VOLUME 2, 2018

ISACA® Journal

INNOVATION GOVERNANCE

+

TECHNOLOGY'S ROLE IN ENTERPRISE RISK MANAGEMENT

APPLYING A TECHNOLOGICAL INTEGRATION DECISION FRAMEWORK TO INNOVATION GOVERNANCE

INFORMATION SECURITY ARCHITECTURE GAP ASSESSMENT AND PRIORITIZATION

ISACA.ORG

THE EXPERTISE FOR WHAT'S NEXT.

THE TRAINING YOU NEED, NOW.

- Dive deep into IS audit, security, cybersecurity, privacy, governance, risk and more.
- Interact with experienced ISACA® or Deloitte instructors who are experts in their field.
- Save time with focused, 2- or 4-day Training Week courses offering hands-on learning.
- Earn up to 32 CPEs at each 4-day course toward certification maintenance and develop real-world skills you can apply immediately.
- Choose the Training Week courses that fit your goals and schedule.
- Build your expertise and boost your reputation with ISACA training.

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

SEE WHAT'S NEXT, NOW

REGISTER TODAY AT
ISACA.ORG/TRAINING18JV2

PREPARE FOR YOUR NEXT ROLE, NOW.

Gain new tools and techniques as you advance or refresh your knowledge.

ISACA TRAINING COURSES

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

CISM Bootcamp: 4-day Exam Prep

COBIT 5: Strategies for Implementing IT Governance

Cybersecurity Fundamentals 4-day Cram Course

Foundations of IT Risk Management

Fundamentals of IS Audit & Assurance

Governance of Enterprise IT

RSA 2018 TRAINING COURSES

TUITION:
ISACA Members and Non-Members US $1,200

CISM 2-day Cram to the Max Course

CSX Cybersecurity Fundamentals 2-day Workshop

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

Healthcare Information Technology

Information Security Essentials for IT Auditors

Internal Audit Data Analytics & Automation

An Introduction to Privacy and Data Protection

Network Security Auditing

Taking the Next Step—Advancing Your IT Audit Skills

For details on discounts, deadlines, registration, cancellation and more,
VISIT ISACA.ORG/TRAINING18JV2

International Basic Compliance & Ethics ACADEMIES

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

INTERNATIONAL ACADEMIES

OFFERED IN 2018

AMSTERDAM, NETHERLANDS
23–26 APRIL

SINGAPORE
9–12 JULY

SÃO PAULO, BRAZIL
20–23 AUGUST

MADRID, SPAIN
24–27 SEPTEMBER

RIO DE JANEIRO, BRAZIL
26–29 NOVEMBER

REGISTER EARLY TO RESERVE YOUR SPACE

ACADEMIES LIMITED TO 75 PARTICIPANTS

corporatecompliance.org/academies

Questions: lizza.catalano@corporatecompliance.org

SCCE™

ISACA Journal

FEATURES

PLUS

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 March and April 2018.

E-Governance of Currencies
Vijayavanitha Sankarapandian, CISA, CIA

Rethinking User Access Certifications
Vincent J. Schira, CISA, CIPT, CISSP, CPA, PCI-ISA

Minimizing the High Risk of Failure of Corporate Innovation
Guy Pearce

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*

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.

ISACA®
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone
+1.847.660.5505
Fax +1.847.253.1755
www.isaca.org

Disaster Recovery Management in the Multi-Modal Era

Multi-modality in IT environments implies complexity. The concept of an organization's information systems operating in a space and on equipment owned by that organization has been replaced by systems residing in:

- A proprietary, "in-house" data center
- A commercial colocation (colo) site
- An outsourced data center
- A managed services provider
- A remote, vendor-operated site, providing a service over the Internet
- The cloud, a commonly used term for a series of commercial data centers in which a customer executes its applications or acquires commercial services

Oh, by the way, all at the same time.

This complexity is difficult to manage even in the best of times. Having a disaster strike any of these venues is decidedly not the best of times. (Others wiser than I can decide whether a physical disaster is the worst case or if that "honor" belongs to being the victim of a destructive cyberattack.) I think that I speak for all of us in saying disasters are pretty bad and ought to be avoided.

Geographic Diversity

Multi-modality is, in part, a response to the threat of disasters. Its very structure ensures that a single disaster does not wipe out everything, just that portion of an organization's systems unfortunate enough to be located where a disaster hits. Or am I being too free with the word "ensures"?

One of the factors that should influence decisions about moving a system out of a proprietary data center is where it will then be located—beyond what it can do, how it is secured and how it performs. If the intent is to reduce risk, then moving systems to a colo across the street from the organization's headquarters and to an outsourcing provider next door will not accomplish very much. As ever, poor design can undermine the best of controls and security features. The word "ensures" should be replaced with "enables"; it is up to system architects to provide assurance that a multi-modal environment contains sufficient geographic diversity to meet its overall disaster recovery objectives.

Proprietary Data Centers

Even in a multi-modal architecture, there is still a need for a proprietary data center.[1] It is the central point for communicating with all the systems elsewhere. It also houses computers driving building management and access control systems, as well as Internet of Things (IoT)[2] equipment, around the building.

Planning for recovery from a disaster at an "in-house" data center is actually more difficult now than previously. In the old days (oh, about a decade ago), most of an organization's applications and infrastructure resided in its own data center.

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.

http://bit.ly/2rTqwSL

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.

Therefore, planning for a disaster in that location required having a second data center somewhere else, far enough away that the same disaster would not incapacitate both.

Now, simply finding another place to run these systems is insufficient, perhaps unavailing. If they could have been transferred out of the data center, they would already have been, in the move to multi-modalism. What would be the point of a remote telecommunications termination hub if a building's demarc is destroyed? Even if a remote link could be established, how would data be delivered to the desktop? How would the phones ring?

Colo Sites and Outsourcers

Use of a colo site often has more to do with mechanical, electrical and plumbing (MEP) issues than IT. For many organizations, the economics of powering and cooling a data center just do not make sense if those burdens can be transferred to a third party. For others, migrating from an organization's own data center to a colo is simply a transitional phase on the way to Anything as a Service (XaaS).[3] Whatever it is, the decision to move servers, storage and telecommunications into a colo means moving them into not one, but two sites: a prime and a backup. An organization may already have a disaster recovery facility and it may serve for the transferred systems, or maybe not. Testing is in order before total reliance is placed on the colo-based systems. The same point can be made about outsourcing[4] one or more applications and their associated infrastructure. In choosing an outsourcer, it is incumbent on the customer to ensure that that hosting company has at least a second data center, as well as a well-tested and maintained plan for using it if the time should ever come. The basic premise of dual data centers is still in force.

Managed Services and Software as a Service

A special case of outsourcing is managed services: in essence, hiring someone else (a managed services provider [MSP]) to do work that an organization does not want to or cannot do itself. These include certain IT functions, particularly email hosting, performance management, security monitoring, storage, backup and recovery, and network monitoring.[5] Of course, many of these activities can be done anywhere an MSP decides, but some require hands-on work. So, buyers should consider how these services will be provided if there is a disaster wherever the systems and, even more important, the workers happen to be.

> "A TRUE CLOUD IS A SUPERB SOLUTION TO DISASTER RECOVERY PROBLEMS."

The need for due diligence is greater in the case of Software as a Service (SaaS) accessed by a customer over the Internet.[6] An organization has the use of software, typically on a subscription basis, but does not own that software nor the servers and storage on which it runs. That equipment is somewhere and, in preparing for recovery from disasters, has to be somewhere else as well. Where that "somewhere" is matters, as does the frequency with which the software and customer data are replicated from place to place. These are not novel considerations, but many SaaS subscriptions are made by business functions, not IT, and disaster recovery may be overlooked.

The Cloud

A true cloud is a superb solution to disaster recovery problems. Note the modifier "true." There are vendors claiming to offer cloud services, but a little investigation will show that they are just hosting services with a few sites. They do not offer the underlying infrastructure and mechanics of a true cloud, in which the same software (usually virtualized) runs simultaneously in two or more locations, with data replicated at frequent intervals among them. The intent, and in many cases the actuality, is that operations can be switched from

site to site with little or no impact on the customers. This may be done for performance reasons, load balancing or recovery. With attention to the latter, it is essential to verify the infrastructure claims of the salesperson and validate that this automatic failover actually works before committing to a cloud provider.

In this era of multi-modal technology, many disaster recovery issues are solved, some are simply transferred and a few are made worse. Disaster recovery is manageable, but only with one's eyes open.

Endnotes

1 This assumes that an organization has a building where its people work, which is only partially true today. Many people work remotely some or all of the time. The future may lead companies and government agencies to divorce work from real estate and the residual data center may actually disappear.

2 Addressed in Ross, Steven J.; "The End of the Beginning?" *ISACA® Journal,* vol.3, 2017, *http://www.isaca.org/Journal/archives/Pages/default.aspx*

3 McLellan, C.; "XaaS: Why 'Everything' Is Now a Service," *ZDNet*, 1 November 2017, *www.zdnet.com/article/xaas-why-everything-is-now-a-service/*. Pronounced zăss, it means "Anything as a Service."

4 In using a colo, an organization owns the equipment and rents the floor space and MEP. If a system is outsourced, the organization owns the application(s), but not the equipment on which it runs, nor the floor space, nor the MEP. These are subtle differences, to be sure, but crucial in planning for disaster recovery.

5 Olavsrud, T.; "How to Get the Most From a Managed IT Services Provider," *CIO*, 30 June 2017, *https://www.cio.com/article/2930498/it-strategy/why-businesses-are-turning-to-managed-it-services.html*

6 Hufford, J.; "Cloud Vs SaaS: What's the Difference?" *nChannel*, 13 July 2016, *https://www.nchannel.com/blog/cloud-vs-saas/*. All such services based on software in a cloud are SaaS, but SaaS need not be in the cloud. The services can be accessed directly without passing through a cloud provider. This is a source of confusion and some controversy, into which I do not intend to enter here.

Innovation in the IT Audit Process

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.

http://bit.ly/2Eqjnfz

In June 2015, ISACA® began publishing a set of white papers titled "Innovation Insights."[1] The papers covered the top 10 emerging digital technology trends most likely to deliver significant value, in excess of cost, to the vast majority of enterprises.[2] The topics covered included big data analytics, mobile, cloud, machine learning, the Internet of Things (IoT), massive open online courses, social networking, digital business models, cybersecurity and digital currency. Unfortunately, from an audit perspective, the papers were targeted at business leaders and board members. While they are not all topics that an IT auditor can influence on a day-to-day basis, does that mean that IT auditors cannot innovate?

Innovation is defined as the introduction of something new or a new idea, method or device[3]; therefore, introducing something new to a process is innovating. Further, if it is new to the enterprise, it is also innovation. So, how can we innovate throughout the IT audit process?

According to ISACA, the typical audit process consists of three phases (**figure 1**). The following are my thoughts for potential innovation during each phase. Please bear in mind that what may be new and innovative for enterprise A may be business as usual for enterprise B.

Ian Cooke, CISA, CGEIT, CRISC, 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.

Planning—Collaborate

The Internet allows us to communicate with peers instantly and has enabled innovative ways of doing many things. Fundamentally, however, we are each still planning and creating audit programs as if this revolution had not taken place. In an earlier column,[4] I advocated for the ISACA community to develop open-source audit/assurance programs. In the meantime, organizations can innovate by collaborating on audit/assurance programs through their local chapters or industry groups. For example, does the next seminar have to take the format of an expert explaining the fundamentals of a new law or regulation? Can it not be a facilitated open forum that results in, or at least is the basis for, an audit program for said regulation?

Also, please remember that collaboration is always possible in the ISACA Knowledge Center.[5]

Planning—Implement Audit Management Software

Over the years there have been several discussions on the ISACA Knowledge Center on the benefits (or otherwise) of adopting audit management software. Those against point to the inflexibility of many of the tools available and the fact that it is just easier to get things done with Microsoft Word and Excel. However, one of the real benefits is that they enforce a standardized process. This is the very essence of what we, as auditors, like to see in processes we review.

Standardization ensures that each audit goes through steps defined and agreed on by the enterprise. These will likely include risk assessment, peer review and audit management approval. They will, in turn, improve the quality and consistency of audits. Consistency of message is key for audit functions and, indeed, for auditees.

Further, it means that IT auditor A should be in a better position to pick up, understand and continue work initiated by IT auditor B.

Planning—Utilize Data Analytics Earlier

Traditionally, the use of data analytics is considered only at the audit fieldwork stage. However, if an engagement enables access to all the enterprise's data for the subject under review, then it may be worth employing data analytics earlier. By mining the data, it is possible to determine which countries, business units, and business processes or other areas hide outliers that could represent increased risk or compliance issues. Once a business unit or geography is identified, the scope of the engagement can be further refined by drilling deeper into the data, increasing scope in higher-risk areas and reducing scope in sectors where analytics suggests the risk may be less. The overall result is a more dynamic audit plan based on continuous, just-in-time risk assessment; more efficient audits that are aligned with areas of risk; more effective results from audits that are focused on those areas of high risk; and automated reporting.[6]

> "TRADITIONALLY, THE USE OF DATA ANALYTICS IS CONSIDERED ONLY AT THE AUDIT FIELDWORK STAGE."

Planning—Implement Control Self-Assessment

In enterprises where a sizable portion of the evidence is provided by interviewing and there is a good, proven working relationship between

management and audit, one can truly innovate and save significantly on time by adopting control self-assessment (CSA). CSA was also discussed in a previous column.[7] To recap, ISACA defines CSA as an assessment of controls made by the staff of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable.[8]

CSA requires the auditee to answer a series of questions on the relevant criteria or the standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter.[9] With management agreement, these results can be used as a basis for audit recommendations.

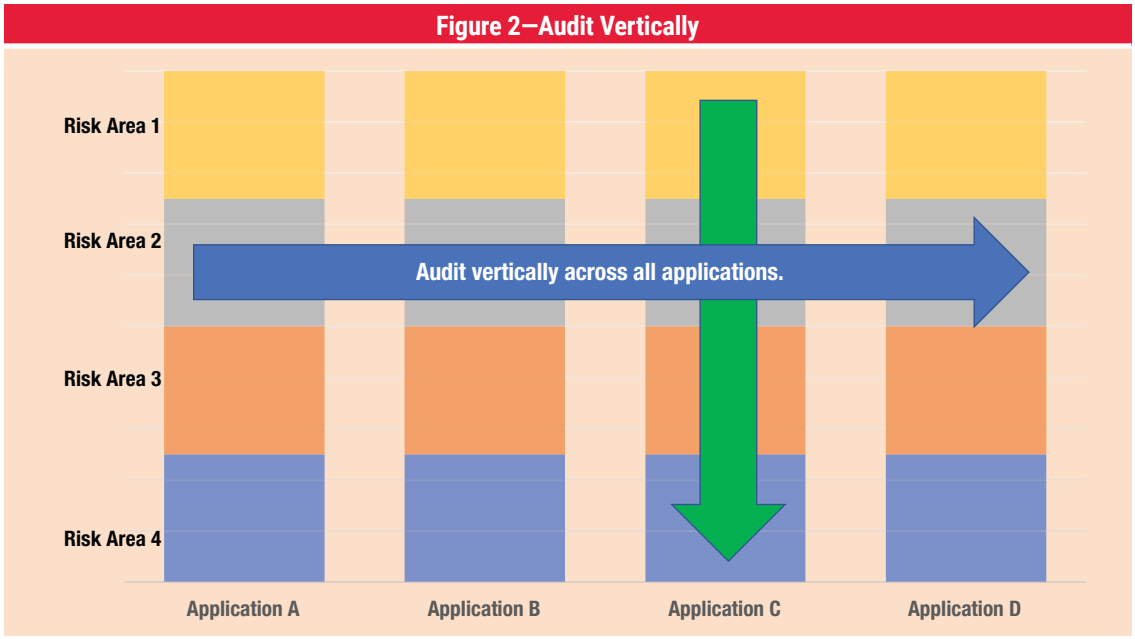
Planning—Audit Vertically

It is widespread practice to audit applications or subject areas horizontally, that is, reviewing all the

Figure 1—Typical Audit Process Phases

Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016. Reprinted with permission.

Figure 2—Audit Vertically



selected risk areas for a given application. Each application or subject is audited independently (**figure 2**). However, auditing in this manner can result in recurring findings or common themes.

> IF THE IT AUDITOR IS GIVEN PRIMARY, READ-ONLY ACCESS TO THIS EVIDENCE, IT WILL REDUCE THE TIME THE AUDITOR NEEDS TO SPEND WITH THE AUDITEE, ULTIMATELY SAVING THE ENTERPRISE MONEY.

For example, several applications may not be fully compliant with the defined change management process. This will result in multiple similar findings across the different applications. In such circumstances, it may make sense to audit the change management process itself vertically across all the applications (**figure 2**) perhaps utilizing the COBIT® 5 enablers.[10] The purpose of such an audit would be to address the underlying causes of the recurring theme and mitigate risk across several applications.

Fieldwork/Documentation—Get Primary Access to the Evidence

At the fieldwork stage of an audit, an IT auditor attains evidence to measure against the criteria. The traditional way to do this is via interviewing and walk-throughs, where the IT auditor will ask for a print screen, copy of a report or other evidence to confirm that the criteria have been met. However, if the IT auditor is given primary, read-only access to this evidence, it will reduce the time the auditor needs to spend with the auditee, ultimately saving the enterprise money.

Further, the IT auditor need not be limited to sampling. Some examples follow:

- **Change management**—If a change management application is in place and the IT auditors have direct access to it, they do not necessarily need to walk through the changes with the auditee. They can sample or test all changes directly on the application or by extracting the data from the application for further analysis.
- **Vulnerability management**—If the IT auditors have direct, read-only access to the vulnerability scanner, they can tell if the associated assets are being scanned by the tool. Further, by reviewing the results of previous scans they can gain assurance on whether an ongoing process is in place and vulnerabilities are continuously being mitigated.

- **Audit and logging**—If the IT auditors have direct, read-only access to the enterprise's security information and event management (SIEM) tool, they can tell whether the related application assets are captured in the tool and the auditing is at a level that matches the required criteria.

This concept could also be applied to other processes where automated software is in use or evidence is captured and maintained by second-line functions.[11] This could include the leavers and movers process, disaster recovery testing, backup restore testing, and database scanners.

Fieldwork/Documentation—Repurpose Generalized Audit Software

ISACA defines generalized audit software (GAS) as multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting.[12] From an IT auditor's perspective, the use of GAS tools is traditionally restricted to supporting operational or general audits by aiding in the extraction and analysis of data from the database of a given application. However, these tools will equally support data extracted from servers, application logs and views, and meta data from databases. They can be used, therefore, to support IT audits.

Once extracted, the data can be analyzed and compared against known compliant data sets and other sources of data, such as the company payroll. Further, the process can be repeated and used as part of a continuous monitoring and/or audit. Examples of this approach in use include "Auditing Oracle Databases Using CAATs"[13] and "Auditing SQL Server Databases Using CAATs."[14]

Reporting/Follow-Up—Utilize the ISACA Glossary

In a 2015 white paper, ISACA defined the five attributes of an audit finding (**figure 3**).[15] A potential issue with the condition attribute is that the report audience may not always be technical even though a technical finding is being described. Therefore, it makes sense to include a definition of the area under review with the audit finding (e.g., vulnerability management). An effective way to do this is to use the definitions from the ISACA glossary.[16] This provides clear explanations and will also create consistency, in that vulnerability management, for example, will be defined in the same way across multiple audit reports. This, in turn, means that the audience will learn and understand the terminology over time.

Even, if the ISACA glossary does not currently meet organizational needs, it can be used as a baseline or starting point.

Reporting/Follow-Up—Use Video

IT audit reports can be complex documents containing layers of interrelated findings that affect multiple areas of the business and often require further explanation. This may be overcome by

Figure 3—Attributes of an Audit Finding

Attribute	Description	Identifies
Condition	Findings	Identifies the auditor findings. It is a statement of the problem or deficiency. This may be in terms such as control weaknesses, operational problems, or noncompliance with management or legal requirements.
Criteria	Requirements and baseline	Statement of requirements and identification of the baseline that was used for comparison against the auditor findings, based on the audit evidence.
Cause	Reason for the condition	While the explanation of the cause may require the identification of the responsible party, it is suggested that, unless required by audit policy, the report should identify the organizational business unit or person's title and not the individual's name. The same should be applied to the identification of the person representing the relevant point of accountability.
Effect	Impact of the condition	The statement of impact answers the question "So what?" It explains the adverse impact to the operational or control objective. By articulating impact and risk, the element of effect is very important in helping to persuade auditee management to take corrective action.
Recommendation	Suggested corrective action	While the corrective action should eliminate the problem or deficiency noted in the condition, the corrective action should be directed toward addressing the cause.

Source: ISACA, *Information Systems Auditing: Tools and Techniques—IS Audit Reporting*, USA, 2015. Reprinted with permission.

Enjoying this article?

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

meeting the audience face-to-face and providing further detail. However, due to the size, complexity and geographical dispersity of some enterprises, this is not always possible.

I had the honor of working with a colleague on an ISACA committee who overcame this problem by recording the executive summaries on video. The videos were uploaded to a private YouTube channel with the required technical controls (e.g., two-factor authentication). Besides adding context and meaning to the audit reports, it also allowed him to deliver the results with empathy—something that is difficult to get across in a written report.

Reporting/Follow-Up—Track and Measure Progress

ISACA's Information Technology Assurance Framework (ITAF) recommends that a report on the status of agreed-upon corrective actions arising from audit engagement reports, including agreed-upon recommendations not implemented, should be presented to the appropriate level of management and to those charged with governance (e.g., the audit committee).[17] This can be achieved by bringing the recommendations together in an assurance-finding register.

In addition, if these findings are allocated attributes (e.g., significance, status, owner, country, department, region), the data can be analyzed, summarized and presented in a meaningful manner—becoming information. This information can then be used to clearly show compliance to standards and regulations and even act as lead indicators for new initiatives. For further details, see "Enhancing the Audit Follow-up Process Using COBIT 5."[18]

Conclusion

My overall message is that innovation, much like beauty, is in the eye of the beholder. If it is new to the enterprise, it is innovation. Furthermore, innovation does not have to include the latest technology, such as machine learning. Neither does it have to be a revolution; it can be an evolution. To innovate, we auditors do not have to be futurists; we can be "now-ists."[19]

> "INNOVATION, MUCH LIKE BEAUTY, IS IN THE EYE OF THE BEHOLDER."

Endnotes

1 ISACA, "Innovation Insights," USA, 2015, *www.isaca.org/Knowledge-Center/Research/Pages/isaca-innovation-insights.aspx*
2 *Ibid*.
3 Merriam-Webster, "Innovation," *https://www.merriam-webster.com/dictionary/innovation*
4 Cooke, I.; "Audit Programs," *ISACA® Journal,* vol. 4, 2017, *https://www.isaca.org/archives/*
5 ISACA Knowledge Center, Audit Tools and Techniques, *www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/Pages/Overview.aspx*
6 Kress, R.; D. Hildebrand; "How Analytics Will Transform Internal Audit," *ISACA Journal,* vol. 2, 2017, *https://www.isaca.org/Journal/archives/Pages/default.aspx*
7 Cooke, I.; "Doing More with Less," *ISACA Journal*, vol. 5, 2017, *https://www.isaca.org/archives/*
8 ISACA, *CISA Review Manual, 26th Edition*, USA, 2016
9 ISACA, ITAF: Information Technology Assurance Framework, USA, 2014, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx*
10 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/Pages/default.aspx*

11 Chartered Institute of Internal Auditors, "Governance of Risk: Three Lines of Defence," *https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/*

12 ISACA Glossary, *https://www.isaca.org/glossary*

13 Cooke, I.; "Auditing Oracle Databases Using CAATs," *ISACA Journal,* vol. 2, 2014, *https://www.isaca.org/archives/*

14 Cooke, I.; "Auditing SQL Server Databases Using CAATs," *ISACA Journal*, vol. 1, 2015, *https://www.isaca.org/archives/*

15 ISACA, *Information Systems Auditing: Tools and Techniques—IS Audit Reporting*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/information-systems-auditing-tools-and-techniques.aspx*

16 *Op cit* ISACA Glossary

17 ISACA, *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition*, USA, 2014, *www.isaca.org/ITAF*

18 Cooke, I.; "Enhancing the Audit Follow-Up Process Using COBIT 5," *ISACA Journal,* vol. 6, 2016, *https://www.isaca.org/archives/*

19 Ito, J.; "Want to Innovate? Become a 'Now-ist,'" TED, 2014, *https://www.ted.com/talks/joi_ito_want_to_innovate_become_a_now_ist*

Building Tomorrow's Leaders, Today

Stephen Doyle, CISA, CGEIT, PMIIA
Is director, internal audit with the Department of Agriculture and Water Resources in Canberra, Australia. He is responsible for the development and delivery of the internal audit work program and reports to the audit committee. He is the liaison between the department and other audit and assurance providers, including the Australian National Audit Office. Doyle has many years of experience in internal audit and advisory roles since joining Ernst & Young as an IS auditor in 1991, including the delivery of technical and business advice for both government agencies and private organizations. Doyle's internal audit and IS audit-related experience, qualifications and background provide strong support when advising in the areas of organizational risk management and control, enterprise governance, information management and security, and business continuity management. He is also an experienced presenter and educator.

Q: How do you think the role of the IS audit professional is changing or has changed?

A: The role has changed from being primarily a technically focused role to one that is predominantly business focused. The IS auditor must understand the business environment and functions, as well as the supporting technology, in order to truly understand and evaluate risk. Recommendations for improvements to control processes should be cost-effective and practical. To achieve this, the IS audit professional must appreciate the business context and its priorities.

A trend toward the use of outsourced service providers has also influenced the nature of the role. The use of outsourced IT services, for example, often necessitates the establishment of audit and assurance arrangements that are agreed on among the various parties. Depending on the contractual provisions, the IS audit professional may rely on independent assurance providers to undertake work that would previously have been undertaken internally.

There is an increased demand for internal and IS auditors to provide timely advice on governance, risk and control issues, especially for new developments and implementations. IS auditors often find themselves acting as advisors to project boards and technical work groups for application systems being developed or purchased.

Q: What leadership skills do you feel are critical for professionals to be successful in the field of IS audit?

A: The most important leadership skill in the field of IS audit is communication, from clarifying tasks through to conveying strategic direction. In most activities they undertake, auditors need not only to understand and articulate their evaluation of organizational risk, but also to speak with clarity on control objectives and options.

Other critical skills are motivation, the ability to build trust and creativity. A leader needs to be positive and motivated to encourage an effective and pleasant work environment. Given that auditors identify and report on process weaknesses and risk management issues, trust is important to instill confidence that sensitive issues will be handled appropriately. Creativity is needed to maintain effective audit operations with the available resources and to advise on emerging technology risk scenarios.

Q: What is the best way for someone to develop those skills?

A: A broad base of both life and professional experiences is a good start. When choosing employment, look for a role that has opportunities for variable and challenging tasks. Take on a volunteer role. While there are many opportunities to volunteer with ISACA®, there are also opportunities to assist community and charity associations in roles that may provide completely different challenges from the normal nine-to-five.

Seek out and have regular contact with people who can provide mentoring and guidance. It is always beneficial to have feedback on behaviors that may be in your blind spot. Finally, make time for the odd moment of quiet reflection.

Q: What advice do you have for IS audit professionals as they plan their career paths and look at the future information security?

A: There are many career paths for IS audit professionals in information security and it may be useful to think about the different specialty areas and decide on the ones that are of most interest. Of course, there is the requirement to develop an ongoing knowledge and competency in the field. Do

not be afraid to experiment with career choices or change direction as you progress and mature. Be flexible to change and stay true to your values.

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

I undertook my Certified Information Systems Auditor® (CISA®) qualification very early in my audit career and found it invaluable in consolidating my knowledge and skills. It introduced me to what some describe as the 'black art' of IS audit.

While my certifications have enabled me to easily demonstrate my competencies and professionalism, they reveal their true value only when placed in the broader context of the professional association, ISACA. I sometimes wonder what my career might have been without access to ISACA's support, knowledge bases, networking and volunteer opportunities, professional development, research, and publications.

Q: How do you see the roles of IS audit, governance and compliance changing in the long term?

A: I would predict changes in practices and organizational structures, the expertise of auditors and the use of tools will bring about an overall broader role for IS audit, governance and compliance professionals. Increasing use of information technology will result in the reduction of routine tasks such as those associated with data analysis, compliance testing and monitoring.

Chief executives will expect assurance that their organizations are performing well and that their objectives are being achieved. The roles of IS audit, governance and compliance professionals will change accordingly. There will be increased attention on the alignment of processes to support organizational outcomes. The traditional risk management and control activities will be supplemented with analysis of behavioral changes, process complexity and efficiency, costs, and outcomes. There will be improved integration of risk management, compliance, governance and audit functions to support this.

Organizations will expect these roles to provide more predictive analysis of process and risk rather than the traditional "after the event" analysis. Professionals will be asked to apply their insights and contribute as an independent strategic adviser.

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

A: My biggest workplace challenge was to understand the use of enterprise systems across government agencies on behalf of the Ministry of Finance in Singapore with a view to recommending shared services strategies. The task involved having to interview 13 chief information officers (CIOs) over three days.

I was able to use a locally based team for support in arranging meetings and to help with my understanding of, at times, heavily accented English. Planning and review were critical in undertaking the work. Prior to each meeting, we collated a series of questions to ensure that we were able to capture the basic information required. Given that each operating environment was quite different, it was then necessary to explore each agency's use of systems and associated costs, and understand their business processes and the risk of disruption. It was important to have a detailed debrief after each meeting to review our tactics and prepare for the next round.

1 What is the biggest security challenge that will be faced in 2018?

The risk associated with third-party access to systems and information.

2 What are your three goals for 2018?

- Establish a consistent methodology for assessing governance systems and processes
- Explore methods to consolidate analysis across a variety of audit and assurance engagements
- Experiment with different reporting options to provide timely advice on organisational initiatives and developments

3 What is your favorite blog?

I enjoy the blogs on ZDNet and, in particular, Eileen Yu's By The Way.

4 What is on your desk right now?

Chocolate! Thanks to the influence of my staff.

5 What is your number one piece of advice for other IS audit professionals?

Be curious. An auditor needs to be inquisitive to be successful. As Albert Einstein said, "I have no special talent. I am only passionately curious."

6 What is your favorite benefit of your ISACA membership?

The opportunity to volunteer at both the local and international levels and work with people who have had a variety of adventures.

7 What do you do when you are not at work?

I am the primary carer for my wife and we spend time with our two daughters, their spouses and our two grandchildren. Listening to music is a favorite pastime and we are regular concertgoers. I am a keen cyclist. My greatest achievement was cycling from Everett, Washington, USA, to Williamsburg, Virginia, USA—a journey of 5,500 kilometers (3,400 miles) completed in 26 days.


CSX
CYBERSECURITY NEXUS
CYBER SECURITY TRAINING
JUST GOT REAL
NOW YOUR STAFF CAN COMBAT REAL THREATS IN REAL TIME TO BUILD REAL TECHNICAL SKILLS.
Yesterday's lecture-based cyber security training won't protect your organization against tomorrow's advanced cyberthreats. That's why ISACA's new Cybersecurity Nexus™ (CSX) Enterprise Training Platform offers your security team:
On-demand access to 200+ hours of training for less than the cost of one typical course
Practical, hands-on training labs performed in a live, dynamic network environment
Continually updated content based on the latest real-world threats and scenarios
Performance-based assessment of current and prospective employees' technical skills
SCHEDULE A DEMO OF THE CSX TRAINING PLATFORM AT WWW.ISACA.ORG/CSXCYBERTRAINING
ISACA®, the Cybersecurity Nexus™ (CSX) Mark, and ISACA's Cybersecurity Nexus™ (CSX) products, certifications, and services are not affiliated with CSX Corporation or its subsidiaries, including CSX Transportation, Inc.
ISACA

FEATURE

Technology's Role in Enterprise Risk Management

亦有中文简体译本
www.isaca.org/currentissue

The new COSO ERM framework document, *Enterprise Risk Management—Integrating With Strategy and Performance*,[1] is expected to have a level of global influence similar to *Internal Control–Integrated Framework*.[2] The ERM framework is designed to provide reasonable expectation that an entity that adopts it understands and manages all kinds of risk associated with business strategy and performance objectives. It provides a strong foundation for integrating the management of all types of risk. Technology innovation is acknowledged as a key enabler for strategy decision support and an example of a strategic business objective. Technology risk is one of many examples of enterprise risk the document uses to illustrate the ERM framework.

Framework Synergies

Like COBIT 5, the COSO ERM framework is principles-based and emphasizes that strategic plans to support the mission and vision of an organization must be supported with governance elements, performance measurement and internal control. It describes how risk managers in all professions weigh the probability that activities prompted by a given strategy may result in foreseeable future events that impact an entity's mission. Also like COBIT 5, the COSO ERM framework advocates continuous process improvement that relies heavily on governance structures to assist in framing decisions.

ERM framework principles operate as closed-loop systems. Although the specific list of principles differs, both frameworks speak to objective setting, risk prioritization, information system leverage, monitoring and reporting. Just as depicted by the COBIT 5 goals cascade (**figure 1**), some ERM components must be established in cascading order to provide goals for others, but, once established, there is no prescribed sequential order for the continuous operation of risk management activities. Just as depicted by the information flow of COBIT 5 (**figure 2**), processes occur simultaneously and rely on shared information to form a holistic approach to risk management. At a more granular level, the principles are also familiar to cybersecurity professionals who are familiar with prevent-detect-recover, observe-orient-decide-act and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework's identify-protect-detect-respond-recover loops. These all have components that rely on shared goals and strategies and are expected to run simultaneously and support each other.

The corresponding COSO ERM framework diagram appears in **figure 3**. As in the COBIT 5 goals cascade, strategy follows from stakeholder values, and business-related objectives and performance goals follow from enterprise goals. As in the COBIT 5 information flow, information flows from

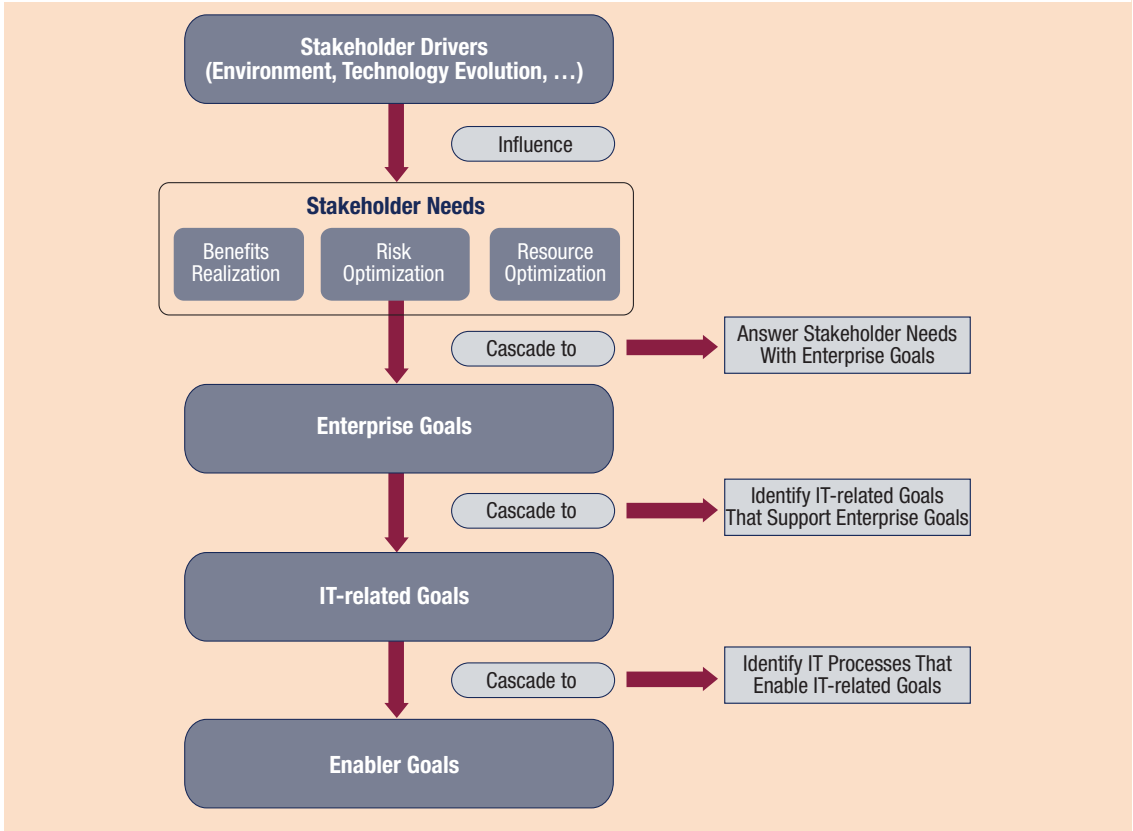
Do you have something to say about this article?

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.

http://bit.ly/2rY4UVJ

Jennifer Bayuk, CISA, CISM, CGEIT
Is a frequent ISACA author and volunteer. She represented ISACA on the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management Framework Committee.

Figure 1—COBIT 5 Goals Cascade



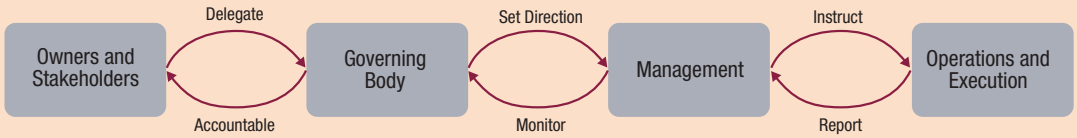
Source: ISACA, COBIT 5, USA, 2012. Reprinted with permission.

stakeholders to governors to management to enablers and back. It is important for technology professionals to understand that ERM framework components are not just paper exercises, but are enterprise-level frameworks that can be leveraged to frame decisions in support of technology risk management objectives. Particularly in the dimensions of governance, strategy and reporting, if technology risk is managed independently of ERM, it is not as likely to be supported from the top down with professional risk management resources.

> “THE COSO ERM FRAMEWORK ADVOCATES CONTINUOUS PROCESS IMPROVEMENT THAT RELIES HEAVILY ON GOVERNANCE STRUCTURES TO ASSIST IN FRAMING DECISIONS.”

The key to effective design and implementation of a technology risk management framework is to recognize that ERM framework components are understood at the board level and to leverage the strengths of the board-level ERM program within the organization to support technology risk management. Of course, there has always been guidance that technology professionals should engage senior management in addressing technology risk. The difference in this version of COSO’s guidance is that it is becoming far more obvious that ERM professionals have a professional obligation to meet technology professionals more than halfway. Although in the past it may have seemed to technology risk professionals that higher-level ERM activities within their organization take technology risk management for granted, this scenario has changed and is rapidly evolving. Cybersecurity threats and other disruptive technology concerns are top of mind for today’s board members.[3]

Figure 2—COBIT 5 Information Flow



Source: ISACA, *COBIT® 5: Enabling Information*, USA, 2013. Reprinted with permission.

In all large enterprises, and in many midsized ones, ERM has long been a formal endeavor to ensure that the mission, vision and core principles of the firm are the basis of strategic planning. These activities drive resource allocation and decision support, clearly articulating the tone at the top. Technology strategy planning, however, often originates with goals of lower-level objectives such as infrastructure migrations, people location strategies, cost cutting and/or development timeline reduction. These are not strategic goals that cascade directly from enterprise mission and values, and sometimes conflict with the technology activities that would more directly support those values. For example, a cost-cutting initiative wherein development activities are targeted to be outsourced may conflict with a goal to streamline customer experience, as the latter goal would require close collaboration among development teams in different business areas. In recognition that the activities of enterprise risk have not always been particularly transparent to stakeholder organizations such as technology, the COSO ERM framework begins with a thorough explanation of the underlying dynamics that are expected to occur between the board and executive management in defining an approach to ERM. It starts with a definition of enterprise risk management: "the culture, capabilities and practices, integrated with strategy setting and performance, that organizations rely on to manage risk in creating, preserving and realizing value."[4]

As the definition spans multiple complex concepts, each concept is described in the context of the challenges inherent in managing risk at the enterprise level. Many of these challenges are also described in COBIT 5. **Figure 4** specifies the sections in both documents that show how the COSO ERM definition relates to COBIT's key principles for governance and management of enterprise IT.[5, 6]

Figure 3—COSO Enterprise Risk Management, Components and Principles

Source: COSO, *Enterprise Risk Management: Integrating With Strategy and Performance*, USA, 2017. Reprinted with permission.

Figure 4—How COSO's ERM Definition Relates to COBIT Key Principles for Governance and Management of Enterprise IT

COSO ERM	COBIT 5
Recognizing culture, developing capabilities	Establishing a holistic approach (Principle 4)
Applying practices	Applying a single, integrated framework (Principle 3)
Integrating with strategy setting and performance	Covering the enterprise end-to-end (Principle 2)
Managing risk to strategy and business objectives	Separating governance from management (Principle 5)
Linking to value	Meeting stakeholder needs (Principle 1)

Although both frameworks are principle-based, and appear similar at a high level, COSO ERM is a higher-level framework as it encompasses consideration of all types of risk, including technology risk. Nevertheless, like COBIT 5, it emphasizes the importance of management unity at the framework level and emphasizes that alignment and integration of potentially separate frameworks are the shortest path to improved decision support.[7,8]

As depicted in **figure 3**, the COSO ERM framework includes 20 principles that are grouped into five framework components:

1. Governance and culture
2. Strategy and objective setting
3. Performance
4. Review and revision
5. Information, communication and reporting

COBIT 5's principles do not map to COSO ERM's principles, but to the technology environment in which ERM's principles operate. That is, the ERM component principles are observed in the definition and execution of COBIT 5's deep dives into the special issues inherent in technology risk management at the COBIT 5 enabler level, rather than at the COBIT 5 framework level.

This is particularly true for the COBIT 5 process enabler, which contains COBIT 5's most prescriptive guidance specific to risk management.[9] COBIT 5 thus delivers more detailed guidance for technology professionals for the successful application of both the COBIT 5 framework and the ERM framework principles. **Figure 5** specifies the sections in both documents that show how COSO framework components and principles relate to COBIT 5 enablers.

"COBIT 5'S PRINCIPLES DO NOT MAP TO COSO ERM'S PRINCIPLES, BUT TO THE TECHNOLOGY ENVIRONMENT IN WHICH ERM'S PRINCIPLES OPERATE."

Risk Information Enabler

The last four rows of **figure 5** specify the sections in both documents that show how COSO ERM performance principles relate to COBIT 5 process enabler APO12 Manage Risk—Key Practices. It shows that, in both COSO ERM and COBIT 5, there is an expectation that risk management relies on data collection and use of that data in risk analysis, risk articulation and risk profiling. This highlights the critical dependency or ERM on risk management information collected in the course of running business processes. It thus puts a spotlight on risk information systems that are increasingly reliant on business analytics tools to provide reports and calculate potential losses based on risk models.

As business analytics systems have become more popular and widespread, data gathering has often been placed in the hands of risk analysts, with the result that end-user computing has become a

Figure 5—How COSO Framework Components Relate to COBIT Enablers	
COSO ERM Component/Principle	**COBIT 5 Primary Corresponding Enabler**
Component 1. Governance and Culture	Culture, Ethics and Behavior Enabler
Component 2. Strategy and Objective Setting	Process Enabler: EDM03.01 Evaluate Risk Management Process Enabler: EDM03.02 Direct Risk Management Process Enabler: APO02 Manage Strategy
Component 3. Performance	Process Enabler: APO12 Manage Risk Process Enabler: MEA01.01 Monitor, Evaluate and Assess Performance and Conformance
Component 4. Review and Revision	Information Enabler: Contextual and Representational Goals for Risk Profile Information Item
Component 5. Information, Communication and Reporting	Information Enabler: Information Model Process Enabler: EDM03.03 Monitor Risk Management Process Enabler: MEA01.02 Monitor, Evaluate and Assess the System of Internal Control.
Principle 10. Identifies Risk	Process Enabler: APO12.01 Collect Data (key output—risk issues and factors)
Principle 11. Assesses Severity of Risk	Process Enabler: APO12.02 Analyze Risk
Principle 12. Prioritizes Risk	Process Enabler: APO12.04 Articulate Risk
Principle 13. Implements Risk Responses	Process Enabler: APO12.05 Define a Risk Management Action Portfolio Process Enabler: APO12.06 Respond to Risk
Principle 14. Develops Portfolio View	Process Enabler: APO12.03 Maintain a Risk Profile
Principle 18. Leverages Information Systems	Information Enabler: Enabling Information for Risk Management
Principle 19. Communicates Risk Information	Process Enabler: EDM01.02 Direct the Governance System Process Enabler: APO08 Manage Relationships
Principle 20. Reports on Risk, Culture and Performance	Process Enabler: EDM03.03 Monitor Risk Management

de facto mode of operation in many risk management departments. Even when their business analytic engines are server-based or use big data analytic software, the risk information databases are often populated with spreadsheets downloaded by risk analysts from a wide variety of disparate systems. Risk analysts sometimes download data without indexes and deal with record-mapping problems by creating their own translation table and formulas. Where multiple such systems exist in the same organization, it is hard to aggregate data across multiple risk domains, and aggregation tools sometimes depend on mapping as well. This situation is so widespread that the Bank of International Settlements produced specific guidance on risk aggregation reporting.[10] This critical dependency on information technology is called out in the COSO ERM framework. That is, the risk that technology supporting ERM may itself be flawed is brought to the highest level of enterprise risk awareness, setting forth a condition for the integration of ERM capabilities as: "When making necessary investments in technology or other infrastructure, management considers the tools required **to enable** enterprise risk management activities"[11] (emphasis added).

The strategic importance of maintaining business analytics systems correctly and effectively is finally getting the board-level attention it deserves. Data structures used to represent the enterprise, its business units and organizational structures are fundamental components of risk management information architecture, and consistency of such

Enjoying this article?

- Read *Getting Started With Risk*. *www.isaca.org/getting-rtarted-with-risk*
- Learn more about, discuss and collaborate on information security management in the Knowledge Center. *www.isaca.org/information-secuirty-management*

structures across risk management domains is essential to complete an accurate profile at the enterprise level.

COBIT 5 addresses this problem in a general manner that is relevant to any business process in the *COBIT® 5: Enabling Information* publication.[12] It describes information as composed of physical, empirical, semantic, pragmatic dimensions that should be transparently articulated. It distinguishes information life cycles into phases for plan, design, build/acquire, use/operate, monitor and dispose. It emphasizes the importance of offsetting quality requirements and corresponding goals. It is the special role of the technology risk management professional to use such tools and techniques to protect the integrity of that information design and data-gathering process for all risk information, not just that related to technology risk. Happily for a technology risk management audience, *COBIT 5: Enabling Information* uses a risk profile as an example of an information item, and provides illustrative data content, information life cycle roles and responsibilities, and quality goals for the risk profile information item.[13]

Key Takeaways

Where technology risk management is aligned with corporate risk management organizations conducting ERM activities at the board level, technology strategic plans may be expected to be in lockstep with the enterprise's mission, vision and core principles. The COSO ERM and COBIT 5 frameworks represent a body of knowledge shared across a large community of practitioners that may be utilized to create that alignment. Technology and cybersecurity risk and audit professionals should be conversant with both frameworks, and be familiar with the integration touchpoints between them. Key takeaways from this overview include:

- Effective technology risk management requires that the ERM framework encompass technology.
- As technology risk management professionals are specialists in risk related to information integrity and availability, they play a special role in ERM. The processes they use to identify, assess, quantify and monitor technology risk apply not just to risk in the technology or cybersecurity category, but should be designed to support the integrity of information used by risk managers in other risk domains.
- Technology professionals are uniquely positioned to identify issues related to risk aggregation strategies, and to support ERM activities with information life cycle process and quality control objectives.
- Where both COSO ERM and COBIT 5 are explicitly used by an organization, both enterprise risk and technology professionals should be educated on how they are compatible and why they should be used together and not separately.

Endnotes

1 In 2014, ISACA and other similarly influential associations affiliated with other risk-management-related professions were invited to participate in a committee focused on enhancing enterprise risk management (ERM) guidance provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which was first published in 2004. COSO is an independent private-sector association sponsored jointly by five major professional associations focused on financial statement integrity: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA). COSO's goal is to provide thoughtful leadership dealing with three interrelated subjects: ERM, internal control and fraud deterrence.

2 COSO's flagship publication, *Internal Control–Integrated Framework*, is also a product of widespread collaboration across numerous industry associations and private sector contributors, and is the foundation for most global organizations' internal control frameworks. There was a multiyear effort when it was first published in 1992, and in a subsequent update in 2013. ISACA participated in that update committee as well.

3 National Association of Corporate Directors, Resource Center: Emerging Issues, USA, 2018 *https://www.nacdonline.org/Resources/BoardResource.cfm?ItemNumber=38149*

4 The Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management: Integrating With Strategy and Performance*, USA, 2017, *https://www.coso.org/Pages/ERM-Framework-Purchase.aspx*

5 *Ibid.*
6 ISACA, *Relating the COSO Internal Control—Integrated Framework and COBIT®*, USA, 2013, *https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Relating-the-COSO-Internal-Control-Integrated-Framework-and-COBIT.aspx*
7 *Op cit* COSO 2017
8 *Op cit* ISACA 2013
9 ISACA, *COBIT 5: Enabling Processes*, USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*
10 Basel Committee on Banking Supervision, *Principles for Effective Risk Data Aggregation and Risk Reporting*, Bank for International Settlements, January 2013, *www.bis.org/publ/bcbs239.pdf*
11 *Op cit* COSO, 2017, p. 19
12 ISACA, *COBIT 5: Enabling Information*, USA, 2013, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product-page.aspx*
13 *Ibid.*

FEATURE

Applying a Technological Integration Decision Framework to Innovation 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.

http://bit.ly/2GsEYo5

亦有中文简体译本
www.isaca.org/currentissue

Innovation is the process of transforming an idea or concept into a functional and marketable value proposition reflecting creative opportunity.[1] Moreover, innovation is a total process of interrelated subprocesses.[2] Thus, innovation includes the creation of an idea or concept and subsequent implementation of the idea or concept as a perceived new product, process, service[3] or strategy.[4] Continually developing innovations could aid an organization in sustaining or acquiring a competitive advantage.[5] However, enterprises often need an innovation framework to support organizational innovation governance.

Business leaders who seek to manage innovation must ensure that personal repositories of knowledge are accessible and available for collaborative efforts.[6] "In order to benefit most from different types of partners, firms need to optimize external search strategies[7,8] and adopt appropriate partnership governance systems."[9] Knowledge sharing positively affects innovation performance and accidental knowledge leakage negatively moderates relationships.[10] Consequently, organizations must balance the inevitable trade-off between knowledge sharing and governance mechanisms.[11] A contextual discussion will take place in the following sections concerning the framing of supply chain innovation strategies supporting innovation governance for selecting appropriate knowledge sharing and governance mechanisms.

Robert E. Davis, DBA, CISA, CICA
Is a freelance information systems audit senior manager/consultant, author and university-level instructor. He has provided data security consulting and information systems auditing services to the US Securities and Exchange Commission, the US Enrichment Corporation, Raytheon Company, the US Interstate Commerce Commission, Capital One, Dow Jones & Company, Fidelity/First Fidelity (Wells Fargo), and other organizations. His workbook credits include *Assuring Information Security*, *Assuring IT Governance*, *Assuring IT Legal Compliance*, *IT Auditing: An Adaptive Process* and *IT Auditing: Information Assets Protection*. He has also authored articles and presented materials addressing information system issues.

Sustaining Innovation Using a Technological Integration Framework

There are stakeholders and societies that assert that organizations have a responsibility to support environmental and social sustainability efforts in a financially responsible manner.[12] As a result, enterprise innovations may necessitate generating socially acceptable benefits and value appropriation. The implication of this is that organizations without sustainable business practices will face dwindling value propositions (and dwindling competitive advantage, by extension). In other words, innovation sustainability necessitates a technological integration selection framework to ensure effective innovation governance.

Regarding social responsibility integration, a powerful linkage exists between environmental compliance and green new product developments (NPDs).[13] Nonetheless, there are problems associated with constructing sustainable supply chain capabilities in the era of global complexity.[14] In response, enterprises have deployed processes to obtain competitive advantages through sustainable business practices—enhancing stakeholder perceptions of corporate citizenship and green technology during various product life cycle stages.

Supporting this perspective, it is worthwhile to consider the manufacturing of automatic teller machines (ATMs) through the product life cycle assessment (LCA) lens. The purpose of the assessment is to determine the overall impact the product has on the environment in support of environmental management and sustainability strategy development. Therefore, an LCA traces an ATM from resource extraction to disposal and incorporates associated byproducts in its evaluation.

National Cash Register Corporation (NCR) was pursuing competitive advantage through differentiation using a customer relationship strategy

that employed global supply chain management using the product LCA lens. NCR gave funding priority to sustainability research and development programs creating new products and improving the manufacturing process. For instance, based on the LCA of ATMs, NCR was extracting energy in the ATM product construction process and creating various byproducts. Thus, NCR's ATM waste products were minimized by incorporating biodegradable materials wherever possible in the production process. Additionally, NCR also used recyclable packaging and packing materials. Last, non-biodegradable materials were becoming a part of NCR's recycling initiative.

Suppliers have a role in enhancing the manufacturer's ability to realize a successful green innovation in product development.[15] Buyer management power assertion can occur through procurement tactics and coordination with the suppliers. Specifically, through leveraging buyer power applied to suppliers, management can influence energy consumption, renewable resource use, pollution, byproduct toxicity and final product component waste. As a compliance requirement, through logics management, organizations can ban suppliers that do not produce sustainable products from the authorized vendors list.

> "APPLYING A TECHNOLOGICAL INTEGRATION DECISION FRAMEWORK ENABLES APPROPRIATE PLATFORM SELECTION FOR GOVERNING INNOVATION."

Principal suppliers in green NPD for environmentally demanding customers and markets can bring environmental and commercial success.[16] Moreover, a strategically close relationship of environmental collaboration between suppliers and the buying firm through technological integration play a role in NPD.[17] Therefore, aligning the organization's

sustainability and business strategies and aligning the organization's management systems and environment performance strategies are critical to implementing effective innovation processes.

Affecting the business strategy is strategic intent directed toward the pursuit of innovation and imagining future endeavors that may lead to redefining an organization's core strategies and related industries.[18] Core value chain activities typically influence business strategy through assessed capabilities.[19, 20, 21] Cross-boundary industry disruptions may, in turn, change value networks to multisided markets.[22] With the increased global competitiveness, development of platforms for IT disruptive advantage and sustainability is a top strategic issue for business leaders.[23]

Selecting an Innovation Platform

Applying a technological integration decision framework enables appropriate platform selection for governing innovation. Platforms are technologies, products or services furnishing crucial resources, enabling the capability to build complementary technologies, products or services.[24] Multisided platforms (MSPs) encompass technologies, products or services connecting different types of customers to one another. An MSP is both a platform and a market intermediary.[25] For technologies, the IT architecture of a platform refers to technology priorities and choices allowing applications, software, networks, hardware and data management integration into a cohesive configuration.[26] As a business formation, organizations are market intermediaries when

employees engage in minimizing search and transaction costs for more than one group of players.[27]

A few necessary steps can assist manager-leaders in setting a platform strategy. First, manager-leaders should decide whether to use an existing MSP, build their own platform, or do both. If the manager-leaders conclude that a third-party MSP can benefit the business, the manager-leaders must determine how many the firm should join. Once manager-leaders know which MSPs are appropriate for the organization, selection or rejection of features or services should occur to enable sustaining a competitive advantage. The enterprise that controls the MSP manages the interface between players and end users and dictates the rules of engagement.[28] Contextually, business formations can address disruptive IT from three abstraction levels employing the technological integration decision framework:

- Defender
- Prospector
- Analyzer[29]

"CONTEXTUALLY, BUSINESS FORMATIONS CAN ADDRESS DISRUPTIVE IT FROM THREE ABSTRACTION LEVELS EMPLOYING THE TECHNOLOGICAL INTEGRATION DECISION FRAMEWORK."

Defender Strategy

It is common for disruptive IT to produce a response from the industries serving the same market.[30] Defender organizations pursue narrow product market domains and rarely make adjustments in their operational technology, structure or methods. They devote primary attention to enhancing efficiency.[31] Some strategy theorists recommend that firms take an aggressive transformation approach by redesigning the business into something entirely new.[32] Recent theoretical and empirical research suggests organizations can simultaneously pursue efficiency and innovative adaptation through a process of ambidexterity.[33] Other strategy theorists suggest there are two strategic business alternatives besides adaptation when confronting a disruptive technology: racing or retreating.[34]

However, organizational transformations can occur with the pursuit of two different efforts in parallel. An enterprise can reposition core business through adapting the current business model to meet customer needs in the altered market and simultaneously create a separate envisioned disruptive IT innovation that will enable future growth.[35] Beneficially, the dual transformation business strategy allows enterprises to harness disruptions repeatedly to build sustainability.

Three themes to guide business strategy development of platforms when addressing disruption are:[36]

- Embrace disruption
- Build shared value
- Dare to be open

Prospector Strategy

Prospectors are change and uncertainty creators that require their competitors to respond, almost continuously seek market opportunities and possess flexible technologies.[37] Innovation intermediaries provide a filtering process for potentially disruptive technologies. Within the intermediary classifications, an often overlooked middle option between unvetted ideas and market-ready products are market-ready ideas developed by the innovation capitalist. Innovation capitalists pursue and evaluate product concepts in the inventor community, develop and refine those concepts, and market the results to organizations. Even so, many large organizations have traditionally acquired single-product enterprises to source innovation externally, particularly within the consumer products and technology sectors.[38]

In contrast, some enterprises have sought market-ready products or businesses without the

assistance of intermediaries. These enterprises typically provide a platform and the resources for start-ups or independent innovators to develop and sell their product ideas.[39] Beneficially, these firms can attract and carefully examine an innovative concept or businesses they might want to acquire through creating captive marketplaces or offering in-house incubation services for external ventures[40] by which radical changes in IT platforms have resulted in revolutionary and pervasive innovations in software development organizations across three innovation types:[41]

- Adopted base technologies
- Produced services
- Selected processes

> "DISRUPTIVE IT BUSINESS STRATEGIES FOR COMPETITIVE ADVANTAGE AFFECT BUSINESS STRATEGIES AND ORGANIZATION PERFORMANCE."

Analyzer Strategy

Analyzers function in two marketplace or product domain types, one stable and the other morphing. The analyzers behave like defenders in stable areas and like prospectors in morphing areas.[42] As applied to IT, the business shaping strategy platforms provide leverage for participants, thereby reducing their risk. Beneficially, shaping platforms allow participants to do more with less. The shaping strategy platform transparently defines standards and practices to guide the activities of large numbers of participants. Additionally, the shaping business strategy fosters specialization among participants. Last, the shaping business strategy for disruptive IT enables increases in value and functionality as more participants join.[43]

The IT industry commonly deploys an *ad-hocracy* organizational structure. Whereby, a primary *ad-hocracy* goal is fostering adaptability, flexibility, and creativity where uncertainty, ambiguity or information overload is typical. A significant challenge for these organizations is producing innovative products and services and rapidly adapting to new opportunities. A strong emphasis is placed on individuality, and risk taking and anticipating the future endure since almost everyone in the organizational *ad-hocracy* takes an interest in every functional aspect of the firm.[44] Given that NCR employees operate under a clan culture, management should deploy innovation governance using an MSP analyzer strategy to obtain a competitive advantage.

Conclusion

Disruptive IT business strategies for competitive advantage affect business strategies and organization performance. IT systems, processes, activities and tasks represent the critical support structure for effective information and communication configurations. Almost every organizational formation aspires to use technology for integrating information, achieving process efficiencies and transforming service delivery into a paragon of effectiveness.[45] However, most organizational formations have come to realize that emphasizing technologies and enterprise-centric solutions will not produce the desired results and a holistic approach is required.[46, 47]

NCR's mission reflects a multisector organization with a second-to-none leadership position in each of their products and services, thereby exceeding the expectations of customers, employees and the community. NCR's vision of quality products and sustained services to every customer and user helps to align the organization's strategy for sustainability. NCR reduced costs by controlling waste and using the waste to generate byproduct products. NCR also has a strong organizational principle to maintain a pollution-free organization. However, NCR can create immediate value by reducing the level of raw material consumption for its principal products by using modern technologies. The presented technological integration decision framework can aid NCR in placing

organizational activities in perspective. Moreover, applying a technological integration decision framework to innovation governance can work toward creating and maintaining value and simplicity in strategy decision-making.

Endnotes

1 Hunter, M.; "On Some of the Misconceptions About Entrepreneurship," *Economics, Management and Financial Markets*, vol. 7, iss. 2, 2012, *https://www.addletonacademicpublishers.com/contents-emfm/129-volume-7-2-2012/1514-on-some-of-the-misconceptions-about-entrepreneurship*

2 *Ibid*.

3 Dasgupta, M.; R. K. Gupta; A. Sahay; "Linking Technological Innovation, Technology Strategy and Organizational Factors: A Review," *Global Business Review*, vol. 12, iss. 2, 2011, p. 257-277

4 Kim, W. Chan; R. Mauborgne; *Blue Ocean Strategy*, Harvard Business School Press, USA, 2005

5 *Ibid*.

6 Zhou, K. Z.; C. Bingxin Li; "How Knowledge Affects Radical Innovation: Knowledge Base, Market Knowledge Acquisition, and Internal Knowledge Sharing," *Strategic Management Journal*, vol. 33, iss. 9, 2012, p. 1090-1102

7 Frenz, M.; G. Ietto-Gillies; "The Impact on Innovation Performance of Different Sources of Knowledge: Evidence from the UK Community Innovation Survey," *Research Policy,* vol. 38, iss. 7, 2009, p. 1125-1135

8 Laursen, K.; A. Salter; "Open for Innovation: The Role of Openness in Explaining Innovation Performance Among UK Manufacturing Firms," *Strategic Management Journal*, vol. 27, iss. 2, 2006, p. 131-150

9 Kim, Y.; S. S. Lui; "The Impacts of External Network and Business Group on Innovation: Do the Types of Innovation Matter?" *Journal of Business Research*, vol. 68, iss. 9, 2015, p. 1964-2973

10 Ritala, P. *et al*.; "Knowledge Sharing, Knowledge Leaking and Innovation Performance: An Empirical Study," *ISPIM Conference Proceedings*, 2013, *https://www.ispim-innovation.com*

11 Yang, D.; "How Does Knowledge Sharing and Governance Mechanism Affect Innovation Capabilities?—From the Coevolution Perspective," *International Business Research*, vol. 4, iss. 1, 2010, p. 154-157

12 Glavas, A.; J. Mish; "Resources and Capabilities of Triple Bottom Line Firms: Going Over Old or Breaking New Ground?" *Journal of Business Ethics*, vol. 127, iss. 3, 2015, p. 623-642

13 Lee, K.; J. Kim; "Integrating Suppliers Into Green Product Innovation Development: An Empirical Case Study in the Semiconductor Industry," *Business Strategy and the Environment*, vol. 20, iss. 8, 2011, p. 527-538

14 Gunasekaran, A.; P. Hong; T. Fujimoto; "Building Supply Chain System Capabilities in the Age of Global Complexity: Emerging Theories and Practices," *International Journal of Production Economics*, vol. 147, 2014, p. 189-197

15 *Op cit* Lee and Kim

16 *Ibid*.

17 *Ibid*.

18 Graetz, F.; "Strategic Thinking Versus Strategic Planning: Towards Understanding the Complementarities," *Management Decision*, vol. 40, iss. 5, 2002, p. 456-462

19 Gottfredson, M.; R. Puryear; S. Phillips; "Strategic Sourcing: From Periphery to the Core," *Harvard Business Review*, vol. 83, iss. 2, 2005, p. 132-139, *https://hbr.org/2005/02/strategic-sourcing-from-periphery-to-the-core*

20 Handfield, R.; R. Sroufe; S. Walton; "Integrating Environmental Management and Supply Chain Strategies," *Business Strategy and the Environment*, vol. 14, iss. 1, 2005, p. 1-19

21 Porter, M. E.; "The Five Competitive Forces that Shape Strategy," *Harvard Business Review*, January 2008, p. 25-40, *https://hbr.org/2008/01/the-five-competitive-forces-that-shape-strategy*

22 Pagani, M.; "Digital Business Strategy and Value Creation: Framing the Dynamic Cycle of Control Points," *MIS Quarterly,* vol. 37, iss. 2, 2013, p. 617-632, *https://misq.org/catalog/product/view/id/1601*

23 Berman, S.; A. Marshall; "Reinventing the Rules of Engagement: Three Strategies for Winning the Information Technology Race," *Strategy and Leadership*, vol. 42, iss. 4, 2014, p. 22-32
24 Hagiu, A.; D. B. Yoffie; "What's Your Google Strategy?" *Harvard Business Review*, vol. 87, iss. 4, 2009, p. 74-81, *https://hbr.org/2009/04/whats-your-google-strategy*
25 *Ibid*.
26 Masa'deh, R. E.; "The Impact of Information Technology Infrastructure Flexibility on Firm Performance: An Empirical Study of Jordanian Public Shareholding Firms," *Jordan Journal of Business Administration*, vol. 9, iss. 1, 2013, p. 204-224
27 *Op cit* Hagiu and Yoffie
28 *Ibid*.
29 Blumentritt, T.; W. M. Danis; "Business Strategy Types and Innovative Practices," *Journal of Managerial Issues*, vol. 18, iss. 2, 2006, p. 274-291
30 Gilbert, C.; M. Eyring; R. N. Foster; "Two Routes to Resilience," *Harvard Business Review*, vol. 90, iss. 12, 2012, p. 65-73, *https://hbr.org/2012/12/two-routes-to-resilience*
31 *Op cit* Blumentritt and Danis
32 *Op cit* Gilbert, Eyring and Foster
33 Mahsud, R.; G. Yukl; G.E. Prussia; "Human Capital, Efficiency, and Innovative Adaptation as Strategic Determinants of Firm Performance," *Journal of Leadership and Organizational Studies*, vol. 18, iss. 2, 2011, p. 229-246
34 Adner, R.; D. Snow; "Old Technology Responses to New Technology Threats: Demand Heterogeneity and Technology Retreats," *Industrial and Corporate Change*, vol. 19, iss. 5, 2010, p. 1655-1675
35 *Op cit* Gilbert, Eyring and Foster
36 *Op cit* Berman and Marshall
37 *Op cit* Blumentritt and Danis
38 Nambisan, S.; M. Sawhney; "A Buyer's Guide to the Innovation Bazaar," *Harvard Business Review*, vol. 85, iss. 6, 2007, p. 109-118, *https://hbr.org/2007/06/a-buyers-guide-to-the-innovation-bazaar*
39 *Ibid.*
40 *Ibid*.
41 Carlo, J. L. *et al*.; "Early vs. Late Adoption of Radical Information Technology Innovations Across Software Development Organizations: An Extension of the Disruptive Information Technology Innovation Model," *Information Systems Journal*, vol. 24, iss. 6, 2014, p. 537-569
42 *Op cit* Blumentritt and Danis
43 Hagel, J.; J. S. Brown; L. Davison; "Shaping Strategy in a World of Constant Disruption," *Harvard Business Review*, vol. 86, iss. 10, 2008, p. 80-89, *https://hbr.org/2008/10/shaping-strategy-in-a-world-of-constant-disruption*
44 Übius, Ü.; R. Alas; "Organizational Culture Types as Predictors of Corporate Social Responsibility," *Inzinerine Ekonomika-Engineering Economics*, vol. 1, iss. 1, 2009, p. 90-99, 2009, *http://www.ktu.lt/en/inzeko*
45 Davis, R. E.; *Assuring IT Governance*, Robert E. Davis, USA, 2011
46 *Ibid*.
47 De Haes, S.; W. V. Grembergen; R. S. Debreceny; "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities," *Journal of Information Systems*, vol. 27, iss. 1, 2013, p. 307-324

Information Security Architecture

Gap Assessment and Prioritization

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.

http://bit.ly/2Erqrs4

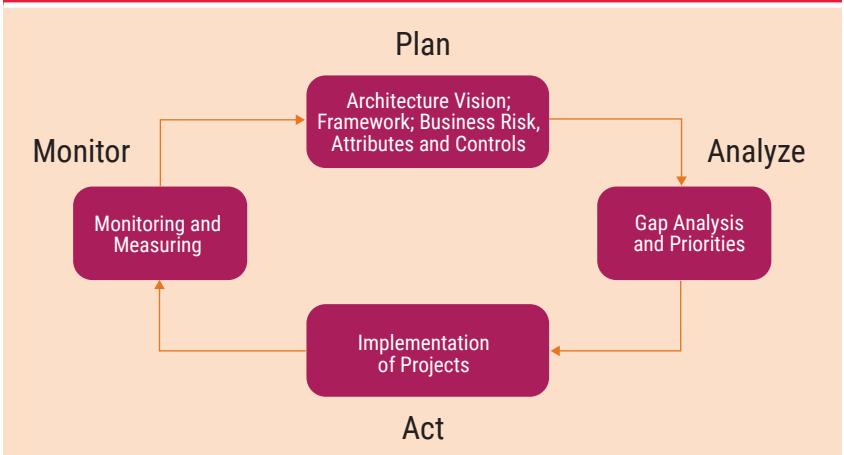
A top-down approach to enterprise security architecture can be used to build a business-driven security architecture.[1] An approach to prioritizing the security projects that are identified as part of architecture assessment while ensuring business alignment follows.

Business risk and attributes can be used to identify relevant security controls and a maturity assessment can be performed to identify the current and desired maturity level of those controls and build an action plan. The steps can be summarized as follows:[2]

1. Select a security framework that is relevant to business such as those developed by the Payment Card Industry (PCI), the US National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO).
2. Understand and document business goals and attributes.
3. Identify the framework controls that are relevant to business and can be verified by business risk.
4. Adjust and customize the controls based on business requirements and operation.
5. Perform a gap analysis and maturity assessment to identify what is missing or incomplete.
6. Develop a program to implement the missing or incomplete controls.

Figure 1 is a summary of these steps and a visual representation of the architecture life cycle.

Figure 1—Security Architecture Life Cycle



Architecture Framework and Gap Assessment

Using frameworks such as COBIT® or ISO 27001 can help identify a list of relevant security controls that can be used to develop a comprehensive security architecture that is relevant to business.

COBIT® 5 for Information Security[3] covers the services, infrastructure and applications enabler and includes security architecture capabilities that can be used to assess the maturity of the current architecture.

Figure 2 illustrates an example of how service capabilities and supporting technologies in COBIT can be used to build a security architecture framework and controls. All identified controls should relate to business risk and attributes.

Maturity Assessment

Once the security architecture framework is developed and the gaps are identified, the next step is to create an implementation plan and specify priorities. This would normally be a long-term program, depending on the size and budget of the organization. This is an important step in the

Rassoul Ghaznavi-Zadeh, CISM, COBIT Foundation, SABSA SCF, TOGAF 9
Has been an IT security consultant since 1999. He started as a computer network and security professional and developed his knowledge around enterprise business, security architecture and IT governance. Ghaznavi-Zadeh is an IT security mentor and trainer and has written books about enterprise security architecture and ethical hacking and penetration.

Figure 2—Service Capabilities and Supporting Technologies

Service Capability	Supporting Technology	Benefit
Provide information security escalation service.	• Vulnerability management • Information security vendor advisories • Industry information security advisories • Escalation hierarchy system (organizationally based) • Information security policies	Timely resolution of information security-related incidents by establishing a hierarchical path for escalation
Provide information security forensics (analysis).	• Memory inspection tools • Network analyzers • Log analyzers • Application and data inspection tools • Reverse-engineering tools • Malware analysis tools • Vendor and OSS forensic tool sets • Network traffic • Malware and code snippets • Security information and event management (SIEM)	Support of the investigation and discovery of information security-related incidents

Source: ISACA, *COBIT® 5 for Information Security*, USA, 2013.

architecture life cycle and should be done carefully in alignment with business requirements. **Figure 3** shows an example of the first outcome of a gap assessment and project planning.

Maturity levels are calculated based on a number of different factors such as availability of required controls, effectiveness of the controls, monitoring of their operation and integrity, and regular optimization.

The list of controls specifies the projects and tasks that need to be done once the gaps are identified. This list could be quite long, depending on the business, and the main question is how to prioritize these tasks and projects.

Risk Management

Risk is commonly categorized into two categories: business risk and operational risk. While business risk is identified by the business and used to define security architecture controls, operational risk includes threats, vulnerabilities and new audit findings, and managing those can complement the controls that are already in place. **Figure 4** offers a view of information security risk sources, including business risk vs. operational risk.

Information security risk is normally calculated using qualitative or quantitative methods. Risk assessment techniques such as The Open Group Open FAIR[4] can be used to assess the likelihood

Figure 3—Security Control Register

Identified Control	Current Maturity Level	Desired Maturity Level	Notes
End-point malware protection	1	3	• Fifty percent of machines lack malware protection. • A host-based intrusion prevention system (HIPS) is not enabled on end points.
Data loss prevention (DLP)	0	2	• There is no DLP solution in place.
Disaster recovery (DR) plan	1	3	• The DR plan is not practiced. • The DR plan is not updated on a regular basis. • An offsite communication plan is not available.

Figure 4—Risk Sources, Business Risk vs. Operational Risk

impact of a risk, calculate a risk score, and identify the appropriate mitigation controls to remediate the risk (**figure 5**).

While not going into a deep discussion about risk management techniques and how they are done, the goal is to have a heat chart for areas of security risk, calculate a severity level for each and assign a risk score to each based on the severity level. For example, a critical risk would have a score of 5, a high risk would have a score of 4, and so on. Two important comments should be made about information security risk assessments:

1. Ultimately, all information security risk should be mapped to business risk. Any information security risk that cannot be related to a relevant business risk is not valid and would not be considered business-critical.

Figure 5—Example of a FAIR Risk Matrix

		Risk				
Probable Loss Magnitude (PLM)	Severe	H	H	C	C	C
	High	M	H	H	C	C
	Significant	M	M	H	H	C
	Moderate	L	M	M	H	H
	Low	L	L	M	M	M
	Very Low	L	L	M	M	M
		VL	L	M	H	VH
		Loss Event Frequency (LEF)				

Source: J. Jones. Reprinted with permission.

Figure 6—Example of a Business Risk Register

Risk	Likelihood	Impact	Remediation Plan
Critical IT failure	Medium	High	Follow DR plan.
Intellectual property (IP) theft	Low	High	Obtain patent protection.

2. Although it would follow the same logic to prioritize the operational risk, this article focuses on and covers only prioritization of the security controls that were identified as part of the security architecture gap assessment. These controls would be used to remediate high-level business risk and would normally be taken from standard frameworks such as COBIT or those developed by ISO or NIST.

Architecture Controls Prioritization

The method used to identify priorities involves a business risk register. Every business has (or should have) a risk register in place. Normally, a business risk register captures overall business risk, its likelihood and impact on business, and a mitigation strategy.

An example of a standard business risk register is shown in **figure 6**.

A heat chart is then built using the business risk captured in the risk register, and a score assigned to each risk, as explained previously (**figure 7**).

> “NORMALLY, A BUSINESS RISK REGISTER CAPTURES OVERALL BUSINESS RISK, ITS LIKELIHOOD AND IMPACT ON BUSINESS AND A MITIGATION STRATEGY.”

To bring this into context, the two examples of risk listed in **figure 6** will have the risk scores shown in **figure 8**.

Figure 7—Risk Heat Chart

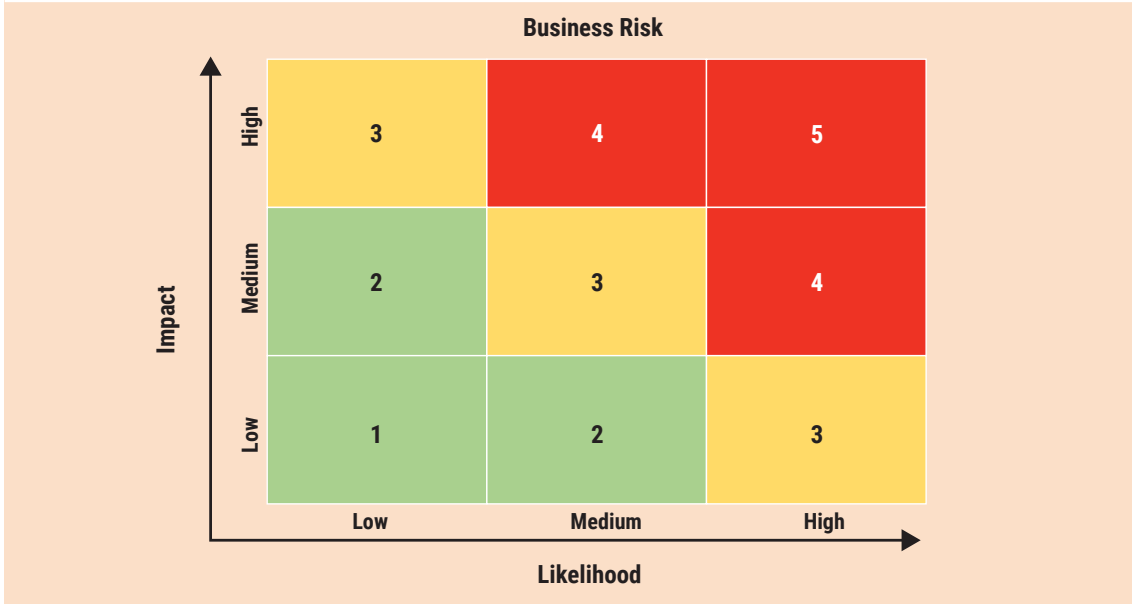


Figure 8—Business Risk Scores

Risk	Likelihood	Impact	Score
Critical IT failure	Medium	High	4
IP theft	Low	High	3

As previously explained, any of the controls identified as part of the security architecture assessment are mapped to a relevant business risk and a relevant information security risk. The business risk score and the information security risk score are used to calculate the overall risk score, as follows:

> Overall risk score = business risk score x information security risk score

This calculation is used to prioritize the implementation.

To explain this with an example, using the control register table shown in **figure 3**, **figure 9** depicts the linking of the controls to the business risk with already identified scores. In addition, assuming the control is not in place, the information security risk score is calculated separately. For example, if the end point malware protection is not in place, the risk of IP theft is quite high (5).

It should be noted that this is a very simple explanation and risk management techniques such as Open FAIR may need a bit more effort to calculate the risk score, but the approach would stay the same.

Using this method, it is easy to prioritize controls or projects and plan their implementation properly. This is useful expertise in managing the architecture life cycle. It will ensure the alignment of security and business priorities and automatically justify them.

In the example shown in **figure 9**, the priority of implementing an end-point malware protection system is much higher than having a DLP solution in place.

Conclusion

Using a business risk register to prioritize security projects is an appropriate approach that not only justifies the life cycle management of security

Figure 9—Security Controls Overall Risk Scores

Identified Control	Relevant Business Risk	Relevant Information Security Risk	Business Risk Score/Impact (1-5)	Information Security Risk Score/Likelihood (1-5)	Overall Risk Score
Endpoint malware protection	IP theft	Endpoint virus/ Trojan infection	3	5	15
DLP	IP theft	Unauthorized access to digital IP	3	3	9
DR plan	Critical IT failure	Unavailability of critical IT services in disaster	4	3	12

projects, but also ensures business alignment and minimizes potential impact.

The essential steps required to ensure that security controls and projects are in alignment with business priorities include:

1. Mapping security controls with business risk scenarios
2. Identifying the information security risk score if the control is not in place
3. Identifying the business risk score for the relevant control
4. Calculating the overall risk score using the formula: Overall risk score = business risk score x information security risk score
5. Prioritizing projects based on the overall risk score

Endnotes

1 Ghaznavi-Zadeh, R.; "Enterprise Security Architecture: A Top-Down Approach," *ISACA® Journal*, vol. 4, 2017, *https://www.isaca.org/Journal/archives/Pages/default.aspx*
2 *Ibid*. See the previous article for more details on this process.
3 ISACA, *COBIT® 5 for Information Security*, USA, 2013, *www.isaca.org/cobit/pages/info-sec.aspx*
4 The Open Group, The Open Group Open FAIR Certification Program, *www.opengroup.org/certifications/openfair*

SPONSORED FEATURE

Centralized, Model-Driven Visibility Key to IT-OT Security Management

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.

http://bit.ly/2Eqo6Or

The threat landscape has changed significantly for operational technology (OT) environments as their connectivity to IT networks and the Internet has exponentially increased. Today, Internet of Things (IoT) devices such as remote sensors transmitting data over Wi-Fi have introduced millions of new access points in organizations responsible for utilities, energy, manufacturing and more. Additionally, there is a greater need to connect OT computer, control and inventory systems to corporate IT networks to better manage the business and production.

Challenges

While connectivity has been a boon to efficiency, it has introduced new risk to both IT and OT environments. In the first half of 2017, an average of 20 percent of industrial control system computers were attacked worldwide each month.[1] As the knowledge, tools and services to carry out these attacks become more widely available, this figure will only increase.

But an even bigger challenge to secure hybrid IT/OT networks is internal. First, the scale and complexity of such networks are immense. Second, their management teams are generally disconnected, working with different processes, technologies and objectives. The gap created between the security management demands of IT/OT networks and the resources available to meet them are where attackers find their opportunity.

To overcome these challenges while maximizing uptime and maintaining safety, organizations need to gain seamless visibility of their entire attack surface. While visibility solutions are available for OT networks, they are not widely in use and not integrated with the IT security program, leaving a large and high-risk blind spot of cyberrisk. To unify IT and OT security management, organizations need to have a centralized solution that gives all teams a common view of the entire network and its risk scenarios.

Threats to OT on the Rise

For attackers, limited visibility and organizational vulnerabilities create a perfect storm. Security experts and governments worldwide are warning of the increased threat to OT networks, including to critical infrastructure.[2] Traditionally, advanced persistent threat (APT) groups or nation-states have given OT engineers the biggest headaches, but the democratization of attack tools and increasing organization of cybercrime are expanding the variety of threats to these networks. Using attack methods commonly seen in IT networks, such as phishing and ransomware, hackers have set their sights on notoriously unpatched—or unpatchable—OT assets to disrupt operations, cause damage, perform reconnaissance or profit the attacker.

In the last two years, there have been major incidents demonstrating what the new threat to OT looks like. WannaCry forced hospitals to turn away patients and brought production lines to a halt.[3,4] NotPetya disrupted radiation monitoring systems at the Chernobyl nuclear site, and cost Maersk alone US $300 million.[5] And Industroyer is largely credited with taking a Kiev transmission substation offline, causing a power outage in the middle of winter.[6]

Ingredients for Unified IT/OT Security Management

Considering these events, boards want to reduce business and operational risk; IT teams want to reduce cyberrisk across all networks; and OT teams want to keep production running smoothly—and safely—without becoming full-time security experts. To meet these objectives, organizations need to have the right tools and processes in place.

First, security teams need to be able to automatically and nonintrusively collect data from various levels

Ron Davidson
Is a 30-year IT veteran who has worked with many of today's leading minds in the security industry. As chief technology officer and vice president of research and development at Skybox Security, Davidson is responsible for advancing product innovation and leading the Skybox Research Lab intelligence group.

of the connected environments, including IT and OT assets, OT protocols, network devices, and firewalls. To make sense of these data, they should be built into a comprehensive, visual and interactive model spanning physical IT and OT, virtual and cloud networks.

An offline model gives IT teams access to the OT network to troubleshoot connectivity, analyze network paths, and simulate potential attack paths between and within different networks, without disrupting production. Understanding the connections between IT and OT gives visibility to the state of the perimeter and whether the appropriate security controls are in place. For instance, the model can show Internet connections to the OT network—a major source of risk, but increasingly common in OT networks where the convenience of IoT devices has outweighed security concerns.

> "THE GAP BETWEEN THE SECURITY MANAGEMENT DEMANDS OF IT/OT NETWORKS ARE WHERE ATTACKERS FIND THEIR OPPORTUNITY."

The model can also be used to assess vulnerability status on demand without an active scan, which is difficult to run in OT environments requiring constant uptime. Scanless assessments utilize other data repositories (patch and asset management systems, network device data and system information). That information is correlated with Common Vulnerabilities and Exposures (CVE) listings, manufacturer advisories and other public vulnerability databases to discover vulnerabilities on demand—even in systems where scanning is not an option.

By combining vulnerability data and threat intelligence with the network model and attack simulations, IT teams have an accurate view of their attack surface and can spot security issues attackers are most likely to target, such as vulnerabilities exposed in the network or actively being exploited in the wild. For example, vulnerabilities used in WannaCry, NotPetya or Industroyer should be top priorities. Intelligent vulnerability prioritization can better facilitate the workflow between IT and OT. During planned production downtime, IT teams can make informed recommendations of patching priorities or other mitigation measures that can cut off vulnerabilities from attack paths.

Take the Holistic Approach

A holistic security management program is one that balances objectives: reducing cyberrisk without sacrificing uptime, availability or safety. To create this kind of program, visibility is the first step. Seamless visibility across IT and OT networks lays the foundation for centralized security management that can mature and adapt even as the organization and the threat landscape evolve.

Endnotes

1 Kaspersky Lab ICS CERT, "Threat Landscape for Industrial Automation Systems in H1 2017," 28 September 2017, *https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/10/KL-ICS-CERT-H1-2017-report-en.pdf*

2 Ashford, W.; "Industrial Control Systems Under Attack, Warns MIT Researcher," *ComputerWeekly.com*, 11 October 2017, *www.computerweekly.com/news/450428010/Industrial-control-systems-under-attack-warns-MIT-researcher?utm_medium=EM&asrc=EM_EDA_83784149&utm_campaign=20171011_Government%20proposes%20changes%20to%20make%20Britain%20safer%20online&utm_source=EDA*

3 Brandom, R.; "UK Hospitals Hit With Massive Ransomware Attack," *The Verge*, 12 May 2017, *https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin*

4 Reuters Staff, "Honda Halts Japan Car Plant After WannaCry Virus Hits Computer Network," *Reuters.com*, 21 June 2017, *https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI*

5 Burton, G.; "Maersk Pins $300m Cost on NotPetya Ransomware," *Computing*, 7 November 2017, *https://www.computing.co.uk/ctg/news/3020561/maersk-pins-usd300m-cost-on-notpetya-ransomware*

6 Greenberg, A.; "'Crash Override': The Malware That Took Down a Power Grid," *Wired*, 12 June 2017, *https://www.wired.com/story/crash-override-malware/*

The Missing Link in Assessing Cyberrisk Factors Through Supply Chains

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.

http://bit.ly/2DLe3SF

In February 2014, one of the biggest discount retailers in the United States, Target Corporation, reported a data breach within its network system that caused the leak of 110 million customers' financial and personal information. Target told reporters that the initial intrusion into its system was traced to network credentials that were stolen from a third-party vendor.[1] An investigation launched by the US Secret Service discovered that the attackers first broke into the retailer's network that previous November.

The hackers used network credentials to obtain access to Target's network, stolen from Fazio Mechanical Services, at the time Target's supplier for heating, ventilation and air conditioning (HVAC) and refrigeration systems. According to a US Senate report, "The vendor did not appear to follow broadly accepted information security practices,"[2] thereby allowing the attackers to compromise Target's network. Various sources have claimed the total cost of the breach as US $252 million and counting. With an offsetting amount of US $90 million in insurance proceeds, the total net expense comes to US $162 million.[3]

Ofir Eitan, CISM, CCSK, CTI
Is a cybersecurity manager at Leumi Card, the second largest payment company in Israel. He is former head of the Israel National Cyber Bureau Situation Room and acting head of the CERT-IL Hotline. Prior to that, Eitan served in the Israeli Intelligence Corps in various positions as an information security officer and a cyberthreat intelligence team leader.

Both Target and Fazio Mechanical Services stated that their IT systems and security measures were in full compliance with industry practices, noting that Target was compliant with the Payment Card Industry Data Security Standard (PCI DSS) at the time of the attack. This claim raised multiple concerns regarding Target's security architecture, design and mitigation efforts. For example, two security concerns arose. First, why did Target provide an HVAC company with credentials to the corporate network? Second, why did Target give the HVAC company access to a network that was not segregated from its payment system network?

In the wake of the Target breach, the threat of cyberattacks using an enterprise's supply chain as a delivery vector has become a common concern within the information security community. This has led to a significant increase in articles researching and analyzing supply-chain cyberthreats. Unfortunately, statistics show that any kind of vendor evaluation is still not widely in use among enterprises. For example, a cybercrime survey published in 2014 by the consulting firm PricewaterhouseCoopers (PwC) shows that only 53 percent of firms in 2013 had a process for evaluating third-party vendors. Surprisingly, the number dropped to 50 percent the following year.[4] Although years have passed since the statistics were published, it is unlikely that the number has changed drastically.

The increasing threat led to the publication of a framework by the US National Institute of Standards and Technology (NIST), which was updated in 2017.[5,6] According to NIST, any organization should identify, prioritize and assess suppliers and partners

of critical information systems, components and services using a cyber supply-chain risk assessment process. Moreover, in 2017, the New York State Department of Financial Services published the regulation 23 NYCRR 500,[7, 8] which is applicable to entities operating under the banking, insurance or financial service law in New York state. The new regulation instructs such firms to implement rigorous third-party cybersecurity risk management policies and procedures across the full life cycle of their relationship with third parties.

Nevertheless, the framework for a cyberrisk assessment of a vendor is still missing an important process. In this regard, a scoring method is necessary for defining the vendors that impose the highest cyberthreat to an enterprise. The methodology in this matter has certainly shown strong development in recent years, e.g., the demand to practice cyber supply-chain risk management (SCRM) monitoring and response.[9] However, risk assessment should first include a theoretical analysis based on a scoring method for defining high-risk vendors. This article offers such a scoring method to help information security managers protect against supply-chain cyberattacks.

> “RISK ASSESSMENT SHOULD FIRST INCLUDE A THEORETICAL ANALYSIS BASED ON A SCORING METHOD FOR DEFINING HIGH-RISK VENDORS.”

It is important to emphasize that a supply-chain cyberrisk can be imposed by an adversary or by an inside threat. Furthermore, any cyberthreat through a supply chain intrinsically means that the vendor has been hacked.

Step 1: Identify Assets

A proper risk assessment process starts with identifying essential assets that contain the enterprise’s critical information. This step is necessary before any mapping process takes place. Once the assets have been mapped, it is important to determine which assets are vulnerable to cyberattacks through supply chains and to classify them according to business risk and priority. Once finished, this process must be documented properly and approved by senior executives.

Step 2: Identify Enemies

As mentioned previously, supply-chain risk factors are characterized by the delivery vectors an attacker can use to hack into a network. Usually these hacks go undetected because supply-chain risk factors are often overlooked. The challenge is to balance the focus between possible delivery vectors and supply-chain risk factors.

The first step to identifying enemies is to consider the main cyberthreats that supply chains pose to an enterprise, such as:

- **Unauthorized remote access/authentication bypass**—Also known as unauthorized access control, this is the theft of a vendor’s credentials that grant remote access.
- **Malware insertion**—Also known as a web service attack, this is using or exploiting granted online access to a network through a vault or a removable-media gateway.
- **Compromising peer-to-peer (P2P) databases using Structured Query Language (SQL) injection**—This is a likely scenario when online access to a database is granted on an enterprise’s website.

- **Embedded backdoor malware**—This could be introduced through the components of programmable parts during the manufacturing process or during testing or loading of operation systems.
- **Denial-of-service (DoS) attack using P2P servers**—This can occur by launching a volume-based attack or an application-based attack (such as an XML attack) once an attacker compromises a vendor's network and the specific servers are in use.

Step 3: Define Important Vendors

An article published by the SANS Institute suggests that the first step toward building a vendor management program is defining the most important vendors.[10] The SANS article emphasizes the importance of classifying mission-critical vendors as high risk. Examples include the organization's important partners, financial and legal services, and hard-to-replace software vendors.

When it comes to delivery vectors for cyberattacks, the sensitivity of data shared with partners is not a key factor. On the contrary, what should be taken under consideration are the network accessibility mechanisms and the frequency of their usage by both the vendor and the employing enterprise. In other words, it is necessary to focus on the delivery vectors to the enterprise's network. More than any other criteria, this is the key to defining supply-chain cyberrisk factors.

Considering this paradigm, the scoring method described here encompasses the following factors to rate vendors:

- **File/code/access type**—This indicator is the core factor regarding the suggested scoring method. It goes without saying that this indicator corresponds directly with cyberthreats to supply-chain processes. Defining the relevant scoring to an enterprise involves a specific approach to every IT platform.

  Figure 1 presents a majority of the connectivity platforms of supply-chain processes that were described in step 2. A suggested scoring method is offered as well. Defining the highest scoring option to each ranked vendor is recommended.

- **Data-at-motion frequency**—Due to the online accessibility of services in a client-server model, this criterion does not often make a significant impact when it comes to assessing controls within an internal network.

  This indicator is very useful for defining an IT platform that is used to transfer data or to provide external accessibility, as such functions are frequently implemented for supply-chain processes. For example, an enterprise might not grant remote access to a specific vendor around the clock; however, the service might be available during predefined days or hours. The same applies for software code reviewing and examining components before implementation, the latter of which is executed offline.

> "WHAT SHOULD BE TAKEN UNDER CONSIDERATION ARE THE NETWORK ACCESSIBILITY MECHANISMS AND THE FREQUENCY OF THEIR USAGE BY BOTH THE VENDOR AND THE EMPLOYING ENTERPRISE."

  It is strongly recommended to use a distinguished scoring approach for this indicator. This means, for example, giving the highest score (5) to daily online connections (such as web services), a relatively high score (4) to a weekly application programming interface (API) update and a very low score (1) to occasional processes, such as the installation of a new system.

- **Number of delivery vectors**—As mentioned previously, it is highly recommended to base a supply-chain cyberrisk assessment on the delivery

Figure 1—Cyberthreats of Supply Chain Processes

Cyberthreat	File/Code/Access Type	Scoring	Comment
Unauthorized remote access/authentication bypass	Login authentication, VPN access, etc.	5	This gives direct access to a network, although the score should be defined according to its given credentials.
Malware insertion	Media gateway, P2P, etc.	4	It is recommended to distinguish between levels of policies such as connectivity platforms that grant the transfer of executable files (e.g., .exe, .bat) and those that transfer lower-risk files (e.g., .txt).
Compromising P2P databases using SQL injection/web service attacks	Data-driven applications, integrated web-based applications using open standards	3	Due to third parties frequently using these platforms, it is relatively common and easy for hackers to compromise these databases.
Embedded backdoor malware	Software/hardware implementation	2	While this cyberthreat is usually a risk to nation-state agents, it has increased for other groups recently due to deliberately implemented backdoors by worldwide IT enterprises.
DoS attack using P2P services	P2P gateway, integrating web-based applications using open standards	1	This is a rare threat due to a lack of interest and accessibility on the part of adversaries.

vectors to the enterprise's networks. Therefore, the number of both connectivity and gateway platforms is significant when one intends to define the highest-risk potential vendors.

As with the previous indicator, it is advised to embrace a distinguished scoring approach when it comes to scoring the amount of delivery vectors from a specified vendor. For instance, when it comes to cyberrisk, the difference between one delivery vector and four delivery vectors in total is enormous, whereas the gap between three and four delivery vectors is less significant.

To complete the scoring method, the appropriate best-practice equation(s) should be implemented:

- **Risk**—According to the known equation, risk equals severity multiplied by probability. In this case, regarding vendor definition, the risk should be normalized and, therefore, it equals the multiplication of file/code/access type, data-at-motion frequency and the number of delivery vectors.
- **Security controls**—Security controls are safeguards or countermeasures to avoid, detect, counteract or minimize risk factors to physical property, information, computer systems or other assets. The range of security controls is large and typically strongly tied to the enterprise and its network's characteristics. To fulfill the security controls criterion, one should execute sufficient business processes mapping, which should include the mapping of security controls related to the supply-chain processes.
- **Residual risk**—According to risk assessment best practices, residual risk is an assessment of the risk a supplier or vendor would impose after the analysis of the implemented controls, mainly from the information security realm.

Figure 2 presents the scoring method for assessing the residual risk that vendors may impose on an enterprise. **Figure 3** offers a blank scoring method for readers' own use, and **figure 4** provides a blank cyberthreats assessment for readers' own use.

Step 4: Planning the Security Program

Once the risk assessment process is complete, the next step is to consolidate mitigation plans as necessary regarding major vendors. This phase is strongly individual to the enterprise and, therefore, includes multiple considerations. It is imperative to use the best practices associated with each consideration. For readers seeking foundational knowledge about this phase, ISACA's Threats and Controls database[11] is recommended. The database's controls are categorized in six groups: architecture, data management, hardware, network, software and user management.

Figure 2—Supply Chain Cyberrisk Factors Scoring Method

Third Party	File/Code/ Access Type	Data-at-Motion Frequency	Number of Delivery Vectors	Risk	Security Controls	Residual Risk
John Doe and Sons Intel Services*	5	5	3	75	Two-factor authentication, antivirus software, sandbox environment, light security information and event management (SIEM) monitoring	55
Jane Doe Big Data Services**	3	4	5	60	API and service-oriented architecture (SOA) gateways, intense SIEM monitoring	35
Baby Doe Computers***	2	2	4	16	None	16

* A corporation has online data analysis using John Doe and Sons Intel Services Software as a Service (SaaS) platform. The services are provided using both multiple vaults for file transfer with the third-party supplier, and remote access is granted to the supplier to specific directories in the corporate network for file-editing purposes.

** The related customer consumes information offline from Jane Doe Big Data Services, using API web services to update various website databases on a weekly basis.

*** Baby Doe is the enterprise's main computer hardware and device supplier. There are no formal or *de facto* information security controls regarding the supplier. Therefore, neither firmware nor operation systems are checked before they are integrated with the corporate network.

Figure 3—Supply-Chain Cyberrisk Factors Scoring Method Sample

Supplier	File/Code/ Access Type	Data-at-Motion Frequency	Number of Delivery Vectors	Risk	Security Controls	Residual Risk

Figure 4—Cyberthreats of Supply Chain Processes Sample

Cyberthreat	File/Code/Access Type	Scoring	Comment

Conclusion

The bottom line is that cyberrisk factors through supply chains are evolving to be a major concern as part of the cybersecurity threat landscape. Although one can find plenty of sources and analysis covering this subject, there is still one framework missing: a scoring method for how to assess and define the risk of each of the third-party suppliers connected to the network. This article provides a comprehensive framework that covers this topic from a supplier-oriented perspective, as opposed to analysis focused on the attack vectors only. Therefore, this framework can be combined and integrated easily in a wider third-party risk assessment process, which analyzes both cyberthreats and the data leakage risk third parties might pose. To that end, the overall risk refers also to the risk of accidentally transferring sensitive data to a third party, in which case the supplier could be used maliciously as a delivery vector to the organization.

Endnotes

1 Krebs, B.; "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 2014, *https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company*

2 US Senate Committee on Commerce, Science and Transportation, "A Kill Chain" Analysis of the 2013 Target Data Breach," USA, 26 March 2014

3 Roman, J.; "Target Breach Costs: $162 Million," Bank Info Security, 25 February 2015, *https://www.bankinfosecurity.com/target-breach-costs-162-million-a-7951*

4 PricewaterhouseCoopers, *The Global State of Information Security Survey 2015*, USA, *https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf*

5 National Institute of Standards and Technology, "Supply Chain Risk Management Practices for Federal Information Systems and Organization," SP 800-161, USA, April 2015

6 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, January 2017, *https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf*

7 New York State Department of Financial Services, *Regulation 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies*, USA, February 2017, *www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf*

8 Ernst & Young, *Cybersecurity Requirements for Financial Services Companies*, February 2017, *www.ey.com/Publication/vwLUAssets/EY-cybersecurity-requirements-for-financial-services-companies/$FILE/EY-cybersecurity-requirements-for-financial-services-companies.pdf*

9 National Institute of Standards and Technology, *Best Practices in Cyber Supply Chain Risk Management*, USA, *https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-FireEye-Cyber-SCRM-Case-Study.pdf*

10 Shackleford, D.; Combatting Cyber Risks in the Supply Chain, SANS Institute InfoSec Reading Room, September 2015, *https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252*

11 ISACA, Threats and Controls Tool, USA, 2017, *https://cybersecurity.isaca.org/csx-threats-and-controls*

Why Cyber Insurance Needs Probabilistic and Statistical Cyberrisk Assessments More Than Ever

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.

http://bit.ly/2nnbgsF

In 2016, there were instances where cybersecurity stocks did not fare well,[1] and one reason attributed to this occurrence was that investors needed some high-profile breaches[2] to lure them back into investing in cybersecurity stocks. It was not too long before the Mirai botnet attack was unleashed.

When such a breach ensues, the result spurs two effects. First, every time a breach such as the Equifax[3] breach is reported, cybersecurity firms gain some financial traction. Second, it creates fear, uncertainty and doubt (FUD) in the minds of C-level executives, which will directly or indirectly spike security spending. Additionally, chief information security officers (CISOs) are constantly pursuing answers to the intangible yet valid concerns of the board. The most common concerns are: What is the top risk to be addressed for the organization? Will the current cyberinsurance policy cover the cost of a data breach? Which specific security investment matters most?

Indrajit Atluri, CRISC, CISM, CISSP, HCISPP, ITILv3
Is an information security professional with vast experience in IT governance, cyberrisk and regulatory compliance. His current focus is on addressing security gaps in emerging technologies, such as the Internet of Things (IoT), big data and security analytics and their implications on information risk and privacy. He is based in Dallas, Texas, USA, and currently provides leadership and guidance to healthcare organizations to improve their risk posture. He can be reached at iatluri@protonmail.com.

What is the amount of exposure for a cloud-hosted application?[4] What is the return on security investment (ROSI) on a previous investment? Even further—with the Equifax breach in mind—what is the financial impact in case a scenario with a similar unpatched Apache Struts application[5] or any other unpatched application(s) arises? Imagine how this same scenario gets more tortuous in a post-EU General Data Protection Regulation (GDPR) era.

It is the general consensus that cyberrisk is surely a business risk. From a business risk standpoint, the most important question to be answered is to know the adequate cyber insurance coverage for an organization to cover its bases in case of a breach. There is no straightforward answer to this today. This entirely depends on several variables, including the risk posture of the organization and the insurance provider, who can, in most cases, is not willing to offer a package that would cover what the business anticipates, as it does not have the right tools or data to estimate the risk posture of the customer.

Cyberrisk Insurance Landscape

Cyber insurance, along with cyberrisk, has become a very common agenda item on the boardroom discussion list in recent times.[6] Both enterprises and insurance companies are finding it difficult to quantify the controls in place and the amount of risk each of the parties is undertaking. Cyber insurance has undergone a substantial evolution from a coverage perspective as there are several new risk factors that were not witnessed or considered before (such as cyberextortion, espionage and privacy breaches).[7]

Cyber insurance coverage is additional to the liability, property and theft insurance that has been traditionally offered. But the challenge here is twofold.[8] Insurers do not have a set baseline or robust setup to evaluate the organization's cyberrisk to determine insurance premiums. Today, most of this is done by leveraging basic questionnaires

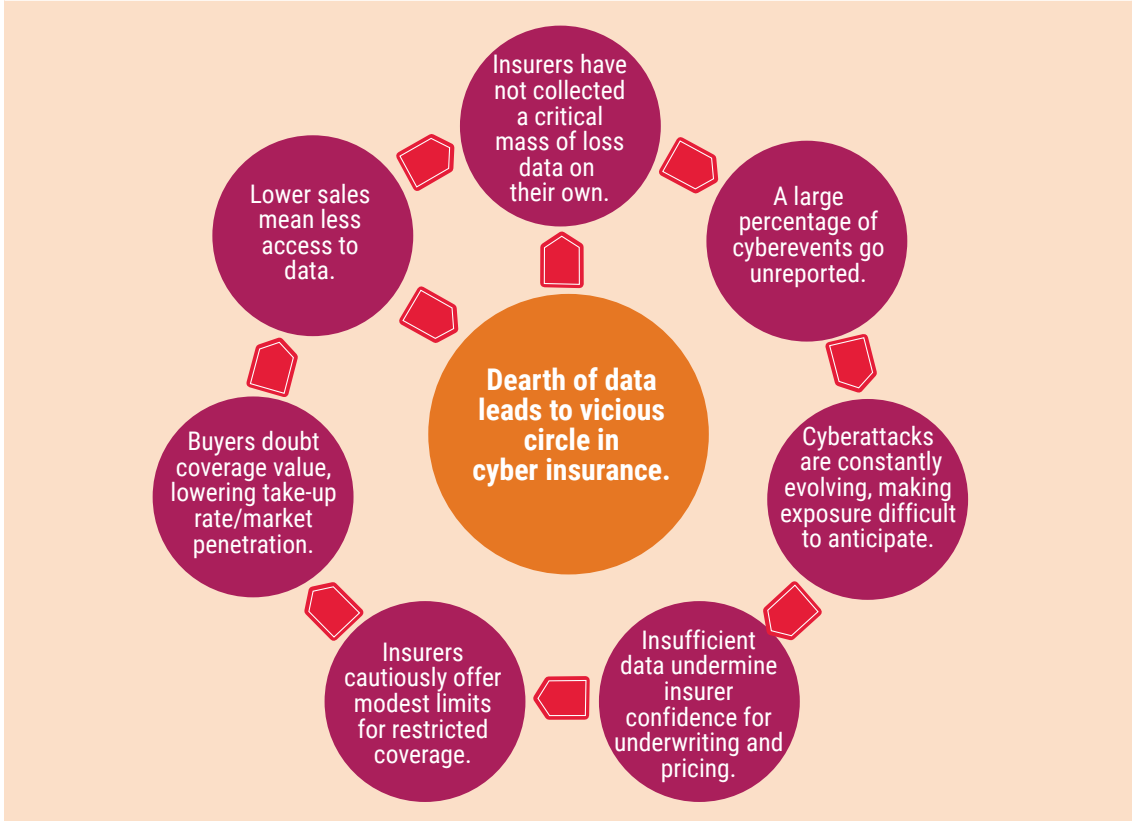
to evaluate the current state of cyberrisk. This practice may result in owning a high risk that could negatively impact the insurance company. On the other hand, if the questions are misinterpreted by the organization, this may result in higher premiums. The post-incident insurance implications are adverse if the organization overstated the controls while acquiring the policy.

Traditionally, auto or home insurance companies provide insurance based on variables such as the driver's age, type of car driven, year a home was built, and proximity to fire and police services. This risk-aware decision-making is possible primarily because the data and metrics have been available for several decades. Similar maturity and metrics are not available for IT risk management, which implies there is a lot of uncertainty. This is where statistics and probability can help. **Figure 1** illustrates that the dearth of data triggers the vicious cycle of cyberinsurance.[9, 10] In fact, it is actually the inability of both the provider and consumer to mine just enough data to estimate the cyberrisk that triggers this vicious cycle.

> "STATISTICAL AND PROBABILISTIC METHODS ARE LEVERAGED WHEN UNCERTAINTY IS INVOLVED."

Fitch Ratings Inc. reported that the Insurance Data Security Model Law was adopted by the US National Association of Insurance Commissioners[11] to promote more rigorous cyberrisk management

Figure 1—The Vicious Circle of Cyber Insurance

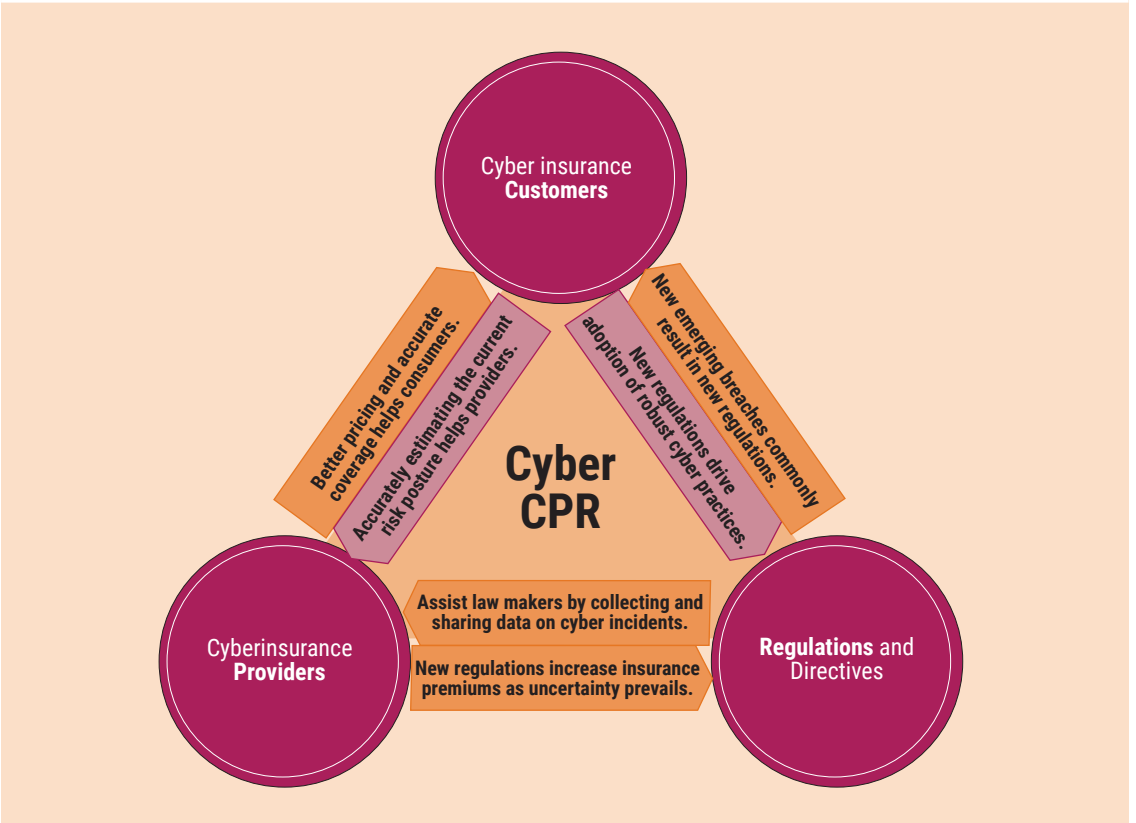


Source: Deloitte University Press. Reprinted with permission.

practices. They point out that limited historical data loss, varying policy language, and terms and challenges in quantifying risk aggregations present considerable uncertainty for insurers. Any slight reduction in this considerable uncertainty would enhance the current state. Statistical and probabilistic methods are leveraged when uncertainty is involved. This article provides evidence that statistical and probabilistic risk assessments can help both parties arrive at a conclusion as to how much risk is being transferred in quantitative terms.

In lieu of the vicious cycle of cyber insurance mentioned previously, a (cyber)consumers, providers and regulators (CPR) cycle in **figure 2** is proposed, and it can enable robust cybersecurity and risk practices if harmony is attained and maintained. The triangle illustrates that the cyberinsurance providers, customers and regulations such as GDPR, Payment Card Industry (PCI), US Health Insurance Portability and Accountability Act (HIPAA), and US Sarbanes-Oxley Act (SOX) are interdependent and together can contribute to improve the state of cybersecurity and insurance. Increases in the number of breaches often result in new regulations that drive insurance providers to raise the cost of coverage. This is conspicuously evident in the case of the upcoming GDPR rollout.[12] In a different vein, new regulations also drive cyber insurance customers to adopt more stringent security controls (possibly reducing future breaches), and with insurance coverage rising, they are forced to accurately estimate potential risk. This would stabilize the coverage price and enforce providers to optimize coverage level. The US Department of Homeland Security emphasizes that a robust cybersecurity insurance market could help reduce the number of successful cyberattacks.[13] Accurately estimating the potential cyberrisk is a good place to start for a security and risk professional. From a security program perspective, the burgundy arrows in **figure 2** should be the top priority to reap the benefit of better coverage at

Figure 2—(Cyber)Consumers, Providers and Regulators (CPR) Cycle



optimal cost and to reduce the number of breaches in the long haul.

Due to recent data breaches, more CISOs have been hired globally in recent times, and some of these individuals have finally procured their long-craved seat at the boardroom table. This simply means that the CISO has an increased responsibility to inform the board of the current risk state and share meaningful security metrics so the board is well informed to make the right decisions. Making the right decisions has paramount importance as enterprises may be able to avert major financial risk and possible reputational damage or even prevent going out of business. This includes securing a robust cyber insurance policy that covers any cataclysmic risk. When these decisions are primarily based on risk assessments, it is critical to use methods that function and, most importantly, measure how well these risk assessment methods work. After all, one cannot manage what one cannot measure. Before all else, a baseline for common cyberrisk language needs to be established.

> "BEFORE ALL ELSE, A BASELINE FOR COMMON CYBERRISK LANGUAGE NEEDS TO BE ESTABLISHED."

Terminology Consensus

"Risk," "vulnerability," "threat" and "asset" each have a contextualized meaning and are often used interchangeably with one another. For example, malicious insiders, weak passwords, nation-state actors, cybercriminals, hacktivists and network shares are not risk. But the taxonomy in most organizations today concerning risk is that most of these are misinterpreted as a potential risk. Risk practitioners need to have a nomenclature consensus and adept understanding of the difference between a threat, threat agent, vulnerability, asset and risk. A common vocabulary harmony needs to exist not only within organizations, but also among insurance providers, law enforcement and corporations, which greatly assists in executing the cyber CPR efficiently. This is best attained by practice and training. Further guidance can be found in the Factor Analysis of Information Risk (FAIR) book.[14]

Quantitative Cyberrisk Assessments Today

It has been relentlessly advocated that attributing numbers to colors on a heat map will not make it a quantitative risk assessment. **Figure 3** is a simpler version of the risk matrix example to explain the range compression problem with heat matrices. Two risk scenarios follow:

- **Risk A**—Likelihood is 40 percent, Impact = US $6 million
- **Risk B**—Likelihood is 80 percent, Impact = US $1.5 million

The risk is evaluated by multiplying impact and likelihood. Clearly the expected loss for Risk A, US $2.4 million, is much greater than the expected loss for Risk B, US $1.2 million.

But the risk matrix depicts otherwise. It shows Risk A to be a medium risk and Risk B to be a high-level risk, which is just the opposite of what the mathematical evaluation of the expected loss suggests.

Figure 3—Simple Heat Map

Likelihood	Impact		
	<US $1M (Minor)	US $1M-$10M (Moderate)	≥US $10M (Catastrophic)
High (>75%)	Medium	High	High
Medium (>25%-75%)	Low	Medium	High
Low (≤25%)	Low	Low	Medium

Change is an unwelcome nemesis anywhere in any form. The priority of organizations, especially dealing with cybersecurity, should be to drive a change in the thought process around adopting probabilistic quantitative risk assessments and clear any misconceptions.[15] "Culture eats strategy

for breakfast"[16] appropriately describes how organizations blindly adopt the proposition to leverage quantitative cyberrisk measurement models based on age-old practices, myths about data availability and statistical ignorance. And sometimes, organizational politics also play a major factor. The blatant fact here is that quantitative risk assessments based on probabilistic models need to be adopted as a standard to help make better, more accurate decisions. Unfortunately, most leading frameworks and consortiums still use heat maps.

> "THE THREE MAIN STEPS IN FAIR INCLUDE DEFINING THE SCOPE, PERFORMING THE RESEARCH AND MAPPING IT TO THE FAIR MODEL."

Quantitative Cyberrisk Assessments That Matter

Research makes it clear that the following facts can help move the progression of cyberrisk assessments one step further:

- Cyberrisk assessments need to adopt quantitative methods based on probabilistic models.[17]
- Heat maps are not accurate and do more harm than good, and there is no single study to prove that these methods have reduced risk.[18]
- Commonly available security metrics that are leveraged today do not represent the state of security accurately and, hence, are of little help in making informed decisions to manage risk efficiently.[19, 20]
- The right balance between accuracy and precision is necessary. Ranges, not precise values, help in defining the state of risk.[21]
- The cybersecurity field has enough data points to make an inference statistically. Fewer data points imply higher uncertainty, which is where statistical quantitative risk assessments help.[22, 23]

"We use probability because we lack perfect information, not in spite of it."[24] One key element addressed in the book from which this quote is taken is that statistics help in estimating rarely occurring events with minimal or just enough data sets.

Key Elements—Analysts, Data and Tools

It is well known that three elements—people, process and technology—form the crux of any successful business transformation. Similarly, for risk estimation, the three elements that are key for quantitative cyberrisk analysis are skill of analysts, having just enough data and leveraging commonly available tools.

The skill of analysts is to extract the data that matters and perform a reasonable estimation. Consider the bald tire scenario[25] when explaining the interpretation of risk terms and mental calculations made by practitioners based on invalid assumptions. The point is that inaccurate assumptions will jeopardize the entire risk analysis exercise. After acquiring enough data, statistical methods can be implemented using commonly available tools, such as Microsoft Office Excel, FAIR-based software or tools like Analytica by Lumina.

The FAIR model is a widely adopted model today that utilizes Monte Carlo and Program Evaluation Review Technique (PERT) to estimate risk. Similarly, a model that utilizes some decomposition tactics along with Monte Carlo simulations and Bayes method has been suggested. Simple analyses or prototyping can be performed by leveraging Excel spreadsheets using built-in statistical functions. For complex scenarios and larger organizations, these preliminary evaluations are scalable and can be integrated into enterprise governance, risk and compliance (GRC) solutions by leveraging programming languages such as Python, R.[26]

Case Study: Risk Due to Loss of PHI Data Via Email

To showcase how this can be done, an example to evaluate the risk for an email misdirection or confidential data loss via email described in the FAIR Institute's blog[27] was chosen. The analysis was done

partially using the FAIR method and Excel functions were used to perform the decomposition and estimate expected losses.[28]

The three main steps in FAIR include defining the scope, performing the research and mapping the results to the FAIR model. After these have been established, one can finally make decisions based on the result.

Define Scope

The key elements of any risk scenario are actor, threat type, event, asset and time. Defining the scope of a scenario is a critical step, and it comprises identifying the asset at risk, the threat actor and the effect. Sensitive or critical data in the email are the asset risk here. An internal user is the threat. The user may be a privileged user who has access to sensitive data (such as protected health information [PHI]) or a nonprivileged user who may have access to sensitive data (such as personally identifiable information [PII]). An inadvertent act or an intentional malicious act would have the same effect. Hence, whether the act is malicious or inadvertent does not matter here, unless cybercriminals are included, and they are out of scope for this discussion as it pertains to emails sent by internal users. The effect of this kind of act will be the loss of confidentiality of critical information.

Risk scenarios involved in this scope are described in **figure 4**.

Research and Map

Instead of mapping it to the FAIR model in this step, another model was used to perform the decomposition and analysis. The threat sources in the previous scope are the line items in the spreadsheet shown in **figure 5**. The line items and decomposition can be anything, including applications, threat sources, business units in an organization or vulnerabilities, depending on the preference. This would determine if it is a risk analysis or a risk assessment.

FAIR ontology recommends evaluating the loss event frequency and loss magnitude to evaluate risk. The following are some questions risk practitioners should pose to subject matter experts (SMEs) to evaluate loss event frequency (LEF):[29]

- How frequently are PHI data sent via email, and how many patient records (on average) are in one email?
- How often does an employee deliver an email to an incorrect recipient?
- Is the PHI within the emails encrypted without needing to login to an account to access the reports? If so, that is a vulnerability.

> “THE THREE MAIN STEPS IN FAIR INCLUDE DEFINING THE SCOPE, PERFORMING THE RESEARCH AND MAPPING IT TO THE FAIR MODE.”

Based on the previous responses, the likelihood that the event will happen is evaluated. (See the second column in **figure 5**.) This can also be decomposed further using Bayes methods.[30]

Then the loss magnitude (in the FAIR methodology) can be evaluated in two steps—primary and secondary loss. Loss of productivity and replacement costs occur mostly as primary loss. Legal liabilities/fines, intellectual property loss and reputational damages occur as secondary loss. Incident response costs fall into both primary and secondary loss categories.

For this case study, primary costs are customer service time to handle the email glitch (investigating and responding to the event) and to replace the terminated employee(s) (if such a thing is part

Figure 4—Risk Scenarios in Scope for Data Loss in Unencrypted Email

Threat Type	Threat Actor/Agent/Source	Asset	Threat Effect/Event
Inadvertent/malicious intent	Privileged insider	Customer information	Confidentiality
Inadvertent/malicious intent	Nonprivileged insider	Customer information	Confidentiality

Figure 5—Decomposing the Unencrypted Email Risk Scenario

Event Name	Probability Event Will Happen (Annual)	90 Percent Confidence Interval for Replacement Costs		90 Percent Confidence Interval for Response Costs		90 Percent Confidence Interval for Fines and Judgments		90 Percent Confidence Interval for Reputational Damage		Expected Loss From Replacement	Expected Loss From Incident Response	Expected Loss Fines and Judgments	Expected Loss From Reputation
		Minimum/ Lower Bound	Maximum/ Upper Bound	Minimum/ Lower Bound	Maximum/ Upper Bound	Minimum/ Lower Bound	Maximum/ Upper Bound	Minimum/ Lower Bound	Maximum/ Upper Bound				
Malicious privileged Insider's unencrypted email	60%	$250	$2,000,000	$4,000	$4,000,000	$2,500	$100,000,000	$1,000	$8,000,000	$560,119	$146,461	$53,727,046	$2,240,475
Malicious nonprivileged insider's unencrypted email	30%	$100	$2,000,000	$2,500	$4,000,000	$2,500	$ 100,000,000	$1,000	$8,000,000	$394,087	$903,113	$26,863,523	$1,120,238

of the policy enforcement). There is no loss in productivity as there is no operational disruption. Secondary costs include offering credit monitoring to customers, fines by a regulator if personal credit and/or health information was released, and potential settlements on customer lawsuits. There is also reputational damage, especially if it is a publicly traded corporation. With this in perspective, the Excel template is leveraged to estimate the loss magnitude by decomposing it into observables: replacement cost, response cost, cost in legal liabilities and fines, and reputational cost. Plugging in the calibrated estimates for these decomposition variables using the knowledge and input from the SMEs provides the expected losses shown in **figure 5**. The range for legal liabilities and fines, for example, should include the 4 percent annual global turnover or US $23.7 million dollars (whichever is greater) fine that is levied if GDPR applies to the organization.

> "THE DIFFICULT PART IS GETTING THE ESTIMATES TO BE ACCURATE, AND EXPERTISE ALONE WILL NOT HELP."

The total loss is then evaluated, and a Monte Carlo simulation of 100,000 such scenarios is run (**figure 6**).

Figure 6—Excel Data Table Showing 100,000 Simulations of Cybersecurity Losses

1	0
2	$7,626,387.23
3	$4,335,137.34
4	$10,096.2319
5	$0
6	$6,396,311.78
7	$16,501,834.40
8	$1,646,087.23
9	$4,362,636.36
10	$102,572.34
11	$1,516,337,309.00
12	$3,096,046.53

A histogram is devised (**figure 7**) that helps plot the loss exceedance curve (LEC) in **figure 8**. These mathematical calculations and simulations can be performed easily by leveraging tools such as Excel or R. The difficult part is getting the estimates to be accurate, and expertise alone will not help. Getting the right estimates involves posing the right questions to the SMEs and slowly narrowing down

to a final value. Posing the right questions comes from practice along with tools (e.g., RiskLens' CyberRisk Suite) that come with preconfigured questions that will assist the risk practitioner.

Figure 7—Histogram for a Loss Exceedance Curve

Estimated Loss	Probability of Estimated Loss or Greater
$ -	72.0%
$ 100,000	57.8%
$ 200,000	52.6%
$ 300,000	49.1%
$ 400,000	46.5%
$ 500,000	44.5%
$ 600,000	42.7%
$ 700,000	41.2%
$ 800,000	39.9%
$ 900,000	38.8%
$ 1,000,000	37.8%
$ 1,100,000	36.9%
$ 1,200,000	36.1%
$ 1,300,000	35.3%
$ 1,400,000	34.6%

Making Decisions

Once all of the math is complete, it is time to paint a picture that highlights the current risk state compared to risk appetite. The LEC shown in **figure 8** depicts that there is a 30 percent chance that the loss will be greater than US $2.2 million. Similarly, there is 10 percent chance the loss will be more than US $30 million.

A similar LEC can be plotted after risk treatment is completed and leveraged to depict residual risk. Also, to prioritize which risk to address first, a return on control percentage is evaluated based on reduction in losses after a control implementation and the control cost using the following formula.[31] This offsets the belief that security is not an investment that provides a return.[32]

Return on control percentage =

$$\left[\left\{\frac{\text{Reduction in Losses}}{\text{Cost of Control}}\right\} - 1\right] X100$$

Figure 9 shows sample events that are categorized based on return on control percentage[33] and a response to mitigate, immediately mitigate or track is suggested.

Figure 8—Loss Exceedance Curve

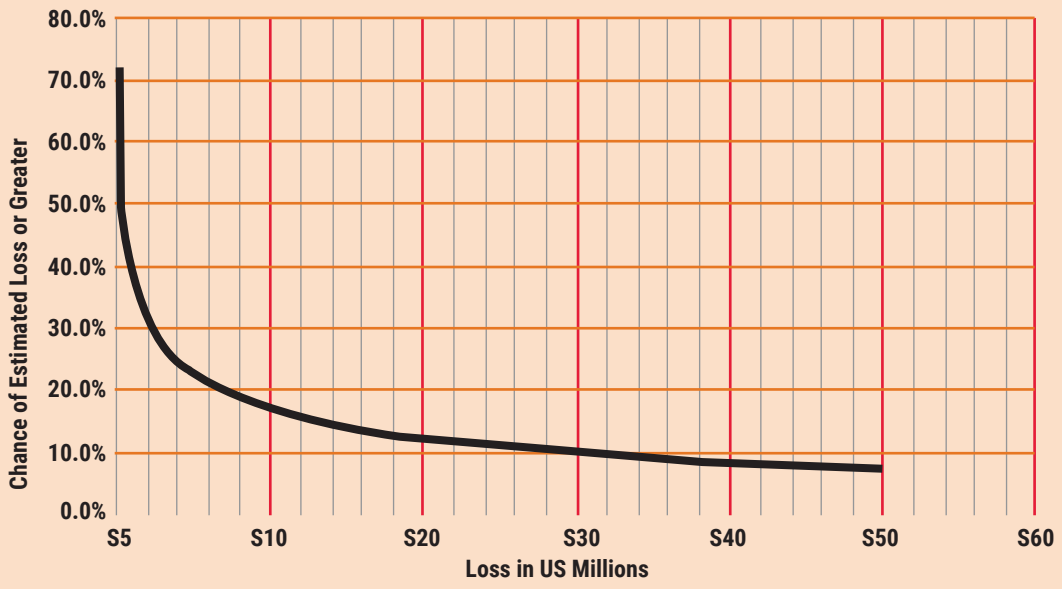


Figure 9—Return on Control					
Scenario/Event	Expected Loss per Year Before Mitigation	Expected Loss per Year After Mitigation	Cost of Control	Return on Control	Risk Response
Unpatched applications	$1.5M	$900K	$50K	1,100%	Mitigate immediately
Data in unencrypted email	$4M	$3M	$700K	42.8%	Mitigate
Unencrypted network traffic	$6M	$5.7M	$1M	-70%	Add to risk register

What Is Next?

Many organizations have already leveraged statistical risk assessments. Work is in progress to make these models widely available and increase awareness of the benefits of embracing uncertainty. All this progress would make it simpler for organizations to evaluate cyberrisk in a meaningful way rather than classifying it as a specific color or assigning it an unrealistic value. This, in turn, will help insurance providers to accurately understand the onus they are bound to undertake and embolden them to come up with better pricing and accurate coverage.

Although these statistical methods include numbers that often perplex boards of directors and CISOs, the fact is that a small patching vulnerability in a web application could result in a breach that can cost millions or even billions of US dollars.[34] There is no doubt that the magnitude will be even higher if such breaches transpire in the GDPR age. One can wait to be part of the historical data or do the actual math (numbers do not lie) upfront to mitigate the risk that really matters. Organizations may not need statistical cyberrisk assessments in the future when historical data are abundant and the uncertainty becomes negligible. But, until then, the goal is to keep reducing that uncertainty.

Endnotes

1 Kenwell, B.; "Jim Cramer—Palo Alto Had a Monster Quarter," *The Street*, 31 August 2016, *https://www.thestreet.com/story/13690555/1/jim-cramer-palo-alto-had-a-monster-quarter.html*

2 Armerding, T.; "The 16 Biggest Data Breaches of the 21st Century," *CSO*, 7 September 2017, *https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html*

3 Zacks Equity Research, "Three Hot Cybersecurity Stocks in Focus Post Equifax Data Breach," 11 September 2017, *https://www.zacks.com/stock/news/275355/3-hot-cybersecurity-stocks-in-focus-post-equifax-data-breach*

4 Jones, J.; "Evolving Cyberrisk Practices to Meet Board-Level Reporting Needs," *ISACA® Journal*, vol. 1, 2017, *https://www.isaca.org/archives/*

5 Newman, L.H.; "Equifax Officially Has No Excuse," *Wired*, 14 September 2017, *https://www.wired.com/story/equifax-breach-no-excuse*

6 Suess, O.; "Fears of Hacking Increase Demand for Cyber Insurance," *Claim Journal*, 10 May 2017, *www.claimsjournal.com/news/international/2017/05/10/278379.htm*

7 Cano, J. J.; "Cyberinsurance—The Challenge of Transferring Failure in a Digital, Globalized World," *ISACA Journal*, vol. 5, 2015, *https://www.isaca.org/archives/*

8 Ishaq, S. K.; "Cyberinsurance Value Generator or Cost Burden?" *ISACA Journal*, vol. 5, 2016, *https://www.isaca.org/archives/*

9 Friedmand, S.; A. Thomas; "Demystifying Cyber Insurance Coverage," Deloitte University Press, 23 February 2017, *https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html*

10 Acrisure, "The Relationship Between Cyber Security Regulation and Cyber Insurance," 23 March 2017, *https://acrisure.com/blog/relationship-cyber-security-regulation-cyber-insurance/*

11 Gonzalez, G.; "NAIC Data Security Model Law a Mixed Bag for Insurers," *Business Insurance*, 16 August 2017, *www.businessinsurance.com/article/20170816/NEWS06/912315213/NAIC-insurance-data-security-model-law-rigorous-costly-cyber-risk-management*

12 JLT, "GDPR Already Influencing Cyber Insurance Buying," 4 July 2017, *www.jlt.com/specialty/our-insights/publications/cyber-decoder/gdpr-already-influencing-cyber-insurance-buying*

13 Department of Homeland Security, "Cybersecurity Insurance," USA, *https://www.dhs.gov/cybersecurity-insurance*

14 Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, UK, 2015

15 *Op cit* Jones

16 Cave, A.; "Culture Eats Strategy for Breakfast. So What's For Lunch?" *Forbes*, 9 November 2017, *https:// www.forbes.com/sites/andrewcave/2017/11/09/culture-eats-strategy-for-breakfast-so-whats-for-lunch/#54e8337a7e0f*

17 Hubbard, D.; R. Siersen; *How to Measure Anything in Cyber Securi*ty, John Wiley & Sons, USA, 2016

18 Hubbard, D. W.; *Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley & Sons, USA, 2009

19 Axelrod, C. W.; "Accounting for Value and Uncertainty in Security Metrics," *ISACA Journal*, vol. 6, 2008, *https://www.isaca.org/archives/*

20 Axlerod, C. W.; "Cybersecurity Risk Metrics…Why Don't They Get It?" 17 April 2017, BlogInfoSec.com, *www.bloginfosec.com/2017/04/17/cybersecurity-risk-metrics-why-dont-they-get-it/*

21 *Op cit* Jones

22 Jones, J.; "No Data? No Problem," FAIR Institute Blog, 18 April 2017, *www.fairinstitute.org/blog/no-data-no-problem*

23 *Op cit* Hubbard and Siersen

24 *Ibid*.

25 FAIR Institute Staff, Video: "What is Risk? The Bald Tire Scenario [Updated]," FAIR Institute, 8 August 2017, *www.fairinstitute.org/blog/video-what-is-risk-the-bald-tire-scenario*

26 Severski, D.; Open Source Toolkit for Strategic Information Security Risk Assessment, *https://github.com/davidski/evaluator*

27 Merritt, R.; "Anatomy of a FAIR Risk Analysis: Confidential Data in Email," FAIR Institute, 30 July 2017, *www.fairinstitute.org/blog/anatomy-of-a-fair-risk-analysis-confidential-data-in-email*

28 *Op cit* Hubbard and Siersen

29 *Op cit* Merritt

30 *Op cit* Hubbard and Siersen

31 *Ibid.*

32 Schneier, B.; "Security ROI," *Schneier on Security*, 2 September 2008, *https://www.schneier.com/blog/archives/2008/09/security_roi_1.html*

33 Hubbard, D.; "Assessing Cybersecurity Risk Within the Finance Office," Government Finance Officers Association, *www.gfoa.org/sites/default/files/AssessingCybersecurityRiskWithinFinanceOffice.pdf*

34 Kim, T.; "Equifax Shares Plunge the Most in 18 Years as Street Says Breach Will Cost Company Hundreds of Millions," *CNBC*, 8 September 2017, *https://www.cnbc.com/2017/09/08/equifax-plunges-as-breach-will-cost-company-hundreds-of-millions.html*

Five Linux Distributions With Tools for Audit

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.

http://bit.ly/2rV2E1a

My father used to say, "Every job is easy with the right tool." Sage advice, but it presupposes that the right tool is available when needed. Sometimes it is not. The "right" tool might be unavailable, challenging (or expensive) to acquire, or out of reach. It is in situations like these where creativity and ingenuity can fill the gaps.

For example, on a recent vacation overseas, I broke my glasses. I was able to repair them using a travel toenail clipper. To say that is not the right tool is an understatement, but being creative in this way allowed me to see (with only a minimum of frustration) until I could get home to my backup pair. The point? Sometimes leveraging what is available can get us around obstacles that would otherwise be crippling to accomplishing our goals.

It is in this vein that it behooves auditors and assessors to know about repositories and collections of special-purpose, freely available tools that they can directly employ to help them in the course of conducting an audit. Believe it or not, there are dozens of such collections in readily accessible, easy-to-use formats that an assessor can just pick up and use to accomplish tasks they might have on their plate. This article identifies Linux distributions that, while their primary purpose is not necessarily audit-related in nature, do provide collections of hundreds or, in some cases, thousands of tools, many of which audit professionals might find valuable. In each case, both the distribution itself as well as an example of how an auditor might employ the tools distributed with it are highlighted in this article.

> "IT BEHOOVES AUDITORS AND ASSESSORS TO KNOW ABOUT REPOSITORIES AND COLLECTIONS OF SPECIAL-PURPOSE, FREELY AVAILABLE TOOLS THAT THEY CAN DIRECTLY EMPLOY TO HELP THEM IN THE COURSE OF CONDUCTING AN AUDIT."

Of course, it bears saying that there are many more out there than those listed here—these are only a starting point. Likewise, there is only so much space available to highlight from among the many, many tools within each distribution (and note that the same tools may be present on more than one environment). That said, the hope is that providing a starting point can help both inform auditors of a potential resource and enable creative options for getting around challenges that might present themselves.

Ed Moyle
Is director of thought leadership and research at ISACA®. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers, and senior security analyst with Trintech. Moyle is coauthor of *Cryptographic Libraries for Developers* and a frequent contributor to the information security industry as an author, public speaker and analyst.

1 BlackArch Linux

BlackArch Linux *(https://blackarch.org/)* is a penetration testing distribution built on the Arch Linux platform. Distribution as a "live" ISO and as a virtual image allows the user to rapidly launch the platform to make use immediately (or nearly so) of its more than 1,900 tools. While the specific tools are focused on penetration testing (as this is the distribution's primary purpose), there is no shortage of tools that might be of interest to an auditor or assessor. Tools such as ssldump or sslmap, for example, can help an assessor validate appropriate configurations for web servers, for example, by allowing them to observe that appropriate ciphersuites are in use and older protocol versions (susceptible to DROWN, POODLE and the like) are not employed. Likewise, tools such as nikto and crawlic can help ensure that a web server configuration is appropriate and in line with requirements (e.g., not containing credentials, temporary files and other undesirable configuration artifacts).

2 Kali Linux

The successor to BackTrack, Kali *(https://www.kali.org/)* is probably the best-known penetration testing distribution in that community. One of the advantages of using Kali specifically is that there is a large body of community-generated "how to" content including instructional videos on how to install the environment and how to employ its tool set. As with BlackArch, there are a number of tools that might be of use to an assessor; for example, a tool such as OpenVAS (an open-source vulnerability scanner) can be used to validate the configuration baseline for hosts on the network or to ensure that document patch management and release processes are being followed. A tool such as nmap can be used to validate that hosts are running only the appropriate services in accordance with defined configuration processes.

3 REMnux

REMnux *(https://remnux.org/)* is an environment designed for security professionals engaged in malware analysis. While most auditors and assessors will not have much call to actively analyze malware, that does not mean that the same tools cannot be of use for an audit task. Tools built into this platform include the network protocol analyzer Wireshark and the network regular expression parser ngrep. These can be used for a range of purposes including ensuring that data exchange is appropriately secured (e.g., that cleartext usernames/passwords are not exchanged).

4 DEFT or CAINE

Distributions that support forensic examination of systems can also assist an auditor in the work they do. For example, distributions such as the Digital Evidence and Forensics Toolkit (DEFT) *(www.deftlinux.net)* or the Computer Aided Investigative Environment (CAINE) *(https://www.caine-live.net/)* are, as one might expect, rife with tools designed to manipulate, view, investigate and otherwise analyze files and file systems. These tools can support efforts of interest to auditors such as evaluation of the appropriateness of file system permissions, validating the existence and operation of data protection tools (e.g., encryption), or any number of other file manipulation tasks.

5 SELKS

This last one, the SELKS platform *(https://www.stamus-networks.com/open-source/)*, is a bit more special-purpose than some of the others. SELKS is a "live" ISO (i.e., a bootable and preconfigured environment) designed specifically to run the Suricata intrusion detection system (IDS) as well as its associated ecosystem and tools. This means that, within a very short period of time, an assessor can stand up a preconfigured IDS/intrusion prevention system (IPS) environment. Why is this helpful in the case of an audit? There are a number of reasons, but the most obvious one is to validate the operation of detective controls, for example, if an auditor wishes to ensure that the IDS, advanced malware detection tools or other controls are operating appropriately. Having an "out of band" way to evaluate events can help as part of that process, particularly when used in combination with earlier distributions (i.e., to generate attack patterns that can be observed by IDS tools.)

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.

http://bit.ly/2rT7Tyn

Q Traditionally, our organization has a policy to adopt established technology solutions. However, new innovative technology-based products are now available that could enhance our business operations, so we are considering adopting these products. What precautions should we keep in mind?

A Until a few years ago, many organizations did not adopt new technologies unless they were proven, stabilized and in use. The primary reason for this stance was to avoid the possible risk of new technology failing to deliver expected results. However, the past two decades have witnessed an evolution and, therefore, revolution in information technology and its use. This has resulted in many new products becoming available to users in rapid succession. Organizations that traditionally adopted a wait-and-watch approach are now forced to adopt new technology-based solutions to stay relevant in the current environment.

Reluctance to adopt new technologies may be because organizational leaders are not willing to invest in new and innovative projects based on traditional return on investment (ROI) measurements rather than looking at enhancements in overall business value.[1] Building a business case using the existing framework of IT strategy aligned to business strategy typically lacks the vision to see the disruption in technology innovations. To overcome this challenge, it is necessary for business leaders to view, as part of business strategy, the technological advances that could disrupt their current view of the marketplace. A case in point is how financial sector organizations have embraced innovations to stay relevant in the marketplace. Some examples of this are mobile banking, automatic payments using near-field communication (NFC) technology and distributed journals using blockchain technology.

Innovations based on technology can be broadly classified into two categories: technology-enabled and technology-centric. The technology-enabled innovations help organizations to become more efficient in delivering services. Technology-centric innovations bring in entirely different approaches that change existing or create new business models. The technology-enabled type is where organizations seem to show more interest.[2] An excellent example of this is the new technology for transaction-oriented payment systems that has been adopted by the banking industry.

The ramifications of the second type of innovations—technology-centric—are typically challenging for businesses to understand. Some of the actions a business could take to better understand such innovations include:

- Setting up a small team whose key responsibilities are to scan the marketplace, look at various innovations taking place and understand their ramifications for the business
- Setting up a small team to try to adopt innovative solutions on a pilot scale to see the impact they would have on the business and IT strategy. This team will require a budget, both for human resources as well as infrastructure, for experimenting with the innovations.
- Conducting a risk assessment to ensure that the risk associated with working with any new technology is within the risk appetite and risk tolerance limits of the organization
- Considering enterprise architecture and how a new solution can be implemented, if it can, within the boundaries of the existing enterprise architecture or to evolve to a better architecture
- Defining a governance framework to measure benefits from new technologies

ISACA® provides guidance for adopting innovations in various ways:[3, 4, 5, 6, 7] The COBIT 5 framework recognizes the importance of innovations and includes guidance on the topic, such as:

- "Product and business innovation culture" under the enterprise goals section Learning and Growth
- "Knowledge, expertise and initiatives for business innovation" under IT goals

In the process reference model, APO04 *Manage Innovation* addresses the need and process to manage innovations within enterprise IT. The six management practices in this process provide appropriate guidance in adopting new technologies in a methodical way.

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.

COBIT 5 also provides guidance on developing metrics for measuring benefits from adopting new and innovative technologies.

Q As a part of performance measurement process for IT, we wish to revisit current performance metrics that were implemented a few years back. Which is the best approach to adopt while reviewing existing metrics and developing new metrics?

A Performance measurement is a requirement for any organization to ensure that the organization's objectives are achieved. This is also applicable to IT-related metrics. The majority of global standards and frameworks, such as ITIL, COBIT 5 and International Organization of Standardization (ISO) standards, prescribe using metrics. COBIT 5 provides a list of generic metrics for each IT-related process defined in its process reference model. ITIL defines three types of metrics: service metrics, process metrics and technology metrics.

When developing these metrics, the sequence of development must be considered since IT is used within organizations for delivering service to the organization's stakeholders (customers).

Service metrics provide an end-to-end measurement of service performance. Some examples of service-level metrics include:

- Results of a customer satisfaction survey that indicate the customers' level of satisfaction with services provided by the organization.
- Cost of executing a transaction or delivering service from the time a customer logs in
- Average time to complete a specific service, not just a process. A service may consist of multiple processes.

Service-level metrics can be used to develop process-level metrics, since a service may consist of multiple processes. Process-level metrics must take input from service-level metrics.

Process metrics measure specific aspects of a process, such as:

- Average time required to complete activities of the process
- Average wait time for a customer to complete a transaction
- Percentage of employees attended on time
- Percentage of services completed within and out of expected time lines

Process metrics provide information about the functioning of processes. Metrics related to critical processes that directly impact customer service levels or achievement of business objectives may be considered for management reporting.

Technology metrics take inputs from service metrics and process metrics to measure specific aspects of the IT infrastructure and equipment such as:

- Response time required for user authentication
- Central Processing Unit (CPU)/bandwidth/storage utilization
- Network status—speed, integrity of information, receipt or acknowledgment
- Average uptime (availability of technology)

COBIT® 5: Enabling Processes[8] provides suggestions for metrics for enterprise and IT goals. It also provides metrics for process goals that can be used to develop metrics for the organization.

Endnotes

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

2 Raval, V.; "Information Ethics: Information Technology and Innovation Ethics," *ISACA® Journal*, vol. 2, 2015, *https://www.isaca.org/Journal/archives/Pages/default.aspx*

3 ISACA, "Innovation Insights," July 2015, *www.isaca.org/Knowledge-Center/Research/Documents/innovation-insights_whp_eng_0615.pdf*

4 *Op cit* Raval

5 ISACA, *Business Innovation Scoring Calculations*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/Documents/scoring-calc_whp_eng_0615.pdf*

6 Delmar, Y.; "Leveraging Metrics for Business innovation: Where Measurement Meets Transformation in IT Governance," *ISACA Journal*, vol. 4, 2014, *https://www.isaca.org/Journal/archives/Pages/default.aspx*

7 ISACA, "What Is COBIT 5?," *www.isaca.org/cobit/pages/default.aspx*

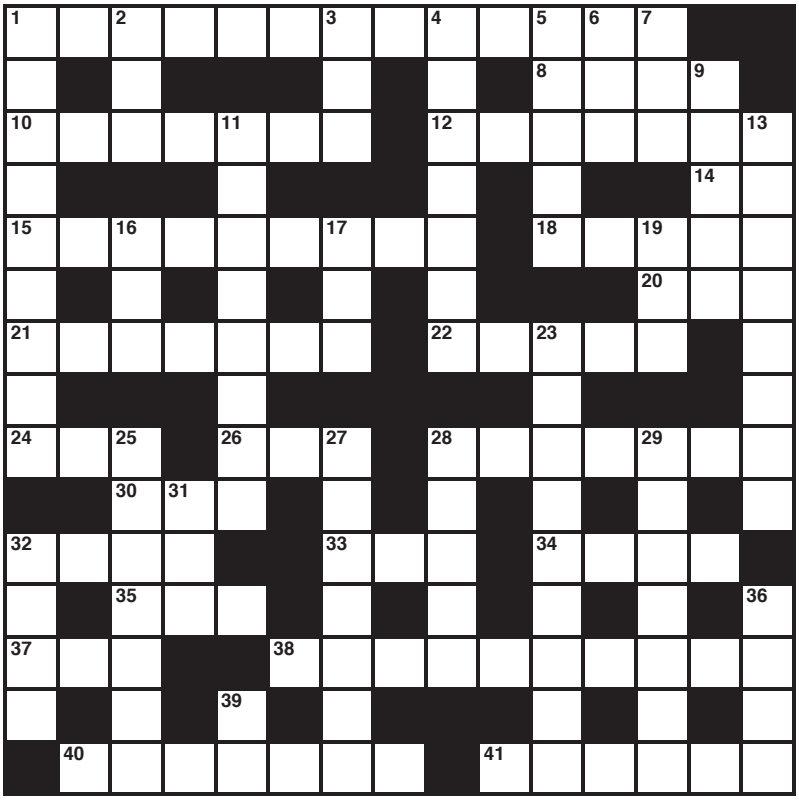
8 ISACA, *COBIT 5: Enabling Process*, USA, 2012, *www.isaca.org/COBIT/Pages/Product-Family.aspx*

CROSSWORD PUZZLE

by Myles Mellor
www.themecrosswords.com

ACROSS

1. Having systems operating in many different spaces and environments
8. Intersect
10. Network serving as an entrance to another network
12. Vulnerability ____
14. E-mail subject line intro
15. Faithful following of a program or regulations
18. Additional
20. X-ray unit
21. Prepare for use, as software
22. Smart
24. Chitchat
26. Printer's paper size
28. Bitcoin and others
30. Revered president
32. Shared facility, for short
33. Arrange
34. Security procedures attempt to prevent or mitigate this
35. Let go
37. Quiet sanctuary, for some
38. See 28 across
40. What backups should enable
41. Joined together



DOWN

1. Changing from one system to another
2. Auction segment
3. Chemical prefix
4. Solutions
5. Visual representation
6. High grade, often
7. Japanese currency
9. ____ firma
11. Effective
13. Mode that enables viewing, but not changing, 2 words
16. Hellos
17. Nada
19. Attempt
23. Watchfulness
25. Adjust loads
27. Lifesaver
28. Keep (from doing)
29. Prerequisite to placing total reliance on any colo-based system
31. White ___
32. Programmer's language
36. Pre-owned
39. CTO is responsible for it

Answers on page 58

CPE QUIZ
#177

Based on Volume 6, 2017—Transforming Data
Value—1 Hour of CISA/CRISC/CISM/CGEIT Continuing Professional Education (CPE) Credit

Take the quiz online.

http://bit.ly/2Eq2OAf

TRUE OR FALSE

BLUM ARTICLE

1. Decentralized directories have been a mainstay of internal control and will remain so under new data sovereignty regulations that are spreading globally.
2. Federated identity capability enables cross-domain single sign-on, attribute management and access control.
3. The principles of the EU General Data Protection Regulation (GDPR) do not address an individual's right to delete or remove records where possible or legally required.
4. The multidomain customer experience has faced challenges at the front end (e.g., weak customer authentication), but not at the back end.

PEARCE ARTICLE

5. Many boards ignore the risk associated with the mismanagement of data. That is one of the reasons that data governance is one of the greatest challenges to corporate governance.
6. The greatest risk boards of directors must protect against is noncompliance with laws and regulations.
7. Data teams must understand the risk of a breach of personal information both before and upon deployment.

AL-MANSOUR ARTICLE

8. Because separation of duties is considered a best practice, system audits are typically performed by a security professional rather than a system administrator.
9. Even though "audit" is a term generally understood to be a technique that is suited for smaller amounts of data, it is still sufficient to describe the security review of a system.
10. Smaller sample sizes make determination of patterns of normal and abnormal behavior easier.
11. Raw data—that is, data that are not delimited or otherwise structured—do not lend themselves to easy system surveys.

PUTRUS ARTICLE

12. Global enterprises are exposed to greater amounts of third-party risk due to the number of third parties and contractors they use. For that reason, they especially need to plan, perform, remediate, monitor and report the results of a risk assessment.
13. Although security breaches and incidents are frequently caused by third parties, PricewaterhouseCoopers reports that the number is neither increasing nor decreasing, but remaining steady.
14. Even when organizations plan, perform due diligence and third-party selection, negotiate contracts, and monitor on an ongoing basis, they must still assume something could go wrong and, therefore, prepare for contract termination or unforeseen contingencies.
15. The process area component of the assessment methodology proposed in the article represents the development steps of the risk register.

GNANA ARTICLE

16. The ISO/IEC 27001:2013 standard requires a Statement of Assessment (SoA), which links risk assessment and risk treatment.
17. Before undertaking an SoA, top management must confirm the organizational perimeter.
18. To build an effective SoA, the organization must focus on all the control objectives identified in the ISO/IEC 27001:2013 standard, even those with minimal/no pertinence to the organization's scope.

KOLBITSCH ARTICLE

19. Some malware now performs evasion techniques to determine whether it is in a sandbox. Three types of evasion techniques focus on user behavior, virtual machine artifacts and timing artifacts.
20. Application.RecentFiles.Count checks the number of files recently accessed. If the count is high, it is unlikely that a human is using the machine, indicating it is a sandbox.
21. The presence of Zone:Identifier metadata generally indicates a virtual machine sandbox.
22. Modern analysis sandboxes are built on full system emulation, which provides instruction-level visibility into the programs under analysis and can, therefore, reason about code paths the malware program did not execute, thus uncovering potential behavior still possible from the malware.

CPE QUIZ
#177

THE ANSWER FORM

Based on Volume 6, 2017

TRUE OR FALSE

BLUM ARTICLE

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

PEARCE ARTICLE

5. _____
6. _____
7. _____

AL-MANSOUR ARTICLE

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

PUTRUS ARTICLE

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

GNANA ARTICLE

16. _____
17. _____
18. _____

KOLBITSCH ARTICLE

19. _____
20. _____
21. _____
22. _____

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current *Journal* subscribers. An electronic version of the quiz is available at *www.isaca.org/cpequiz*; it is graded online and is available to all interested parties. If choosing to submit using this print copy, please email, fax or mail your answers for grading. Return your answers and contact information by email to info@isaca.org or by fax to +1.847.253.1755. 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, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA. Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address. You will be responsible for submitting your credit hours at year-end for CPE credits. A passing score of 75 percent will earn one hour of CISA, CRISC, CISM or CGEIT CPE credit.

Name _____

PLEASE PRINT OR TYPE

Address _____

CISA, CRISC, CISM or CGEIT # _____

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

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

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.

ITAFTM, 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, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

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

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) $75

All international orders:
one year (6 issues) $90.

Remittance must be made in US funds.

ADVERTISERS/ WEBSITES

leaders and supporters

ISACA

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

NEW! ONLINE REVIEW COURSES

Get the training you need. Prepare to obtain your CISA, CRISC, CISM or CGEIT certification and be recognized among the world's most-qualified information systems professionals. ISACA's Online Review Courses provide internet accessible, on-demand instruction and are ideal for preparing you and fellow audit, assurance, control, security and cybersecurity professionals for ISACA's certification exams.

VISIT ISACA.ORG/EXAMONLINEREVIEW TO LEARN MORE.

BROWSE A VARIETY OF PUBLICATIONS FEATURING THE LATEST RESEARCH AND EXPERT THINKING ON STANDARDS, BEST PRACTICES, EMERGING TRENDS AND MORE AT

ISACA.ORG/BOOKSTORE

FEATURED PUBLICATIONS

A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS) by ISACA

This book explains the security requirements, processes and technologies that are required to implement the *Payment Card Industry Data Security Standard (PCI DSS)* which is a compliance requirement for all enterprises that process, store, transmit or access cardholder information for any of the major payment brands, such as American Express®, Discover®, JCB, MasterCard® and VISA® brands.

The guide provides a comprehensive overview of the PCI DSS and explains how to implement its demanding security requirements. The guide also contains a wealth of background information about payment cards and the nature of payment card fraud. The content in this guide goes beyond explaining the requirements by providing the following valued information:

- Concise summaries of the most current PCI DSS requirements Version 3.1 (just released in 2015)
- Consolidated information from numerous PCI Council publications to help the reader better understand the true scope of payment card security
- Techniques to determine the scope of compliance, documenting cardholder data flows and defining the Cardholder Data Environment
- Provides guidance on implementing controls to comply with all 12 PCI DSS requirements and maintain compliance
- PCI DSS requirements mapped to COBIT® 5 processes and International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 270012 controls
- Detailed explanation of compliance requirements for third-party services and cloud computing providers

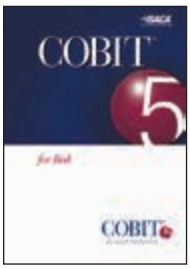
Print Product Code: APG
Web Download Product Code: WAPG
Member price: $35.00
Non-member price: $60.00

COBIT 5 for RISK by ISACA

Risk is generally defined as the combination of the probability of an event and its consequence. *COBIT 5 for Risk* defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

COBIT 5 for Risk provides:

- Stakeholders with a better understanding of the current state and risk impact throughout the enterprise
- Guidance on how to manage the risk to levels, including an extensive set of measures
- Guidance on how to set up the appropriate risk culture for the enterprise
- Quantitative risk assessments that enable stakeholders to consider the cost of mitigation and the required resources against the loss exposure
- Opportunities to integrate IT risk management with enterprise risk
- Improved communication and understanding amongst all internal and external stakeholders



Product Code: CB5RK
Member: US $60.00
Non-member: US $100.00

Web download Product Code: WCB5RK
Member price: $50.00
Non-member price: $90.00

Risk Scenarios: Using COBIT 5 for Risk

Risk Scenarios: Using COBIT 5 for Risk provides practical guidance on how to use COBIT 5 for Risk to solve for current business issues. The publication provides a high level overview of risk concepts, along with over 50 complete risk scenarios covering all 20 categories described in COBIT 5 for Risk. An accompanying toolkit contains interactive risk scenario templates for each of the 20 categories.

Product Code: CB5RS
Member: US $35.00
Non-member: US $70.00

Web Download Product Code: WCB5RS
Member price: $25.00
Non-member price: $60.00

CGEIT Review Manual, 7th Edition by ISACA

The CGEIT® Review Manual 7th Edition is designed to help individuals prepare for the CGEIT exam and understand the responsibilities of those who implement or manage the governance of enterprise IT (GEIT) or have significant advisory or assurance responsibilities in regard to GEIT. It is a detailed reference guide that has been developed and reviewed by subject matter experts actively involved in governance of enterprise IT worldwide.

The manual is organized to assist candidates in understanding essential concepts and studying the following updated job practice areas:

- Framework for the governance of enterprise IT
- Strategic management
- Benefits realization
- Risk optimization
- Resource optimization

The manual is an excellent as a stand-alone document for individual study or as guide or reference for study groups and chapters conducting local review courses, and it can be used in conjunction with *CGEIT® Review Questions, Answers & Explanations Manual 4th Edition*

The manual also serves as a useful desk reference that can be added to the libraries of professionals involved in the governance of enterprise IT.

$50 BONUS SAVINGS! Purchase this book and the eBook version and save $50 on your combined purchase. Amount will automatically be deducted from the checkout cart.

Print Product Code: CGM7ED
eBook Product Code: EPUB_CGM7ED
Member price: $105.00
Non-member price: $135.00

CGEIT Review Questions, Answers & Explanations, 4th Edition by ISACA

The CGEIT® Review Questions, Answers & Explanations Manual 4th Edition is designed to familiarize candidates with the question types and topics featured in the CGEIT exam.

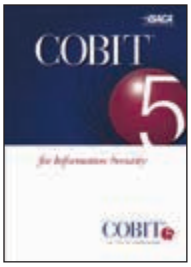
The 250 questions in this manual have been consolidated from the *CGEIT® Review Questions, Answers & Explanations Manual 2015* and the *CGEIT® Review Questions, Answers & Explanations Manual 2015 Supplement.*

Many questions have been revised or completely rewritten to be more representative of the CGEIT 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 CGEIT candidates with an understanding of the type and structure of questions and content that has previously appeared on the exam. This publication is ideal to use in conjunction with *CGEIT® Review Manual 7th Edition.*

Print Product Code: CGQ4ED
Member price: $60.00
Non-member price: $75.00

COBIT 5 for Information Security by ISACA

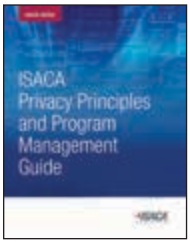
COBIT 5 for Information Security aims to be an 'umbrella' framework to connect to other information security frameworks, good practices and standards. It describes the pervasiveness of information security throughout the enterprise and provides an overarching framework of enablers. The relevant information security frameworks, good practices and standards need to be adapted to suit specific requirements of the enterprise's specific environment. The reader can then decide, based on the specific needs of the enterprise, which framework or combination of frameworks is best to use, also taking into account the legacy situation in the enterprise, the availability of the framework and other factors. For this, the mapping of *COBIT 5 for Information Security* to related standards in appendix H will help find a suitable framework according to relevant needs.



Product Code: CB5IS
Member: US $35.00
Non-member: US $80.00

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: $45.00
Non-member: $90.00

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

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.

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

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

ISACA Privacy Bundle

Purchase the complete ISACA Privacy Bundle and save! These publications are bundled together to provide a discount off the individual list prices.

Print Product Code: IPPSET
Member: $95.00
Non-member: $180.00

Web Download Product Code: WIPPSET
Member: $75.00
Non-member: $150.00

CSX Cybersecurity Fundamentals Study Guide, 2nd Edition by ISACA

The Cybersecurity Fundamentals Study Guide is a comprehensive study aid that will help to prepare learners for the Cybersecurity Fundamentals Certificate exam. By passing the exam and agreeing to adhere to ISACA's Code of Ethics, candidates will earn the Cybersecurity Fundamentals Certificate, a knowledge-based certificate that was developed to address the growing demand for skilled cybersecurity professionals. The Cybersecurity Fundamentals Study Guide covers key areas that will be tested on the exam, including: cybersecurity concepts, security architecture principles, incident response, security of networks, systems, applications, and data, and security implications of evolving technology.

This 2nd Edition accounts for the rapid changes to our global security landscape. It takes a deeper dive into cyberrisk and risk identification, with material from ISACA's CRISC Manual. It also includes updated information on cyber security concepts, such as ransomware, policies and cyber security controls. Architecture principles are updated to consider web application firewalls, SIEM solutions and revised encryption applications. Network security sections are updated to include access controls, wireless network protections, and tunneling. Evolving technology now includes security implications of the internet of things, bit data, artificial intelligence and social media.

Print Product Code: CSXG2
eBook Product Code: EPUB_CSXG2
Member price: $60.00
Non-member price: $65.00

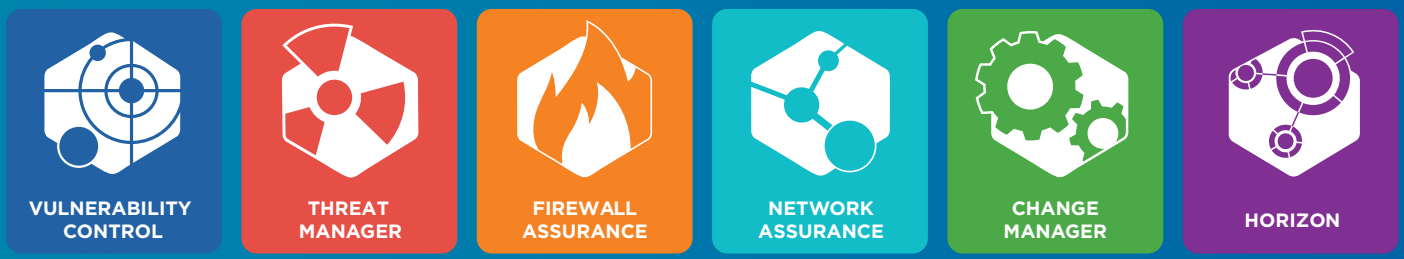
Web Download Product Code: WCSXG2
Member price: $50.00
Non-member price: $55.00

BREAK DOWN SECURITY SILOS.

The Skybox™ Security Suite

MANAGE SECURITY POLICY AND VULNERABILITIES ACROSS PHYSICAL, VIRTUAL, MULTI-CLOUD, AND OT NETWORKS — WITH ONE PLATFORM.

www.skyboxsecurity.com



SKYBOX™ SECURITY

Total Visibility. Focused Protection.™