findings.
10. The Open Group Open FAIR can be used to assess the likelihood and impact of a risk and calculate a risk score, but it will not identify appropriate mitigation controls.

DAVIDSON ARTICLE

11. While connectivity has introduced risk (as well as benefits) to organizations, an even bigger challenge is the gap between the complex security management demands of IT/operational technology (OT) networks and the resources available to meet them.
12. Solutions for OT that offer visibility into the organization's entire attack surface are widely available and in use, and effectively integrated into the IT security program.
13. The connections between IT and OT are a major source of risk, but are also increasingly common due to the convenience offered by a growing number of Internet of Things (IoT) devices.

EITAN ARTICLE

14. As concerns about supply-chain-based cyberattacks increase, the need for a risk assessment that identifies high-risk vendors by using a scoring method becomes more evident.
15. A properly conducted risk assessment starts with mapping.
16. Identifying high-risk vendors calls for evaluating the number of delivery vectors (connectivity and gateway platforms) available to the vendor.

ATLURI ARTICLE

17. High-profile data breaches tend to suppress spending in organizations.
18. New regulations that arise in the wake of increasing data breaches tend to cause cyberinsurance customers to adopt more stringent security controls.
19. Despite the growing number and impact of data breaches, the situation has not resulted in increased hiring of chief information security officers (CISOs).
20. Three elements are key for quantitative cyberrisk analysis: the skill of the analysts, possession of the latest equipment and use of commonly available tools.

CPE QUIZ
#179

THE ANSWER FORM

Based on Volume 2, 2018

TRUE OR FALSE

BAYUK ARTICLE

1. ________________________

2. ________________________

3. ________________________

DAVIS ARTICLE

4. ________________________

5. ________________________

6. ________________________

7. ________________________

GHAZNAVI-ZADEH ARTICLE

8. ________________________

9. ________________________

10. ________________________

DAVIDSON ARTICLE

11. ________________________

12. ________________________

13. ________________________

EITAN ARTICLE

14. ________________________

15. ________________________

16. ________________________

ATLURI ARTICLE

17. ________________________

18. ________________________

19. ________________________

20. ________________________

Name ____________________________________

PLEASE PRINT OR TYPE

____

Address ___________________________________

____

CISA, CRISC, CISM or CGEIT # ________________________

____

Answers: Crossword by Myles Mellor
See page 56 for the puzzle.

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

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 to ISACA Support or by fax to +1.847.253.1755. 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, 1700 E. Golf Rd., Suite 400, Schaumburg, IL 60173 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, CRISC, CISM or CGEIT CPE credit.

ISACA Member and Certification Holder Compliance

The specialized 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 mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

General

1001	Audit Charter
1002	Organizational 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

The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorization as the standards (also divided into three categories):

- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

General

2001	Audit Charter
2002	Organizational 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

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 programs, 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.*

Prior to issuing any new standard or guideline, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director, Thought Leadership and Research, via email (standards@isaca.org); fax (+1.847.253.1755) or postal mail (ISACA International Headquarters, 1700 E. Golf Road, Suite 400, Schaumburg, IL 60173, USA).

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

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 these products will assure a successful outcome. The guidance 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 judgment to the specific control circumstances presented by the particular systems or IS environment.

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

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

ISSN 1944-1967

Subscription Rates:

US:
one year (6 issues) $80

All international orders:
one year (6 issues) $95

Remittance must be made in US funds.

ADVERTISERS/ WEBSITES

Mitsubishi UFJ Trust & Banking Corp		Page 51
SCCE	*corporatecompliance.org/academies*	page 1

leaders and supporters

GENERAL DATA PROTECTION REGULATION (GDPR)
READINESS, ASSESSMENT AND COMPLIANCE

Is Your Enterprise GDPR Compliant?

WHO:
Enterprises that offer goods or services (regardless if payment is required) within the EU as well as enterprises that monitor EU subjects' behavior within the EU.

WHAT:
New data privacy mandates have been issued by European Union regulation.

WHERE:
Includes any organization in the world if it retains or processes information on any citizen in the EU.

WHEN:
GDPR went into effect on 25 May 2018.

WHY:
To better protect any individual's personal information, to secure rights for the individual over that collected information, and to force enterprises to follow a uniform scheme for data protection.

HOW:
Follow ISACA's privacy guidance on how best for your enterprise and its staff to assess your unique data protection needs and meet the GDPR compliance standards set by the EU.

ISACA-CMMI GDPR ASSESSMENT

ISACA-CMMI's complimentary tool, *GDPR Assessment*, provides users with a roadmap for GDPR implementation based on the answers to a series of questions/statements. The resulting customized assessment offers insights as to where your organization should focus its data protection efforts. Over time, as your enterprise's GDPR implementation moves forward, users can retake the assessment to gauge progress on compliance.

The *GDPR Assessment* is powered by the expertise of both ISACA and CMMI. For nearly 50 years, ISACA has supported the global IS/IT community with world-class guidance in the areas of privacy and security. For more than 25 years, CMMI has helped enterprises evaluate performance and maturity through their scoring practices models.

This tool is a valuable resource for data protection officers (DPOs); security, compliance and audit executives and managers; data privacy authorities and their auditors; as well as consultants, external auditors and assessors.

www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-CMMI-GDPR-Assessment.aspx

ISACA®

FEATURED ISACA PUBLICATIONS

CISA® Review Manual, 26th Edition

The *CISA Review Manual 26th Edition* is a comprehensive reference guide designed to help individuals prepare for the CISA exam and understand the roles and responsibilities of an information systems (IS) auditor. The manual has been revised according to the 2016 CISA Job Practice and represents the most current, comprehensive, peer-reviewed IS audit, assurance, security and control resource available worldwide.

The 26th edition is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Service Management
- Protection of Information Assets

The *CISA Review Manual 26th Edition* features an easy-to-navigate format. Each of the five chapters has been divided into two sections for focused study. Section one of each chapter contains the definitions and objectives for the five areas, as well as the corresponding tasks performed by IS auditors and knowledge statements (required to plan, manage and perform IS audits) that are tested on the exam. It also includes:

- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in section two for each knowledge statement
- Self-assessment questions and explanations of the answers
- Suggested resources for further study

Section two of each chapter consists of reference material and content that supports the knowledge statements. The material enhances CISA candidates' knowledge and/or understanding when preparing for the CISA certification exam. In addition, the *CISA Review Manual 26th Edition* includes brief chapter summaries focused on the main topics and case studies to assist candidates in understanding current practices. Also included are definitions of terms most commonly found on the exam.

Print Product Code: CRM26ED
eBook Product Code: EPUB_CRM26ED
Member Price: $105.00
Non-member Price: $135.00

CISA® Review Questions, Answers & Explanations Manual, 11th Edition

CISA Review Questions, Answers & Explanations Manual 11th Edition consists of 1,000 multiple-choice study questions that have previously appeared in the *CISA Review Questions, Answers & Explanations Manual 2015* and the *CISA Review Questions, Answers & Explanations Manual 2015 Supplement*. The manual has been updated according to the newly revised 2016 Job Practice.

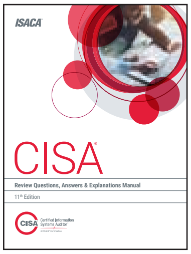
Many questions have been revised or completely rewritten to be more representative of the CISA exam question format and/or to provide further clarity or explanation of the correct answer. These questions are not actual exam items but are intended to provide CISA candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam.

This publication is ideal to use in conjunction with the:

- *CISA Review Manual 26th Edition*
- *CISA Review Questions, Answers & Explanations Database—12 Month Subscription*

To assist candidates in maximizing study efforts, questions are presented in the following two ways:

- Sorted by job practice area—Questions, answers and explanations are sorted by the CISA job practice areas. This allows the CISA candidate to refer to questions that focus on a particular area as well as to evaluate comprehension of the topics covered within each practice area.
- Scrambled as a sample 150-question exam—150 of the 1,000 questions included in the manual are selected to represent a full-length CISA exam, with questions chosen in the same percentages as the current CISA job practice areas. Candidates are urged to use this sample test to simulate an actual exam and to determine their strengths and weaknesses in order to identify areas that require further study. Answer sheets and an answer/reference key for the sample exam are also included. All sample test questions have been cross-referenced to the questions sorted by practice area, making it convenient for the user to refer back to the explanations of the correct answers.



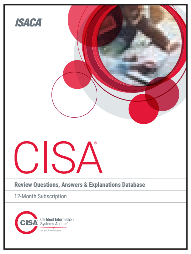
Print Product Code: QAE11ED
Member Price: $120.00
Non-member Price: $156.00

CISA® Review Questions, Answers & Explanations Database—12 Month Subscription

The *CISA Review Questions, Answers & Explanations Database* is a comprehensive 1,000-question pool of items that contains the questions from the *CISA Review Questions, Answers & Explanations Manual 11th Edition.* The database has been revised according to the recently updated 2016 CISA Job Practice. The database is available via the web, allowing CISA Candidates to log in at home, at work or anywhere they have Internet connectivity. This database is MAC and Windows compatible.

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CISA candidates to identify their strengths and weaknesses and focus their study efforts accordingly.

Other features provide the ability to select sample exams by specific job practice domain, view questions that were previously answered incorrectly and vary the length of study sessions, giving candidates the ability to customize their study approach to fit their needs.



Database Product Code: XMXCA15-12M
Member Price: $185.00
Non-member Price: $225.00

Blockchain Fundamentals

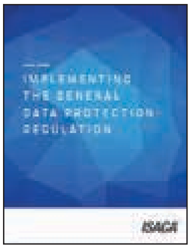
Blockchain has the potential to become a major force for innovation and change the way you process everything with records-from registrations, records of ownership, transfers of value and stock purchases, to identities and healthcare. The current digital world is built on ledger systems that worked well in past generations, but that fail to provide you with the capability to address the ledgers that are needed in an Internet-driven world. The basic blockchain characteristics that successfully create a secure and trustable infrastructure to support the Bitcoin cryptocurrency system are disrupting how we create and use ledgers, which, in turn, has the potential to bring significant value to the global economy and provide new capabilities that enhance government and business functions. Blockchain use is not limited to cryptocurrencies. Other blockchains are being developed so that input and output transactions contain ledger entries for numerous other items, including financial instruments, public records, contract information, other items demonstrating ownership or professional capability, and identities. Using trusted technologies to create its unique structure, blockchain features-such as openness, decentralized infrastructure, ability to transact anonymously while ensuring identity, and elimination of third-party attestation.

Web Download Product Code: WBCB
Member price: $25.00
Non-member price: $50.00

Implementing the General Data Protection Regulation

As of 25 May 2018, all enterprises that conduct business and hold personal data on just one person located in the European Union will fall under the mandates of a new EU requirement—the General Data Protection Regulation (GDPR). All EU businesses are subject to GDPR, but its effect goes even farther. Given the global scope of today's digital-based commerce, the impact of GDPR certainly will be felt by many businesses across the world and located outside the physical borders of the EU.

Undertaking monumental compliance changes to organizational data protection strategy and information security requires trustworthy, comprehensive guidance. ISACA's new guide, *Implementing the General Data Protection Regulation*, was created to address the many data protection and privacy concerns found within commercial and not-for-profit enterprises. From C-suite to legal and IT teams, from operations and vendor management to marketing and communications, this reference provides valuable information on GDPR readiness, assessment and compliance.

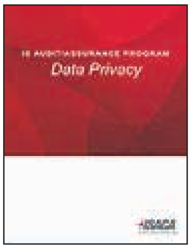


Print Product Code: GDPR
Member price: $40.00
Non-member price: $80.00

Web Download Product Code: WGDPR
Member price: $25.00
Non-member price: $50.00

Data Privacy Audit Program

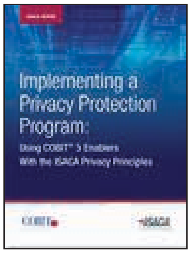
Data Privacy considers the obligations of organizations around the information that can be used on its own or in conjunction with other information to identify, contact or locate an individual. This consideration exists for the data lifecycle from collection to use, disclosure and retention through disposal.



Web Download Product Code: WAPDP1
Member Price: $25.00
Non-member Price: $50.00

Implementing a Privacy Protection Program: Using COBIT 5 Enablers with the ISACA Privacy Principles

Privacy breaches can cause a cascade of negative impacts on enterprises, as well as significant harm to the associated data subjects. Enterprises may suffer financial loss and reputational damage, be charged with failure to comply with regulations and legislation, and alienate key stakeholders who demand safety of personal information. To avoid these outcomes, enterprises must establish and maintain a formal privacy protection program. This publication shows how to optimize a privacy program built on the framework of COBIT® 5 through focused, yet comprehensive, application of its enablers.

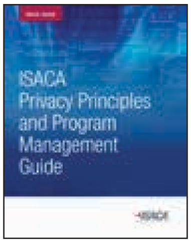

Implementing a Privacy Protection Program:
Using COBIT 5 Enablers With the ISACA Privacy Principles
COBIT
ISACA

Print Product Code: IPP2
Member Price: $60.00
Non-member Price: $100.00

Web Download Product Code: WIPP2
Member Price: $50.00
Non-member Price: $90.00

ISACA Privacy Principles, Governance and Management Program Guide

The main purpose of *ISACA Privacy Principles, Governance and Management Program Guide* is to provide readers with a harmonized privacy framework. The book offers a set of privacy principles that align with the most commonly used privacy standards, frameworks and good practices, as well as fill in the gaps that exist among these different standards. This practical guide can support or be used in conjunction with other privacy frameworks, good practices, and standards to create, improve and evaluate a privacy program specific to the practitioner's enterprise. Special guidance on how to use the COBIT 5 framework to implement a more robust privacy program is included in this publication.



Print Product Code: IPP
Member Price: $45.00
Non-member Price: $90.00

Web-download Product Code: WIPP
Member Price: $35.00
Non-member Price: $70.00

ISACA®

THE KNOWLEDGE FOR WHAT'S NEXT.

THE SKILLS YOU NEED NOW.

- Interact with experienced ISACA® or Deloitte instructors who are experts in their field.
- Save time with focused, 4-day Training Week courses offering hands-on learning.
- Earn up to 32 CPEs per course toward certification maintenance and develop real-world skills you can apply immediately.

Develop career-enhancing expertise that can help shape your future role.

SEE WHAT'S NEXT, NOW

REGISTER TODAY AT

www.isaca.org/training-jv4

PREPARE FOR YOUR NEXT ROLE, NOW.

Gain new tools and techniques as you advance or refresh your knowledge at locations across North America.

ISACA TRAINING COURSES

TUITION: ISACA Members US $2,295
Non-Members US $2,495

CISM Bootcamp: 4-day Exam Prep

Chicago | 6 – 9 August 2018

COBIT 5: Strategies for Implementing IT Governance

San Diego | 4 – 7 December 2018

Cybersecurity Fundamentals 4-day Cram Course

Chicago | 6 – 9 August 2018
San Diego | 4 – 7 December 2018

Foundations of IT Risk Management

Chicago | 6 – 9 August 2018
San Diego | 4 – 7 December 2018

Fundamentals of IS Audit & Assurance

San Diego | 4 – 7 December 2018

ISACA/DELOITTE TRAINING COURSES

TUITION: ISACA Members US $2,495
Non-Members US $2,695

Cloud Computing: Seeing through the Clouds—What the IT Auditor Needs to Know

San Jose | 12 – 15 November 2018

Information Security Essentials for IT Auditors

Tampa | 10 – 13 December 2018

Analytics & Automation in Action: Utilizing Data Analytics & Automation to Enable Internal Audit

Costa Mesa | 24 – 27 September 2018

Network Security Auditing

Atlanta | 8 – 11 October 2018

For details on discounts, deadlines, registration, cancellation and more, visit www.isaca.org/training-jv4.