VOLUME 3, 2020

ISACA Journal

HUMAN ELEMENT OF RISK

+ COMMUNICATING TECHNOLOGY RISK TO NONTECHNICAL PEOPLE

HUMAN ERROR

CASE STUDY—BUILDING A ROCK-SOLID ERM CULTURE ON FAIR

ISACA.ORG

ISACA®

Certify Your Cybersecurity Performance

Build your technical cybersecurity skills online, on demand in CSX's unique live, dynamic network environment. Show you have what it takes to perform cybersecurity tasks with the only comprehensive, performance cybersecurity certification—ISACA®'s award-winning and career-advancing **CSX® Cybersecurity Practitioner**.*

www.isaca.org/csxp-jv3

CSX-P™ CSX Cybersecurity Practitioner™
An ISACA® Certification

*ISACA's CSX® Cybersecurity Practitioner (CSX-P) certification was named 2016 Top Professional Certification program by the SC Magazine Awards.

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®

ISACA® Certifications Are Good…
Too Good Not to Pass Along

Refer your friends to register for a CISA®, CRISC™, CISM® or CGEIT® certification exam. They'll save US$50 off registration and you'll receive a hi-tech reward.

www.isaca.org/cert-referral-jv3

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 May and June.

A Decision Tree to Objectively Determine Policy Compliance
David Doret, CISSP, GRCP, ISO 27001 LA, Lean Six Sigma Green Belt, PMP

Data Rights: Single vs. Multiple Ownership?
Patrick I. Offor, Ph.D., SAP Application Associate

A Fintech Risk Assessment Model
Luis Emilio Alvarez-Dionisi, Ph.D.

Discuss topics in the ISACA® Online Forums: *https://engage.isaca.org/onlineforums*
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/ISACAGlobal*

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, risk management, governance, security, privacy and assurance.

Read more from these *Journal* authors...

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

ISACA®

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

CISOs in the Cloud

Here is an unoriginal observation: The Cloud changes everything. Oh, wait, that was the Internet. Whatever. It seems that if it is novel, it changes everything. So the Cloud makes most of us information security professionals unnecessary. After all, those fortunate few employed by the cloud service providers (CSPs) will take care of everything for us.

If anyone detects a bit of snark in the paragraph above, the reason is I intended to be a little snarky.

While the cloud does certainly alter the rules of engagement for protecting an organization's information resources, it just as certainly does not eliminate the need for an information security function. I would like to make the case that the movement of those resources into the cloud makes the chief information security officer (CISO) and her or his minions even more important.

What CISOs Do

It is a bit difficult to speak authoritatively about how the CISO's position is changing since, in my travels, I have not encountered two CISOs who see the job exactly the same way. There is too much variation depending on industry, organizational scale, technology and, to an extent not usually recognized, the personality and political skill of the individual CISO. That said, there are some commonalities that I believe most CISOs would recognize.

Most CISOs are responsible for issuing and enforcing information security policy and standards. They conduct risk assessments and, on that basis, set short- and long-term strategies. They keep their antennae raised to detect emerging threats and communicate them both to senior management and throughout their organizations.

Most, if not all, CISOs also have tactical responsibilities.[1] Monitoring information system usage for attacks and misuse is, as I see it, the most common component of all CISOs' roles. And then, if and when there is a breach, they manage the response to security incidents.

I said that it is hard to typify what CISOs do; it is even more difficult to state definitively how organizations are currently using cloud services. Some do little more than acquire a few Software as a Service (SaaS) products. Others use the cloud only minimally for archival storage or data backups. Some are in a transitional period, having lifted and shifted their data centers to those of CSPs. For them, the need for security of their information resources is little changed except at the physical layer. Finally, there are those who have re-engineered the way they manage and use information.

What CSPs Do for Security

The common element in all these uses of the cloud is that they relate to services, which are achieved, in part, by transferring facilities and the equipment involved from a customer's site to a CSP's. So, if movement to the cloud (supposedly) reduces the role of a customer's information security function, what security does the CSP provide?

Steven J. Ross, CISA, AFBCI, 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.

Enjoying this article?

- Read *Continuous Oversight in the Cloud.* *www.isaca.org/continuous-oversight*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Let a few of the major vendors explain:[2]

- "Security and Compliance is a shared responsibility between AWS and the customer."[3]
- "Google is committed to doing its part in keeping your projects secure, but security is a shared responsibility."[4]
- "As you consider and evaluate public cloud services, it's critical to understand the shared responsibility model and which security tasks are handled by the cloud provider and which tasks are handled by you."[5]

So then, what exactly is the CSP's share of the responsibility? The answer differs a little from vendor to vendor, but not much.

Amazon Web Services (AWS) says that it is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking and facilities that run AWS Cloud services. (An accompanying diagram on its web page places hardware and its global infrastructure, plus software for compute, storage, database and networking, in Amazon's zone of responsibility.)[6]

Google states its case differently. Its web page on shared security commits the vendor to security over data center physical security, server and software stack security, trusted server boot, and data access and disposal.

Microsoft Azure takes full responsibility for physical hosts, the network and the facilities. It agrees to some responsibility for identity and directory infrastructure, applications, network controls and operating system(s), based on "service types." The exact extent of Microsoft Azure's responsibility is not spelled out in its literature, although I am quite sure that it is in their contracts.

Reduced to the essentials, these three companies, rather dominant in the marketplace,[7] seem to me to be saying to their customers, "We will take care of what is ours. You take care of what is yours." That is not really unfair, but it certainly does raise the stakes for those CISOs whose organizations are migrating to the cloud.

What CISOs Must Do

CISOs are now called upon to keep their own applications and information secure and to ensure that someone else[8] is doing the same with their applications and infrastructure. I think it is fair to say that most CSPs offer little transparency into the details of their security measures. This is justifiable since they do not want to offer a road map to cyberattackers and, so far, their defenses seem to be generally effective. While there is no shortage of Cassandras who tell of the potential for attacks on CSPs,[9] the only significant case I know of was the incident involving the US's Capital One Bank at AWS, and that case involved insider information.[10]

> "IF EVER THERE WAS A TIME THAT INFORMATION SECURITY HAS TO BE A FORETHOUGHT RATHER THAN TAKEN UP AFTER KEY DECISIONS ARE MADE, THIS IS IT."

In addition to everything that CISOs had to do when all of their organizations' information resources were on premises (and, as I have written before, there will always be a residual data center[11]), they must now take on additional duties. In particular, they must occupy key roles in vendor selection and management. If ever there was a time that information security has to be a forethought rather than taken up after key decisions are made, this is it. Selecting cloud vendors is less like a purchase and more like a marriage. The vendors make it easy to enter into a relationship and oh, so hard to get out. The degree of commitment dictates early and ongoing attention to the security of applications, information and infrastructure, both in the cloud and in the building.

Ah, to be a CISO now that the cloud is here.

Endnotes

[1] Or do I have it backwards? The CISOs I am familiar with are in quite strategic roles, but perhaps there are more who are focused more tactically.

[2] Amazon, Google and Microsoft are three of the largest cloud vendors and are listed in alphabetical order. There is no way to represent the position of *all* CSPs, but I have not encountered any that do not adhere to a shared security model.

[3] Amazon Web Services, Shared Responsibility Model, *https://aws.amazon.com/compliance/shared-responsibility-model/*

[4] Google, Google Security Overview, *https://cloud.google.com/security/overview*

[5] Microsoft Azure, Shared Responsibility in the Cloud, *https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility*

[6] *Op cit* Amazon Web Services

[7] Dignan, L.; "Top Cloud Providers 2019: AWS, Microsoft Azure, Google Cloud; IBM Makes Hybrid Move; Salesforce Dominates SaaS," *ZDNet*, 15 August 2019, *https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas*

[8] Ross, S.; "Someone Else," *ISACA® Journal*, vol. 4, 2019, *https://www.isaca.org/archives*

[9] The most egregious I have read is: *Dark Reading* Staff, "Cloud Customers Faced 681M Cyberattacks in 2018," *InformationWeek Dark Reading*, 24 January 2019, *https://www.darkreading.com/attacks-breaches/cloud-customers-faced-681m-cyberattacks-in-2018/d/d-id/1333721*, quoting a security consultant. Sure they did and why stop at 681 million? But how many of them were *successful* cyberattacks? This statistic is unmentioned.

[10] Fitter, E.; K. Weise; "Capital One Data Breach Compromises Data of Over 100 Million," *The New York Times, 29* July 2019, *https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html*

[11] Ross, S.; "The Residual Data Center," *ISACA Journal*, vol. 1, 2020, *https://www.isaca.org/archives*

In Defense of Privacy by Design

In a couple of recent editions of the *ISACA® Journal*[1, 2] (referred to as columns one and two herein), my fellow columnist, Steven J. Ross, made a case whereby he believes that, contrary to the EU General Data Protection Regulation (GDPR), privacy cannot, as a practical matter, be part of a system's design. I beg to differ and will do so by running through the points made in his columns as I understood them.

Genuine Harm

At the end of his first column, Mr. Ross notes that designing "privacy" into systems where a breach will have no real consequences diminishes the attention that is required to protect against truly intrusive systems.[3] This conclusion was reached by providing an example wherein he considered buying a castle in Spain and reviewed the prices online. However, from a privacy perspective, the point is that not everyone may have that simple luxury. A case in point is Facebook being accused by the US government of breaking the law by restricting who can view housing-related ads based on their "race, colour, national origin, religion" (sensitive personal data under the GDPR).[4] For the individuals involved, this had very real consequences. This is a failure of design. Why was this data collected? How could it have been used for that purpose?

Ian Cooke, CISA, CRISC, CGEIT, COBIT 5 Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, FIP, 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 over 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees, was a topic leader for the Audit and Assurance discussions in the ISACA Online Forums and is a member of ISACA's CGEIT® Exam Item Development Working Group. Cooke has supported the update of the CISA® Review Manual and was a subject matter expert for the development of 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 and the 2020 Michael Cangemi Best Book/Author Award. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), LinkedIn (*www.linkedin.com/in/ian-cooke-80700510/*), or on the Audit and Assurance Online Forum (*engage.isaca.org/home*). Opinions expressed are his own and do not necessarily represent the views of An Post.

Privacy by Design and GDPR

At the beginning of the second column, Mr. Ross challenges anyone to remember the beginning of the first sentence of GDPR article 25 (Data Protection by Design and by Default)[5] by the end of it. It appears to be a fault that the article was written by a committee. On the contrary, I consider this a strength and, as a member of the Certified in the Governance of Enterprise IT® (CGEIT®) Item Development Group, I see this very strength in action. For Item Writing Groups, ISACA® requires, to the extent possible, geographical representation. All members must accept the text of every question before it can move forward to the item bank. In other words, ISACA wants to ensure that all points of view are considered. Committees and, indeed, compromise are the very foundations of a liberal democracy.

At the time of this writing, the European Data Protection Board (another committee) has Guidelines on Data Protection by Design and by Default[6] out for public consultation. The document interprets GDPR article 25 discussing the rights and freedoms referenced therein. The rights are documented in Article 8 of the Charter of Fundamental Rights of the European Union[7] and include the right to the protection of personal data and the right to have data processed fairly (for specified purposes) on the basis of the consent of the person concerned or some other legitimate basis laid down by law. The freedoms are discussed in GDPR recital 4,[8] which contains an important addition to the help provided in column two:

> *This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought,*

> *conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.*[9]

In other words, GDPR article 25 is not just about security; it is also about privacy. It is important to remember that security does not (necessarily) mean privacy. Privacy is a possible outcome of security,[10] but it is possible to have a privacy violation affecting these freedoms without a security breach.

Cyberthefts of Personal Information

That is not to say that the breaches identified in column two (Equifax in the United States, British Airways, Caisse Desjardins in Canada, Uniqlo in Japan and from virtually the entire population of Bulgaria)[11] are not privacy breaches; they most definitely are, however, I would like to examine further whether these are a failure of design.

The aforementioned GDPR guidance[12] notes that a technical or organizational measure can be anything from the use of advanced technical solutions to the basic training of personnel, for example, on how to handle customer data. Further, the term "measures" can be understood in a broad sense as any method or means that a controller may employ in the processing. These measures must be appropriate, meaning that they must be suited to achieve the intended purpose, i.e., they must be fit to implement the data protection principles effectively by reducing the risk of infringing the rights and freedoms of data subjects.[13]

Considering this, any reading of the identified cyberattack with which I am most familiar, Equifax,[14] could only conclude that this was, indeed, a failure of design. Further, I am not sure one could claim that everything was done to deter cyberattacks[15] in this instance.

"Big Tech"

The essence of a privacy violation may well be in the use of personal information for purposes other than those for which it was collected.[16] However, Google simply saying that it will share information with other organizations is not enough. Per the UK's Information Commissioner's Office (ICO) report on Real Time Bidding:

> *As bid requests are often not sent to single entities or defined groups of entities, the potential is for these requests to be processed by any organisation using the available protocols, whether or not they are on any vendor list and whether or not they are processing personal data in accordance with the requirements of data protection law.…Multiple parties receive information about a user, but only one will 'win' the auction to serve that user an advert. There are no guarantees or technical controls about the processing of personal data by other parties, e.g., retention, security, etc. In essence, once data is out of the hands of one party, essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls.*[17]

Further:

> *…[R]reliance on contractual agreements to protect how bid request data is shared, secured and deleted…does not seem appropriate given the type of personal data sharing and the number of intermediaries involved. This contract-only approach does not satisfy the requirements of data protection legislation. Organisations cannot rely on standard terms and conditions by themselves, without undertaking appropriate monitoring and ensuring technical and organisational controls back up those terms.*[18]

From reading the ICO's report, it is arguable that Google tells everyone exactly what it will do with their personal information if they use a Google service. Indeed, it is arguable that Google actually knows what is done with users' data. In addition, the only positive thing I can say about Google's privacy policy is that it has morphed over time, mainly in an attempt to keep up with regulations such as GDPR, from when users' data were collected in aggregate to the 4,000-word monster it is now.[19]

And, while we are on the subject of Google, I firmly believe that the controversy about YouTube being used by pedophiles referred to in column one was, indeed, a failure of privacy by design. YouTube was designed to be viral; comments are part of that virality. Similar to the Facebook issue discussed earlier, no thought went into how this could be abused.

> “TO PROTECT THE RIGHTS AND FREEDOMS OF ALL INDIVIDUALS, PRIVACY MUST BE INCORPORATED INTO NETWORKED DATA SYSTEMS AND TECHNOLOGIES BY DEFAULT.”

Privacy by Design and IT Audit

I hope I have made a strong case for privacy by design. If one accepts that there is a need, then for what should we as IT auditors look? Traditionally, designing secure and trustworthy systems has focused on analyzing risk and responding to threats that affect the security goals[20] (i.e., confidentiality, integrity and availability). However, as we have seen, there are other risk factors that may affect the rights and freedoms of data subjects.

The loss of control in decision-making, excessive data collection, re-identification, discrimination and/or stigmatization of persons, biases in automated decisions, users' lack of comprehension of the scope and the risk of unlawful processing or profiling that is invasive or incorrect, are examples of risk to privacy that cannot be managed by using only a traditional risk model that focuses exclusively on security goals.[21]

To cover these risk scenarios, it is necessary to include three new privacy-focused protection goals:[22]

1. **Unlinkability**—Seeks to process data in such a manner that the personal data within a domain cannot be linked to the personal data in a different domain, or that establishing such a link involves a disproportionate amount of effort. This privacy goal minimizes the risk of an unauthorized use of personal data and the creation of profiles by interconnecting data from different sets, establishing guarantees regarding the principles of purpose limitation, data minimization and storage limitation.
2. **Transparency**—Seeks to clarify data processing such that the collection, processing and use of information can be understood and reproduced by all the parties involved and at any time during the processing. This privacy goal strives to delineate the processing context and make the information on the goals and the legal, technical and organizational conditions applicable to them available before, during and after data processing to all involved parties, both for the controller and the subject whose data are processed, thus minimizing the risk to the principles of loyalty and transparency.
3. **Intervenability**—Ensures that it is possible for the parties involved in personal data processing and, especially the subjects whose data are processed, to intervene in the processing whenever necessary to apply corrective measures to the information processing. This objective is closely linked to the definition and implementation of procedures for exercising data protection rights, presenting complaints or revoking consent given by the data subjects, as well as the mechanisms to guarantee the data controller's evaluation of the fulfillment and effectiveness of the obligations that are assigned to them by law.

Conclusion

To protect the rights and freedoms of all individuals, privacy must be incorporated into networked data systems and technologies by default. Privacy must become integral to organizational priorities, project objectives, design processes and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives.[23] I believe that it is incumbent on all IT auditors to defend privacy by design.

Steven J. Ross Responds

Overall, I am delighted that something I have written has aroused enough passion that Mr. Cooke has dedicated one of his columns to reply. Respectful back and forth among professionals only adds to readers' appreciation for the issues involved. I will respond in turn in one of my future columns.

Endnotes

[1] Ross, S. J.; "Why Do We Need Data Privacy Laws?" *ISACA® Journal*, vol. 5, 2019, *https://www.isaca.org/archives*

[2] Ross, S. J.; "Un-Privacy by Design," *ISACA Journal*, vol. 6, 2019, *https://www.isaca.org/archives*

[3] *Op cit* Ross, *ISACA Journal*, vol. 5, 2019

[4] Gabbatt, A.; "Facebook Charged With Housing Discrimination in Targeted Ads," *The Guardian*, 28 March 2019, *https://www.theguardian.com/technology/2019/mar/28/facebook-ads-housing-discrimination-charges-us-government-hud*

[5] Intersoft Consulting, Art. 25 GDPR, Data Protection by Design and by Default, Belgium, 2018, *https://gdpr-info.eu/art-25-gdpr/*

[6] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, *https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en*

[7] European Convention, Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities,* 18 December 2000, *https://www.europarl.europa.eu/charter/pdf/text_en.pdf*

[8] Intersoft Consulting, General Data Protection Regulation, Recital 4, Data Protection in Balance With Other Fundamental Rights, Belgium, 2018, *https://gdpr-info.eu/recitals/no-4/*

[9] *Ibid*.

[10] ISACA®, *ISACA Privacy Principles and Program Management Guide*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-Privacy-Principles-and-Program-Management-Guide.aspx*

[11] *Op cit* Ross, *ISACA Journal*, vol. 6, 2019

[12] *Op cit* European Data Protection Board

[13] *Ibid*.

[14] Cooke, I.; "Lessons From History," *ISACA Journal*, vol. 4, 2019, *https://www.isaca.org/ archives*

[15] *Op cit* Ross, *ISACA Journal*, vol. 6, 2019

[16] *Ibid*.

[17] Information Commissioner's Office, *Update Report Into Adtech and Real Time Bidding*, UK, 20 June 2019, *https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf*

[18] *Ibid*.

[19] Warzel, C.; A. Ngu; "Google's 4,000-Word Privacy Policy Is a Secret History of the Internet," *The New York Times*, 10 July 2019, *https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html*

[20] Agencia Española de Protección de Datos, A Guide to Privacy by Design, Spain, 2019, *https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf*

[21] *Ibid*.

[22] *Ibid*.

[23] Cavoukian, A.; "Privacy by Design: The Seven Foundational Principles," IAPP Resource Center, *https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/*

Enjoying this article?

- Read *Enforcing Data Privacy in the Digital World*. *www.isaca.org/enforcing-data-privacy*
- Learn more about, discuss and collaborate on audit and assurance ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The Patter of Emerging Technologies

The idea that we are all connected via some ethereal or other unknown plane is a belief held by metaphysical enthusiasts and religions all around the world. There is something to be said about the interconnectivity of the human spirit and experience.

The Magic

In light of technological breakthroughs, we have broken through beliefs or magic and stumbled into an age of digital connection and interconnectivity on a massive scale.

Since I have been anointed (that is not a typo) with the title of futurist, I have made it a point to spend time observing people's (and my own) use of technology on a day-to-day basis. The obvious observation is the explosive popularity of the smartphone, with its tendrils that sneak into every facet of our senses. We have applications (apps) and wearables that track our heart rates and blood oxygen levels; apps that track what we eat, our moods, our sleep cycles; and anything else that dives into the figurative and actual viscera of what makes us who we are. We can spit in a vial, send it off to a lab and, four to six weeks later, have a mapping of our genetic makeup paired with a list of markers that indicate our strengths, weaknesses and lineage. Internet of Things (IoT) devices track our every movement and surrounding environments, giving us peace of mind that everything is "OK." The cloud houses the data acquired from our physical world via these devices and processes, where machine learning (ML) and artificial intelligence (AI) algorithms attempt to figure out what is going to happen next.

Dustin Brewer, CSX-P, CCSP, CEH, CHFI
Is ISACA's principal futurist, a role in which he explores and produces content for the ISACA® community on the utilization benefits and possible threats to current infrastructure posed by emerging technologies. He has 17 years of experience in the IT field beginning with networks, programming and hardware specialization. He excelled in cybersecurity while serving in the US military and, later, as an independent contractor and lead developer for defense contract agencies, he specialized in computer networking security, penetration testing, and training for various US Department of Defense (DoD) and commercial entities. Brewer can be reached at futures@isaca.org.

We wake up. Our wrist wearables tell us how well we slept. The lights turn on in our houses automatically and the thermostat sets the temperature to our liking. Our home hub devices tell us what our day looks like and start to play our favorite news broadcast. Our smartphones tell us that if we order our coffee now, it will be ready by the time we pass our favorite coffee establishment on our way to work. Our smartphones then tell us there is a five-minute delay on our way to work due to an accident and suggests an alternate route, changing our very routine behavior. We can walk into an establishment that accepts cryptocurrency and, literally, buy a physical object with nothing more than a group of ones and zeros derived from an algorithm. The tangible of the intangible is palpable. And the cycle starts again.

Emerging technologies have already found their way into our lives and have truly built a network of interconnectivity with all of us on a very personal level.

The Magicians

And, in the middle of all the buzzwords, cryptocurrency fear of missing out (FOMO) hype and privacy concerns in which these new technologies are shrouded stand the IT architects, cybersecurity professionals, IT support staff, governance professionals and everyone in between. We attempt to implement, secure and support these new interconnecting technologies as they are created and as they become popular and lucrative and, in some cases, turn into necessities for day-to-day business. While none of these new age magicians is the alchemist who created the magic, this guild is tasked with implementation, interoperability, privacy and security of this new form of interconnection. These professionals are asked to do what seems impossible when implementing a new technology into a somewhat stable environment. Connecting seemingly unrelated devices that speak totally different languages and making them user friendly is quite the magic trick.

The Trick

It can sometimes seem like emerging technologies are just rebranded old technologies with a gimmick. The cloud is just a reboot of mainframe architecture. IoT devices can be seen as just programmable integrated circuits with connectivity. Blockchain is viewed as another database with some extra metadata. While there are some truths to these claims, if we step back and look at these technologies holistically, we get a much clearer picture of their future potential. An IoT device that turns a light on and off is pretty boring on its own, but combining that device with a home automation device, the cloud and some ML algorithms creates a smart home or office capable of making our lives easier and, possibly, even healthier.

> “WHATEVER IT IS THAT YOU NEED TO DO TO GET A BETTER UNDERSTANDING OF THE TECHNOLOGY SHOULD BE DONE, BECAUSE AN ACTIVE EMPHASIS ON CONTINUAL LEARNING AS AN IT PROFESSIONAL MAY BE THE MOST VALUABLE TRICK OF ALL.”

The trick is not necessarily to find the potential of one emerging technology, but to figure out how these technologies can help us interact with our physical world and connect us in long-lasting and high-impact ways. This requires a certain amount of dedication to the craft and, while expertise in all forms of emerging technology may not be necessary, a working understanding of blockchain, IoT, AI, etc., must be achieved. There are many ways to pursue technology proficiency and mastery. In my case, starting up a container with Hyperledger or opening up a smart device and soldering a serial connection to it and doing some hands-on exploring helps me understand the underlying technology. This approach may be too “in the weeds” for many. If you are a process person, looking into flowcharts, frameworks and theory- or data-driven processes may be your preferred modus operandi. Whatever it is that you need to do to get a better understanding of the technology should be done, because an active emphasis on continual learning as an IT professional may be the most valuable trick of all.

The Curtain Call

The truth is that the magic involved in emerging technologies and their functions has much more to do with science and engineering. To the end user, this functionality, of course, appears as something magic or otherworldly until it breaks or their personal data are stolen in a breach or cybersecurity event. This fall from astonishing convenience to loss of privacy and security makes the crash to reality all the more painful for the user. Conveying the idea of security awareness to end users to help mitigate some of these pitfalls is paramount. We security practitioners not only need to change the behavior of end users, but also the culture surrounding technologies.

“Patter” is the story a magician tells during a magic trick. This narrative brings the entertainment to life and adds a little more wonder to the prestige, or finale. It also distracts the audience from any sleight of hand or trick. This new form of digital interconnectivity that we all have is truly wonderful and groundbreaking, but we need to be wary of the patter, the narrative we tell ourselves and our users about it while, hopefully, not removing too much of the perceived magic from the experience. Because what’s the fun in that?

Enjoying this article?

- Learn more about, discuss and collaborate on emerging technology in ISACA’s Online Forums. *https://engage.isaca.org/onlineforums*

Massive Automation to Reduce Human Risk

Even in large organizations, it is not unusual to find controls that still involve a great deal of manual effort. In fact, evidence for an attestation may be entirely generated by someone taking screenshots. This is certainly one area where innovation needs to play a bigger role. People are an organization's most valuable resource and, often, its greatest risk. Innovating how we collect evidence and perform audits can help with both aspects. It can free up personnel to be more productive and reduce a great deal of the human risk regarding controls and the like. In fact, we are in an era when we need to look at innovating through automation because we simply cannot keep up otherwise.

Virtualization and Cloud

When system administrators managed a handful of servers, auditing these servers manually was not an onerous effort. However, with the prolific use of virtualization and the increase in cloud adoption, the number of devices or hosts has increased exponentially. After all, resources can be provisioned and shut down automatically. We can even script triggers to scale out web farms during periods of heavy usage and other triggers to eliminate web servers when the load dies back down. In a cloud environment, where an organization pays for what it uses, having excess capacity always available is money wasted.

K. Brian Kelley, CISA, CSPO, MCSE, Security+
Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps, and user groups.

> “WE ARE IN AN ERA WHEN WE NEED TO LOOK AT INNOVATING THROUGH AUTOMATION BECAUSE WE SIMPLY CANNOT KEEP UP OTHERWISE.”

Given the scale, which can be an order of magnitude (or two or three orders) more than previous device counts, auditing manually is just not realistic. We could sample, but it would be better if we could evaluate every provisioned resource, would it not? It most certainly would, as a single misconfigured device could be the entry point for an adversary seeking to do harm.

Speaking of auditing every device, how about capturing evidence for devices stood up for a period of time and then retired when load died? How can we be sure that those devices had proper controls? After all, they no longer exist. We can look at the provisioning process, but that does not tell us how well that provisioning process worked during that particular time frame if we are resorting to manual auditing efforts. Devices and systems that came into being after the last audit and were decommissioned before the present one are particularly problematic.

We could have an individual or even a whole team trying to capture information on systems as they come along, but that is a huge resource drain for arguably no gain. If an organization were to go down that route, an auditor could argue that it does not meet a reasonable return on investment (ROI) and would represent waste so far as the organization is concerned.

The Risk With Manually Created Artifacts

Whenever we have a manual process, we are relying on a person to do two things:

1. Capture information on the correct system or device.
2. Perform the proper procedure without error.

If either of these are done incorrectly, we do not have what we need. If there are a lot of artifacts to capture, it may be some time before the error is detected and the evidence is regathered (if that is possible). There is always additional risk due to human error. But what if it is not a case of human error?

Part of manual collection of evidence or validation of controls is that we assume that the person performing the work is trustworthy. With proper controls, we usually have other mechanisms to mitigate this risk. However, that is not always the case. When we can automate, we can reduce the risk due to the human element, not just with respect to error, but also due to malicious intent.

Let us consider what an untrustworthy person could do in manually collecting the evidence. Screenshots can be altered. One does not have to be proficient with the latest imaging tools to make nearly undetectable changes. Certainly, they would be undetectable to the human eye, especially an eye that is going through a large amount of evidence quickly for the purposes of an audit.

Altering a screenshot is not the only way. Old screenshots that have been saved can be reused. But the file date should protect us, right? Nothing stops a person from opening up an image in MS Paint (on Windows) and resaving the document with a different name, thereby creating a new timestamp. Or, if they are more technically clever, they might use other ways to alter the file date without actually touching the contents of the file.

If the evidence is not a screenshot but something such as a text file that is generated as a result of a script, that is even easier. One does not even need a modicum of artistic talent! And, if the script is handed over to be run by a person with the rights to make changes, they can make the changes to look clean for the audit and then put things back after the script runs. This situation is not that unusual because one often has to have elevated rights on systems to audit security—the same privilege level gives them the ability to administer the security.

Something else that comes up from time to time: The actions to gather the evidence for a control may, in and of themselves, generate work for another control. For instance, if logins to a particular set of servers must be explained and documented, logging on to those servers to collect who are the admins, what are the permissions for a particular set of files, etc., would require that documentation.

> “WE CANNOT COMPLETELY ELIMINATE RISK, BUT ANY REDUCTION IS GOOD.”

We have these types of controls because the ability to log in with a privileged account to the server represents a risk to the organization. It would be better for said individual not to have the ability to log in at all. After all, if the person has the ability to log in, if the account is compromised, someone else has the potential to log in. There are countermeasures to this such as multifactor authentication systems and privileged access management solutions, but it is still better if the individual cannot log in. Those systems exist to prevent an unauthorized login. However, if the

Enjoying this article?

- Read *Auditing Artificial Intelligence. www.isaca.org/auditing-AI*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

person is authorized to log in and is also malicious (insider threat), they can do damage to the organization. No login equals no damage.

Automation to Reduce the Risk

Automation takes the human out of the collection tasks. Any risk due to the human element is reduced. Yes, there is still some risk due to human error. For instance, if someone misinterprets the evidence, that is human error. There is also some risk due to malicious intent. Someone can attempt to get rid of evidence, misrepresent the evidence or flat out lie on a report. We cannot completely eliminate risk, but any reduction is good. That includes the amount of time someone spends collecting evidence. When people have to perform manual processes that could be handled by automation, it means they are not available during that time to perform what the organization would consider more valuable work. After all, if I have to spend four hours collecting evidence, that is four hours I cannot spend innovating or solving problems.

Another thing to consider is the scale problem. With automation, scale is not so daunting. I may need to scale my collection process/systems, but as systems increase in number, I do not have to increase my headcount linearly. That is a huge cost savings. Also, if I can automate any artifact collection around any scale out or scale in of systems, that means I can ensure I am capturing the evidence when I need to do so.

Speaking of scale, though, there is a risk with too much automation. If we try to collect too much, there can be a real performance impact on the system. If the information is necessary, the organization has to accept the performance hit or spend to increase capacity, if that is possible. But if it is not absolutely necessary, what is collected should be kept to what is defined as needed. By the way, collecting too much will result in a lot of noise. There will be a large amount of data to sift through for what we want.

Finally, we can automate comparison, at least at a high level. This allows us to detect differences and changes between the audit periods. Those periods could only be a few hours apart. Certainly, when we have to evaluate a great deal of evidence, having a report of detected differences will help tremendously. We will spend less time looking for the differences, there will be less risk of missing a difference and we should also be able to spot trends better.

> “SPEEDING UP PROCESSES, REDUCING RISK AND FREEING PEOPLE TO DO OTHER WORK IS ALL ABOUT BUILDING AND IMPROVING THAT COMPETITIVE EDGE.”

Automation Is Still Innovation

Innovation can be about giving an organization a competitive edge. Speeding up processes, reducing risk and freeing people to do other work is all about building and improving that competitive edge. It also focuses on the greatest risk factor: the human element. Whether we are talking malicious activity or honest mistakes, there is risk. Automation reduces that risk.

The Human Elements of Risk

In classical Greek mythology, Daedalus was helplessly watching Icarus, his son, fall to his death. Daedalus, having designed the Minotaur's Labyrinth, was imprisoned. To escape, he had fitted himself and his son with wings that he had innovated. During the escape, Icarus became intoxicated by this new power of flight and, despite Daedalus's repeated warnings and his own lack of experience, Icarus took the risk of flying so high that the sun melted the wax holding his feathered wings.[1] No matter how well humans try, risk scenarios remain in ways unnoticed or unimagined by human insights.

While nature offers its own set of systems, humans design systems for their wants and needs—systems that inherit subtle attributes of human nature; principally, the way in which people perceive, assess and mitigate risk. Assuming Daedalus did not anticipate anyone flying so high and approaching the sun, there was no design error. However, Icarus, through his own behavior, indulged in flying high and, thus, created an operational error.

Security breaches are on the rise. A 2015 PricewaterhouseCoopers (PwC) survey sponsored by the UK government revealed that the percentage of large organizations affected by breaches increased from 81 percent to 90 percent. The survey estimated an average of 117,339 incoming attacks daily, or 42.8 million annually.[2] According to the Ponemon Institute *2018 Cost of a Data Breach Study*, the root causes of data breaches were human error (27 percent), malicious or criminal attacks (48 percent) and system glitches (25 percent).[3] All three causes essentially point to the human element of risk. While the scope here is on a single aspect—data loss—the findings reveal that, behind all consequences, the human hand is present.

But the difficulty is this: Knowledge of what these elements are and how to proactively address them is limited. The PwC survey showed that, compared to 68 percent in the previous year, staff awareness training was delivered to 72 percent of large organizations.[4] However, it appears to have failed to effect change in human behavior.

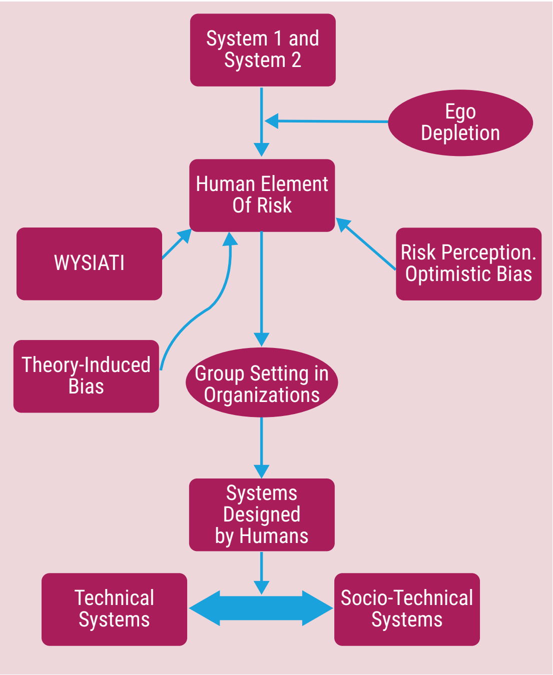
Origins

This view of human elements of risk, shown in **figure 1**, is drawn mainly from the book *Thinking, Fast and Slow*.[5] The author asserts that fast thinking involves intuition and automatic—sometimes almost unconscious—mental activities of perception and memory. In contrast, slow thinking

Vasant Raval, DBA, CISA, ACMA
Is professor emeritus of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and financial fraud. He recently published a book on corporate governance. He can be reached at vraval@creighton.edu.

Rajesh Sharma, Ph.D., CMMI Lead Appraiser, ITIL Foundation, Six Sigma Black Belt
Is a director of product and quality at Software Engineering Services. He has more than 19 years of experience in establishing and managing project management offices (PMOs), quality management offices (QMOs), metrics programs, process improvement, cybersecurity programs, and as a lead for independent verification and validation (IV&V) projects. As a QMO and IV&V lead, he has performed quality audits, process improvement and IV&V assessments. He can be reached at rajsharmane@gmail.com.

Figure 1—A View of the Human Elements of Risk



implies a more deliberate and effortful form of thinking. Originating in different regions of the brain, fast thinking is sometimes called the "hot system" or "System 1," and slow thinking the "cool system" or "System 2."[6] System 1 is dominated by emotions, while System 2 emphasizes a cautious approach and reasoned answers. The author argues that the intuitive System 1 is "more influential than your experience tells you."[7] Both systems are geared to judgment and choice. Unfortunately, System 1 is not designed to incorporate multidimensional, hard evidence offered by statistics in its process; only System 2 can deal with such complex scenarios. Impulsive and intuitive, System 1 is where snap judgments are made using evidence that may be unreliable, but can be retrieved easily. In System 1, associative memory continually constructs a coherent, but not necessarily truthful, interpretation of what is going on in the world. The illusory certainty of hindsight feeds overconfidence, much like in Nassim Taleb's book, *The Black Swan*.[8]

When System 2 is busy, System 1 takes over the task of judgment and choice. When risk-related decisions are made by System 1, chances are, the answers are, at best, inadequate, and may even be faulty. Take, for example, the spread of coronavirus. The media blitz combined with information overload from social networks inundates the social mechanism of availability of information, while the probability of cases of such virus may be unknown or low, say, in a small town in the US. But the availability rules over probability when System 1 is in charge, leading to an unreliable assessment of risk. The bottom line is System 2 should always be in charge of the human elements of risk.

Because the same pool of mental energy powers all voluntary effort of System 2, such energy may be depleted at times, for example, at the end of a tiring day of audit work. If System 2 is too tired to handle any more tasks, due to what one researcher calls ego depletion,[9] System 1 takes over. Ego-depleted people are much more likely to make intuitive errors, and this can happen during a risk assessment exercise. In *Thinking, Fast and Slow*, the author describes a study of eight parole judges who spent an entire day reviewing parole applications. The proportion of approved cases rose to approximately 65 percent in a period of two hours after the last meal and then gradually dropped down to approximately zero immediately before the next meal.[10] The conclusion is clear: Tired and hungry judges resort to the more defensible position of denial of parole requests.

> "WHEN PEOPLE THINK ABOUT RETURN, THEY TEND TO PUT AWAY THE THOUGHT OF RISK, AND WHEN EVALUATING RISK IN ANY DECISION, THEY TEND TO BE MORE OPTIMISTIC."

The same author identifies three additional factors likely to contribute to risk of human judgment:[11]

1. Optimistic bias in risk perception
2. What you see is all there is (WYSIATI)
3. Theory-induced bias

Optimistic Bias

It can be argued that decisions have two sides: risk and return. When people think about return, they tend to put away the thought of risk, and when evaluating risk in any decision, they tend to be more optimistic. This bias toward optimism in risk assessment causes people to expect success, thus predicting failures on the lighter side. They design for acceptable risk and generally remain optimistic when evaluating the downside of an initiative. Optimistic bias has a tendency to overweight gains, while underweighting losses affects risk perception. "It is not going to happen here" is the syndrome that drives overconfidence and nonchalant acceptance of certain risk factors, albeit intuitively and without enough rational thinking. People know more about benefits, less about risk.[12]

WYSIATI

Humans have a tendency to assume that the past predicts the future. WYSIATI causes a restrictive or constrained view of the present, masking potential new risk. The eyes that look at the experience may be blinded, or at least not open enough to interpret what they see. In his 2001 letter to shareholders, Warren Buffett, chief executive officer (CEO) of Berkshire Hathaway, talked about how the company's mistake of focusing on experience rather than exposure resulted in assuming a huge terrorism risk in its insurance business for which the company received no premium.[13] Experience can hinder, rather than help, proper identification of risk.

Theory-Induced Bias

It is quite likely that the manager is projecting from a well-accepted theory in her or his evaluation of risk. But the theory itself may be faulty or incomplete. As stated in *Thinking, Fast and Slow*:

> *Once you have accepted a theory and used it as a tool in your thinking, you assume that there must be a perfectly good explanation that you are somehow missing. You give the theory the benefit of the doubt, trusting the community of experts who have accepted it.*[14]

This is called theory-induced bias and it can lead one to not challenge any anomalies that might be otherwise examined seriously.

"PERHAPS ELABORATE AND CREDIBLE FRAMEWORKS EMPHASIZE TOO MUCH TECHNOLOGY AND VERY LITTLE HUMAN FACTOR."

While individual perception of risk and its mitigation may suffer from optimism, the situation is unclear in a group setting, where much of the work gets accomplished in organizations. The group may resign itself to the loudest voice, an authority's opinion (tone from the top) or to the organization's traditions. The risk scenarios of the Boeing 737 MAX were probably known among engineers, but they reported to business managers who worry more about time-to-market. As a result, it is likely that engineers yielded to an optimistic bias among business managers. The organization's environment and culture, including the tone from the top, should nurture practices that motivate risk-informed compliance to policies and practices.

Together, these origins of the human elements of risk suggest that the scenario is complicated, and it is generally not possible to weed out all gaps in risk assessment. As long as humans are in charge of designing systems, there will be misses.

The human elements of risk are often discussed in the context of employees, the most common user group. However, risk may emanate from other stakeholders (e.g., customers, suppliers, end users) or hackers in both technical and socio-technical systems. In any case, risk should not be equated with committed "errors," for there may be risk related to omissions. The focus should be on all types of consequences of risk, not just errors in a narrow sense of the term. Finally, although the focus is on risk, the ultimate aim is risk mitigation, which is fundamental to governance.[15]

Cybersecurity Risk

Using **figure 1** as a guide, it is important to reflect on the state of cybersecurity risk assessment and mitigation. High-profile cybersecurity breaches are reported in the media almost incessantly, leading to much greater availability of threat scenarios

> “WHILE MUCH OF THE RISK OF THE HUMAN ELEMENT IN SYSTEM DESIGN AND OPERATION CAN BE MITIGATED, SUCH RISK CANNOT BE TOTALLY AVOIDED.”

combined with little understanding of probability of their occurrence in one's own world. At this time, if System 1 takes over, results can be misleading. This exposes the inadequacy of current assurance methods, which can gain much from human reliability assessment and improved statistical methods of obtaining true assurance[16] based on a reasoned approach of System 2. Using security breach statistics, researchers contend that half of significant security incidents are due to people and the unintentional mistakes and errors they make.[17] Citing data, the researchers concluded that it is difficult to apply cybersecurity controls concerning human behavior.[18]

Perhaps elaborate and credible frameworks emphasize too much technology and very little human factor, presumably leading to theory-induced bias. Moreover, human behavior is not consistent (that is, deterministic) and can be influenced by relationships, as in group settings in enterprises. Additionally, people naively assume that bad things only happen to other people.[19] Also, research suggests that people are willing to undertake risky practices,[20] perhaps due to asymmetric risk perception (underweighting risk, overweighting gains) and optimistic bias (**figure 1**).

What Can Be Done?

Human behavior is difficult to change. Perhaps the approach to the human elements of risk is inappropriate. Effective human reliability assessment should complement sound technical analysis of the physical systems with the development of organizationwide safety culture and risk management. The human error assessment and reduction technique (HEART) is one such validated error analysis and quantification technique to provide proactive quantification of human behavior,[21] which may be helpful in effecting change. One researcher asserts that people instinctively resist being forced to do things differently.[22] Appeals to fear may not work effectively; instead, it would help if barriers in their way are removed. The researcher suggests five ways to remove such barriers to change: reduce reactance (people's desire to feel that they are in the driver's seat), ease endowment (attachment to things we know or have used for a long time), shrink distance (keep incoming content close enough to people's current perceptions), alleviate uncertainty (e.g., lower the barrier to trial and experimentation), and find corroborative evidence (hearing from more than one source).[23]

While much of the risk of the human element in system design and operation can be mitigated, such risk cannot be totally avoided. With the continuing explosive growth of the connected world, if anything, the human element will be at the forefront in future risk scenarios. As more of the human role in systems is automated through robotic process automation (RPA), for example, less risk may exist if the modified system is designed properly. Nevertheless, humans will remain the weakest link in the risk management chain.

Author's Note

Opinions expressed in this column are the authors' own and not those of their employers.

Endnotes

1 Duffey, R. B.; J. W. Saul; *Managing Risks: The Human Element*, John Wiley & Sons, United Kingdom, 2008

2 PricewaterhouseCoopers UK, *PwC 2015 Information Security Breaches Survey*, United Kingdom, 2015, *https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf*

3 Ponemon Institute, *2018 Cost of a Data Breach Study: Global Overview*, USA, 2018, *https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/*

4 *Op cit* PricewaterhouseCoopers UK

5 Kahneman, D.; *Thinking, Fast and Slow*, Farrar, Straus and Giroux, USA, 2011

6 *Ibid.*

7 *Ibid.*, p. 13

8 Taleb, N. N.; *The Black Swan*, Random House, USA, 2010

9 Baumeister, R. F.; E. Bratslavsky; M. Muravan; D. M. Tice; "Ego Depletion: Is the Active Self a Limited Resource?" *Journal of Personality and Social Psychology*, vol. 74, iss. 5, 1998, p. 1252–1265

10 *Ibid.*, p. 43–44

11 *Ibid.*

12 *Ibid.*

13 Buffett, W.; "2001 Chairman's Letter," Berkshire Hathaway, 2001, *https://www.berkshirehathaway.com/letters/2001pdf.pdf*

14 *Op cit* Kahneman, p. 277

15 Raval, V.; *Corporate Governance: A Pragmatic Guide for Auditors, Directors, Investors, and Accountants*, CRC Press, Taylor and Francis Group, United Kingdom, 2020, Chapter 3: Risk and Governance

16 Evans, M.; L. A. Maglaras; Y. He; J. Janicke; "Human Behavior as an Aspect of Cybersecurity Assurance," *Security and Communication Networks*, vol. 9, 2016, p. 4667–4679

17 *Ibid.*, p. 4668

18 *Ibid.*, p. 4670

19 Johnston, A.; M. Warkentin; "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, vol. 34, iss. 3, 2010

20 *Op cit* Evans *et al.*, p. 4671

21 Lyons, M.; S. Adams; M. Woloshynowych; C. Wincent; "Human Reliability Analysis in Healthcare: A Review of Techniques," *International Journal of Risk & Safety in Medicine*, vol. 16, iss. 4, 2004, p. 223–237. Also see figure 2 in *op cit* Evans, *et al.*

22 J. Berger, J.; "How to Change Anyone's Mind," *The Wall Street Journal*, 21 February 2020, *https://www.wsj.com/articles/how-to-change-anyones-mind-11582301073?mod=searchresults&page=1&pos=1*

23 *Ibid.*

Enjoying this article?

- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Prove Your Cyber Audit Expertise

Get the knowledge you need to excel in cybersecurity audits and an understanding of cyber-related risk through ISACA®'s Cybersecurity Audit Certificate Program.

www.isaca.org/ca-jv3

ISACA®

Communicating Technology Risk to Nontechnical People

Helping Enterprises Understand Bad Outcomes

Também disponível em português
www.isaca.org/currentissue

Too often, well-meaning technology professionals attempt to explain risk to their enterprises and fail to achieve their objective. These professionals fully understand the state of the computing environment and the importance of securing it. They may even have a relevant third-party affirmation of their beliefs through the US National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), COBIT® or other standards and frameworks. However, they are unable to motivate their nontechnical colleagues to recognize the importance of what they are trying to communicate.

Failures in communication have been studied extensively and are included in any introductory course on the subject. To identify the reasons for failure to communicate technology risk in particular, the body of knowledge related to cybersecurity must be temporarily abandoned to explore what makes communication in general work well and what causes it to fail.

Jack Freund, Ph.D., CISA, CRISC, CISM, CISSP
Is a leading voice in cyberrisk measurement and management. He is the coauthor of an award-winning book on cyberrisk quantification and holds a doctorate in information systems. Freund is an International Association of Privacy Professionals (IAPP) Fellow of Information Privacy and Fellow of the FAIR Institute. In 2018, he was the recipient of ISACA's John W. Lainhart IV Common Body of Knowledge Award and the FAIR Institute's FAIR Champion Award.

Models of Communication

No survey of communication would be complete without reviewing the seminal model proposed by Aristotle.[1] This model has three parts: the sender, the message and the receiver. Most important is the receiver, who ultimately determines whether communication has taken place. This simple model identifies at least one part of the failure to communicate technology risk. Absent the executive team's reception of the message, communication cannot happen, regardless of intentions.

In the context of information technology, it is appropriate to consider Claude Shannon's classic information theory model, published in 1948.[2] Shannon applied mathematical theory to communications, leading to concepts such as signal-to-noise ratio. Indeed, the noise part of the model can help explain problems in technology risk communication. Business executives have so many competing priorities that it is often difficult for technology professionals to rise above the noise and get their point across. Business management is largely risk management, so for an individual security-related message to resonate with decision makers, it has to compete with market risk, credit risk, competitive risk, regulatory risk, conduct risk, reputational risk and all other forms of operational risk. Numerous reports indicate that executives consider cybersecurity a top priority, so clearly they are not ignoring it.[3,4,5] However, the voluminous number of bad things routinely brought to their attention by IT professionals belies their experiences. In fact, when executives weigh these potential calamities against actual incidents, many of them conclude that IT professionals are prone to “Chicken Little-ism,” or prognosticating doom that never happens (fear, uncertainty and doubt [FUD] in other words).[6,7,8]

> “THE MESSAGE BECOMES WATERED DOWN WHEN NUMEROUS SO-CALLED CRITICAL MATTERS ARE COMMUNICATED BUT RARELY RESULT IN ACTUAL PROBLEMS OR INCIDENTS.”

IT professionals are rarely told to their faces that they are Chicken Littles. Instead, they have to interpret the feedback they receive. Thus, the modern communications model differs from the Shannon model in that it contains an explicit feedback loop (**figure 1**).[9]

Business executives employ technology professionals to identify problems and raise important issues. If all technology problems are treated as critical, the result may be apathy. The message becomes watered down when numerous so-called critical matters are communicated but rarely result in actual problems or incidents. Executives are surely aware that bad things can happen, and they may even have peers in other organizations or industries who have experienced bad outcomes, but they probably have little personal experience. Executives desire better information about cyberrisk, but they often assume that the issue is so complex that even the people they hire to deal with it are incapable of doing better. Executives tend to understand the systems that need to be online to serve their customers and the systems that cause regulators to get upset. However, experience tells them that even if they ignore the critical broken things, nothing bad is going to happen.

Too often, executives’ subtle and not-so-subtle messages are poorly received by technology professionals. Instead of changing the message to ensure that the receiver better understands it (by casting the message in terms the receiver cares about), technology professionals may become petulant and secretly wish for a security breach to prove them right. Such sullenness may compel IT professionals to send decision makers articles about bad things that have happened elsewhere.

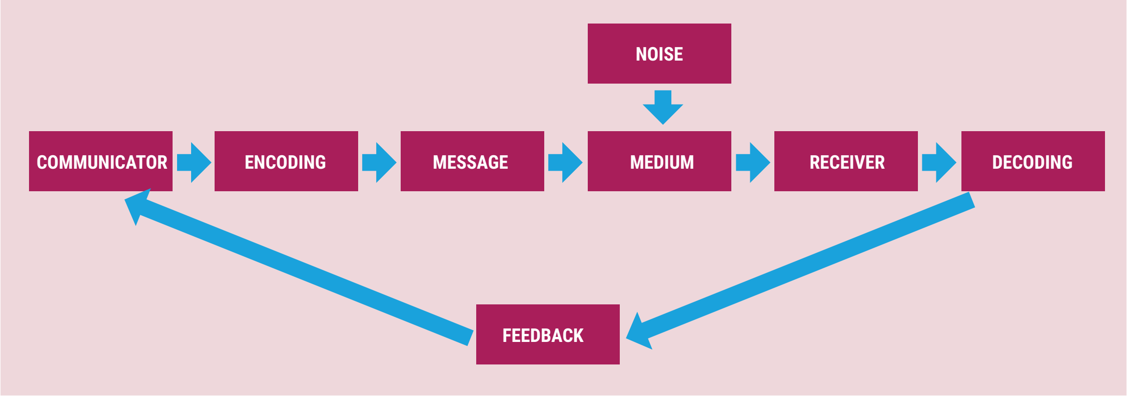
Rectifying these communication failures involves looking at how risk is communicated and how cybersecurity can be made relevant to business executives, starting with how potential risk is communicated to them.

Lists of Risk vs. Risk Scenarios

Too often, technology professionals use confusing terminology to discuss risk. As a result, a risk assessment often looks like a collection of things that are broken; groups of people who could do harm; and abstract, esoteric or even existential notions of consequences.[10] Such a list of risk factors might look like this:

- Privileged insiders
- Reputation
- Untested system recovery process

Figure 1—Modern Communications Model



> “WHEN COMMUNICATING RISK, IT IS IMPORTANT TO REMEMBER THAT MOST PEOPLE HAVE AN INCOMPLETE UNDERSTANDING OF STATISTICS, SO STATISTICAL LITERACY CANNOT BE ASSUMED.”

- Cloud data shares with sensitive data
- Short passwords
- Cybercriminals

It is easy to see that each item on the list is something that might cause concern. However, technology professionals use a kind of shorthand when communicating with other similarly trained and liked-minded professionals, whereas business executives are forced to fill in the blanks with their imaginations (guided by experience). In a fully qualified risk statement, these missing parts are articulated so that they are easily understood by individuals who are unfamiliar with the shortcuts of the profession.

It is important to clearly communicate to the target audience which items on the list are threats, assets and controls (however weak they may be). Executives must understand how the combination of these categories of things can be manipulated to cause harm to the enterprise.

The first step in improving risk communication is to ensure that there is a fully defined risk scenario to which a risk formula can be applied.[11] Each risk scenario statement should tell a story that is instantly accessible to nontechnical people. For example, such a scenario might be: “Privileged insiders leverage legitimately granted credentials to steal data from critical applications.” It specifies who is doing something bad, what methods are being employed to do it and how the organization will be impacted once it is done. A proper risk scenario needs to be forward looking. It should describe a series of bad things that might come to pass, not necessarily something that is happening currently. A good risk statement is also relatively perpetual; if an item can be removed from the risk register after something has been fixed, it is a control deficiency, not an actual risk.

The Classic Risk Formula

The classic risk formula (probability multiplied by impact) can be confusing to those receiving technology risk communications. Consider the compounded problem associated with determining both the probability and the impact of privileged insiders (from the earlier sample scenario). Asking executives to interpret the probability of insiders as 0.45 does nothing to improve communication. The probability of what, exactly? This statement does not help the receiver understand the problem.

When communicating risk, it is important to remember that most people have an incomplete understanding of statistics, so statistical literacy cannot be assumed. As a result, the use of concepts such as the basic risk formula can lead to incorrect calculations along with imperfect communication. The first problem is that the terms “likelihood” and “probability” are used interchangeably when speaking and writing. This does nothing to further mutual understanding.

Next, probability is not temporally bound.[12] It is entirely unhelpful to tell executives that the probability (or likelihood) is 40 percent. Alongside the “probability of what?” question mentioned earlier is the obvious question of when. Is it 40 percent probable that this event will happen today? This week? This year? This decade? Time matters, and taken by itself, this value does not effectively communicate what executives need to know about the probability or likelihood of risk realization.

To overcome this problem, many people apply fixed timelines to their estimates. They describe these values as representing annualized probabilities. Unfortunately, there is a fundamental mathematical problem with these kinds of assessments: What if the event could happen more than once per period? It is mathematically unsound to assert that something has a 200 percent likelihood of happening in the next year, as probability is a value between 0 and 1. And that value is non-inclusive: Probability can never be 0 or 1, because a future event can never be ruled in or ruled out with 100 percent certainty.

The foregoing issues can be overcome by utilizing frequency in place of probability in the equation.[13] This accomplishes several things. First, frequency is a much more accessible concept to represent future events. For those who are uncomfortable with statistics, it is better to ask them how often something might happen rather than the probability of its happening. Second, this variable is better able to capture events that occur more than once per year (or period). A frequency of two per year is easy to comprehend, whereas a 200 percent probability is not only mathematically incorrect but also difficult to understand practically. Additionally, probability values of less than 1 (e.g., 0.5) are more easily recognizable as frequency values and can be communicated in plain language (e.g., once every two years).

Finally, and most important, the simple risk formula does not contain guidance on exactly of what one should assess the probability and impact. Knowing what to measure is just as important as knowing how to measure it. Risk is about loss, so whatever is being measured must be a complete statement of loss relevant to the enterprise. The list of technology-related risk presented earlier is a classic example of things that are not business risk factors because they do not express a complete loss scenario.

Business Process Mapping

Some enterprises may be unfamiliar with business process mapping. However, business continuity teams may already have some version of it. If so, their mappings and process inventories are a good place to start, requiring fewer resources and supporting a single source of information on processes in the enterprise. To initiate business process mapping from scratch, the sampling approach should be followed, and key products and services and the critical processes for each should be the focus. The first year, a sample size that is doable should be chosen, and a plan for increasing the number of samples each year and determining the resources required should be created.

Business process mapping is the first step in creating a fully qualified risk scenario. This requires understanding how enterprises operate and connecting technology to business offerings. It also requires a list of the products and services the enterprise offers (or reasonable groupings of them). This list can often be compiled by considering what is offered in each line of business or some other category in large enterprises (such as geographic location). Then the parts of the enterprise that help deliver each product or service are linked. Considering the business processes that enable each part of the enterprise is helpful. Finally, a connection is made between those business processes and the technology that enables them. The result looks something like **figure 2**.

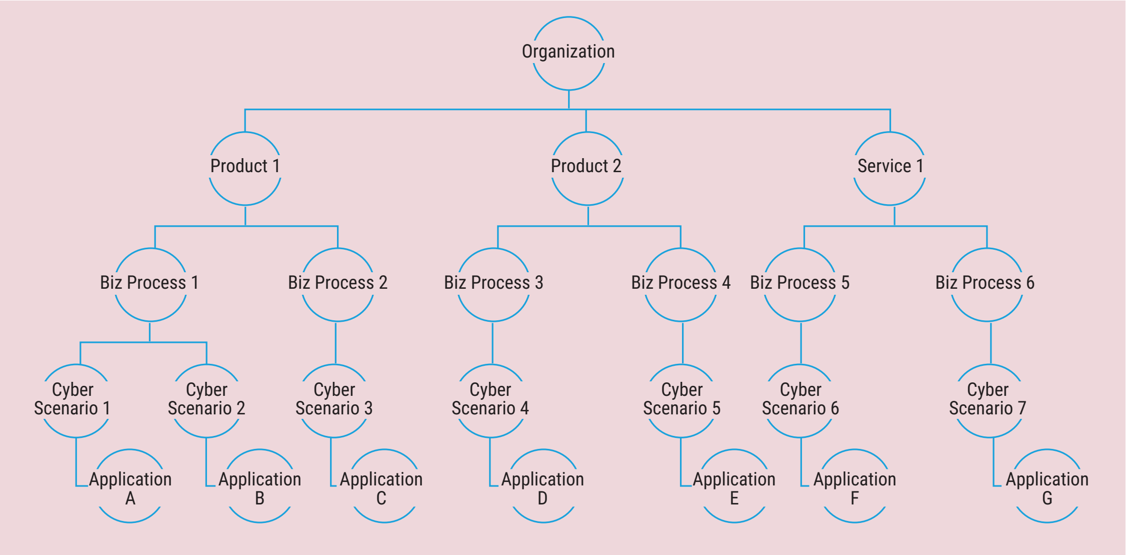
> “BUSINESS PROCESS MAPPING IS THE FIRST STEP IN CREATING A FULLY QUALIFIED RISK SCENARIO.”

Once there is a connection between technology (the tech stack) and products and services (the business stack), it is time to develop the risk scenarios that affect each. This helps decompose the process map into more detailed scenarios. In general, applications are the primary interface between enterprises and their technology and, as such, they serve as the nexus that connects the tech stack to the business stack. Some business processes are enabled by simple applications, such as email. In this case, the supporting infrastructure that enables email is also aligned with the business process and, ultimately, with the products and services that process enables. This provides a sense of what kind of technology-related problems can arise and how they can affect the enterprise and its offerings. Incidentally, this model works for both for-profit and nonprofit, and public- and private-sector enterprises. In all cases, an enterprise exists to offer something, and technology is aligned with those offerings to enable them. In some cases (such as the email example), technology is aligned with multiple business processes and corresponding products and services. Once this mapping of offerings and technology is complete, risk scenarios can be created.

Developing Fully Qualified Risk Scenarios

There are different levels of scenarios, depending on where in the business process map the scenario exists. For instance, at the very top (e.g., board reporting), there are likely to be only a handful of aggregate scenarios. Scenarios in the middle parts of the enterprise (e.g., senior management, heads

Figure 2—Business Process Mapping That Connects Products and Services to Technologies



of various lines of business) will include additional decompositions of those aggregate scenarios that are linked to specific products and services. At the very bottom, there will be many versions of cyberscenarios that trigger upper-level scenarios.[14] An example of this kind of decomposition is presented in **figure 3**.

When designing top-tier risk categories, it is important to consider the specific business in which the enterprise is engaged. However, one can start with the following Basel II event categories, even for enterprises that are not involved in financial services:[15]

1. Internal fraud
2. External fraud
3. Employment practices and workplace safety
4. Clients, products and business practice
5. Damage to physical assets
6. Business disruption and system failures
7. Execution, delivery and process management

Most enterprises will have some version of categories 1, 2, 5, 6 and 7 that covers their technology risk. An example of applicable risk categories (based on **figure 3**) would be the following:

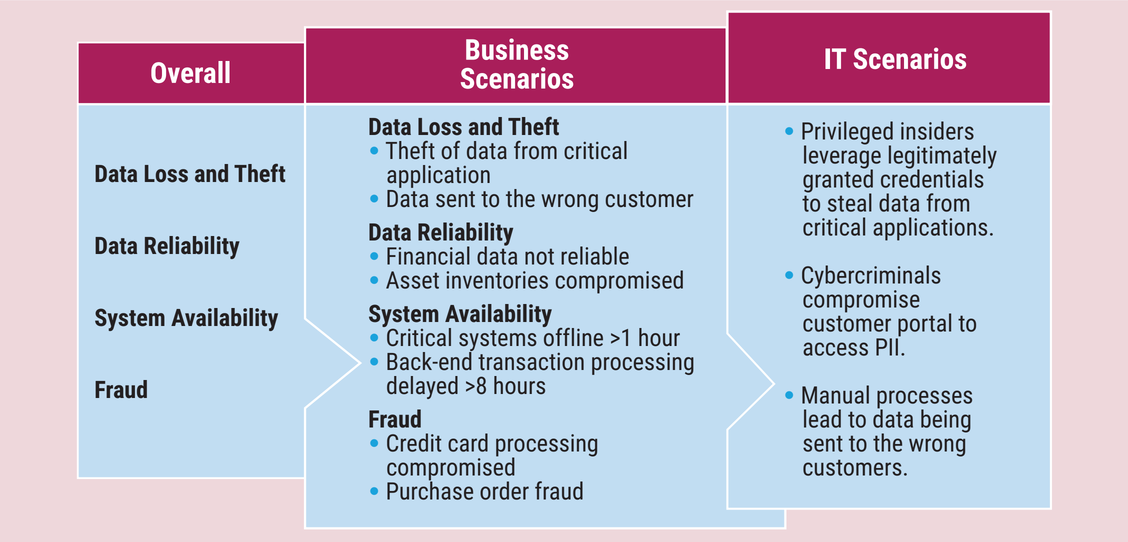
1. Data loss and theft
2. Data reliability
3. System availability
4. Fraud

> “WHEN DESIGNING TOP-TIER RISK CATEGORIES, IT IS IMPORTANT TO CONSIDER THE SPECIFIC BUSINESS IN WHICH THE ENTERPRISE IS ENGAGED.”

These four risk categories are suitable for board-level reporting. They can then be decomposed into product- and service-specific versions that reflect scenarios in a particular line of business as shown in **figure 3**.

Although such labels are helpful for grouping risk, these categories need to be decomposed one more level to get a fully qualified risk scenario that provides a greater degree of precision in the risk assessment. For instance, “Theft of data from critical applications” is a useful category, but it does not provide enough detail about what is happening, who is doing it, and how to assess risk factors and the efficacy of controls. A fully qualified risk scenario might be: “Privileged insiders leverage

Figure 3—Decomposition of Risk Categories to Scenarios



Overall

Data Loss and Theft

Data Reliability

System Availability

Fraud

Business Scenarios

Data Loss and Theft
- Theft of data from critical application
- Data sent to the wrong customer

Data Reliability
- Financial data not reliable
- Asset inventories compromised

System Availability
- Critical systems offline >1 hour
- Back-end transaction processing delayed >8 hours

Fraud
- Credit card processing compromised
- Purchase order fraud

IT Scenarios

- Privileged insiders leverage legitimately granted credentials to steal data from critical applications.
- Cybercriminals compromise customer portal to access PII.
- Manual processes lead to data being sent to the wrong customers.

legitimately granted credentials to steal data from critical applications.”

This statement reveals several critical things. First, it states who is taking the action. Next, it states how they are accomplishing it. In this case, the enterprise has already granted these individuals the tools they need to perpetrate bad acts, which are also clearly identified as stealing data from critical applications. Most important is that the statement tells a story, and this type of narrative ensures that communication is clear and complete. As a category of loss scenario, “data loss” is useful, but the phrase may conjure different images to different people. A fully developed risk scenario articulates the specific way in which data loss occurs.

The next step is to connect the loss scenarios to the relevant technology assets. To accomplish this, it is necessary to identify the inherent attributes of those assets that connect them to the scenario. For instance, the preceding sample scenario would require only a single attribute: users permitted to see sensitive data. This is similar to the way insurance underwriters use demographic information to determine insurance premiums. Here, these inherent attributes link the right risk scenarios to the assets that could bring them about. Also, because the risk scenarios are worded in such a way that the risk formula can be applied accurately, technology assets can be linked, via their demographics, to risk ratings that represent how loss could occur in that system. The scenario tells a narrative that is specific to the tech stack and that can be aligned with the risk categories reported up through the enterprise.

Top-Down vs. Bottom-Up Risk Assessments

Bottom-up risk assessments are typically acknowledged to be far more complete than top-down assessments. However, because bottom-up assessments require the collection of large amounts of information from various technologies and individuals, most enterprises consider them overly time consuming, possibly resulting in an incomplete assessment before the due date for reporting.

Top-down risk assessments, in contrast, have the reputation of being fast and easy. They require fewer resources to accomplish and can provide meaningful results. They are, however, subject to the bias of the people conducting them at the top, who are usually disconnected from the day-to-day problems and risk scenarios that are well known to those at the bottom.

In practice, those performing audit functions typically do not suffer from these either/or scenarios. They acknowledge that they cannot possibly assess everything, and they select samples at the bottom for the categories at the top on which they want to report. Such a sampling approach can be very helpful for enterprises trying to bridge the gap between top-down and bottom-up risk assessments. Sampling, in

Enjoying this article?

- Read *Bridging the Digital Risk Gap.* *www.isaca.org/Bridging-the-Digital-Risk-Gap*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

conjunction with the risk scenario decomposition outlined earlier, provides the tools needed to confidently report on the state of risk in an enterprise.

The Sampling Approach to Risk Assessment

To use the sampling method:

1. Select a handful of samples from the lowest level to inform each top- and intermediate-level risk category. For example, in the data loss and theft category, correlate several intermediate-level risk statements from each business unit (e.g., theft of data from critical applications).
2. Select the cyberscenarios and tech stacks linked to them. This results in several specific, low-level resource stacks to assess. These can become the risk ratings used to justify the ratings applied at other levels.

This approach allows a top-down-style risk assessment with the benefit of assessing risk at the bottom to validate those ratings.

Initially, these samples should cover critical and key applications and infrastructure, but over time, an enterprise can sample most of its technology environment. For example, it can sample top applications in the first year, followed by second- and third-tier applications in the following years. The resulting risk assessments should include a scoping statement indicating that the rating is based on a sample (e.g., 15 percent) of critical applications and infrastructure. Such scoping can also be included in annual strategic plans, and any additional sampling requested by an enterprise can help security and risk leaders prepare better budgets for resources to support these requests.

Addressing "Broken Things"

Too often, lists of "broken things" find their way onto organizational risk registers. A good rule of thumb is that if an item in the register can be checked off, removed or completed with the right configuration change, technology or process implementation, it is probably not a risk scenario and does not belong on the risk register. However, these lists of broken things are very important to the overall risk management capability of an enterprise. Alongside each level in the risk scenario hierarchy, there should be a corresponding list of broken things, at increasing levels of detail as one goes down the list.

For example, a list of missing patches or misconfigured servers should not be on the risk register. Instead, they should reside on their own list of problems requiring attention, such as an issue management register or a break/fix register. These individual items can be categorized at an aggregate level in a way that allows them to be linked to cyberscenarios. For instance, several users may have been overprivileged with access to critical applications. This can be categorized as unnecessary permissions or privilege creep. That category can be aligned with the cyberscenario of "privileged insiders misusing legitimately granted permissions," for example. At a higher level, such broken things can be grouped in a category called "identity and access management."

> "BOTTOM-UP RISK ASSESSMENTS ARE TYPICALLY ACKNOWLEDGED TO BE FAR MORE COMPLETE THAN TOP-DOWN ASSESSMENTS."

Risk Ownership

It is a popular notion that a business entity "owns" risk. What this means in practice is that every item in the risk register must be aligned with an owner who is not in IT, risk management, cybersecurity and so forth. The risk should be aligned with someone responsible for the products and services articulated in the business process map. This represents a significant culture shift for most enterprises. For many, it is anathema to think that an IT professional does not "own" a data loss and theft risk. More to the point, IT may "own" a series of what operational risk professionals call risk triggers or a causal taxonomy, such as those "unnecessary permissions" mentioned earlier. Ultimately, the loss is owned by those responsible for the products and services affected. An important side effect of allocating risk ownership this way is that the assessment of a risk scenario varies from one business unit to the next. The amount of loss associated with customers is likely to vary significantly from one product to another. Thus, a risk statement can appear on multiple internal risk registers, likely with different risk ratings. For all such risk factors aligned with business units, it is important to assign a liaison person to act as a bridge between IT and the business unit to help with communication and translation of IT terminology and to assist with risk treatment decisions, including following up on fixing the broken things aligned with these risk statements.

Conclusion

Ultimately, technology programs exist so that enterprises can deliver the products and services for which they are chartered. With rare exceptions, enterprise leaders are not experts in delivering technology solutions. Every profession has its own language, acronyms and shorthand that enable professionals to communicate with one another expediently. However, IT is a profession that exists to serve an organizational objective and, as such, it needs to adjust its communications to help organizational leadership achieve their goals.

Being better aligned with the enterprise allows for better value creation, facilitates the perception of competence and alleviates internal feuds that distract from delivering on customers' expectations. Rearranging IT risk reporting to better align with the enterprise's understanding of its purpose and priorities improves communication and provides decision makers with the information they need to be better managers.

> "A RISK STATEMENT CAN APPEAR ON MULTIPLE INTERNAL RISK REGISTERS, LIKELY WITH DIFFERENT RISK RATINGS."

Endnotes

1 Griffin, E.; *A First Look at Communication Theory, 6th Edition*, McGraw-Hill, USA, 2006
2 Shannon, C. E.; "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, iss. 3, 1948, p. 379–423, 623–656
3 ISACA®, *State of Cybersecurity 2019*, *www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf*
4 Risk.Net, "Top 10 Operational Risks for 2019," 14 March 2019, *https://www.risk.net/risk-management/6470126/top-10-op-risks-2019*
5 Marsh & McLennan, Microsoft, "2019 Global Cyber Risk Perception Survey," September 2019, *https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf*
6 *Ibid.*
7 Copeland, J.; "No Time to Talk Cyber Risk, Senior Executives Say," Fair Institute Blog, 19 September 2019, *https://www.fairinstitute.org/blog/no-time-to-talk-cyber-risk-senior-executives-say*
8 Jones, J.; "Jack Jones: Quit Blaming Executives for Cybersecurity Problems," Fair Institute Blog, 19 August 2019, *https://www.fairinstitute.org/blog/quit-blaming-executives-for-cybersecurity-problems*
9 Laws, S. M.; "Corporate Communication: Identity, Image and Reputation," *International Journal of Business Competition and Growth*, vol. 3, iss. 4, 2014, p. 344–349
10 Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, USA, 2014
11 Maurice, D. R.; J. Rathod (ed.); "Cybersecurity and Technology Risk," *Operational Risk Perspectives: Cyber, Big Data, and Emerging Risks*, Risk Books, UK, 2016
12 *Op cit* Freund, Jones
13 *Ibid.*
14 Freund, J.; "Keep It Simple: How to Avoid Drowning in Cyber Risk Information," Risk.net, 2017, *www.risk.net/risk-management/3938516/keep-it-simple-how-to-avoid-drowning-in-cyber-risk-information*
15 Bank for International Settlements; " QIS 2–Operational Risk Loss Data," 2001, *https://www.bis.org/bcbs/qisoprisknote.pdf*

ISACA

Keep Learning

Get the training (and CPEs) you want from the comfort of your own home with **ISACA's online training solutions**. Choose from a variety of flexible training options for individuals and groups.

www.isaca.org/OnlineLearning-jv3

Human Error

A Vastly Underestimated Risk in Digital Transformation Technology

Também disponível em português
www.isaca.org/currentissue

There should be no doubt that digital transformation is an organizational necessity performed in the interest of maintaining, sustaining and enhancing an enterprise's relevance to its constituents. Specifically, relevance can concern everything from attracting customers in the private sector to increasing the convenience of and access to government services by citizens.

While there has been a strong focus on the "digital" aspect of digital transformation, the conversation has increasingly taken a more inclusive view of the impact of digital transformation on an enterprise—its customers, operating model and business model.[1]

Awareness of the extensive human risk factors extant in digital transformation needs to be enhanced.

Overview of Digital Transformation Technologies

Of all the emerging technologies out there, a number of them have been identified as being most likely to change the way organizations do business.[2] Given the dynamic nature of technological development, this list is subject to change, but there are several technologies that are most relevant today.

Drones

Drones, or unmanned aerial vehicles (UAVs), were originally built for military purposes.[3] They represent a convergence of several technologies, including robotics, artificial intelligence (AI) and aeronautics.

In 2013, one reason for the high number of drone crashes was believed to be the variety of control interfaces used for piloting the vehicles, resulting in the creation of the American National Standards Institute/Human Factors and Ergonomics Society (ANSI/HFES) 100-2007, with the goal of standardizing the control interface.[4] However, by 2016, technology was cited as the major cause of drone crashes, specifically, the loss of signal between the operator and the drone.[5] In a military context, drones are subject to human error and can have a negative impact on civilian life.[6]

Robotics

Robotics is also a convergence of technologies, including mechanical engineering, electronic engineering and computer science.

The word "robot" is "derived from the Czech word *robota*, meaning serf or laborer."[7] Robots need robust programming to be fully productive, and at this point, humans are still tasked with their programming. In spite of the right skills and due diligence, human coding errors can and do occur, disrupting workflow and production while codes are

Guy Pearce, CGEIT
Is the chief digital transformation officer at Convergence. He has also served on governance boards in the fields of banking and financial services, for a not-for-profit, and as chief information security officer of a financial services organization. Pearce has more than a decade of experience in data governance and IT governance and created a Digital Transformation course for the University of Toronto SCS (Ontario, Canada). He is the recipient of the 2019 ISACA® Michael Cangemi Best Author Award for contributions to the field of IT governance.

> “AI IS PROGRAMMED BY HUMANS AND, THAT AGAIN, IS EXACTLY WHERE THE ISSUES CREEP IN TO CREATE RISK.”

debugged, which can cost enterprises significant time and money.[8] Improper or erroneous maintenance can result in a malfunctioning robot, which can also be costly.[9]

Blockchain

While blockchain technology has moved beyond the hype of 2018, there are organizations that are using blockchain to solve real business problems, such as the sustainable production of cashmere in Mongolia.[10]

Although errors in blockchain are rare, the point of interface between the blockchain and other websites, interfaces and platforms is where human error can occur, and this needs to be resolved by deeper developer education.[11] Also, it is important to remember that when blockchain is used as a database, those data are subject to the same human shortcomings as any other database.[12] Integration risk and software vulnerability are the greatest human risk factors in this technology.[13]

3D Printing

With 3D printing, three-dimensional objects are formed layer by layer using a wide range of materials, rather than being created by skilled, precision artisans. This technology is used in manufacturing, where human error is a bigger factor than in other sectors.[14]

As with other emerging technologies, the lack of expertise and the software development requirements associated with 3D printing[15] still present human risk associated with the technology. While there are still challenges with the use of 3D printing in healthcare,[16] errors introduced due to human error in this sector can also have ethical consequences.

Internet of Things and Industrial Internet of Things

Faster Internet speeds with higher bandwidths have led to a proliferation of devices that can communicate with a central device or with other devices. This trend will accelerate with the adoption of 5G. Although a smartphone can be considered a type of Internet of Things (IoT) device with features such as a Global Positioning System (GPS) and a three-axis accelerometer, the Industrial Internet of Things (IIoT) explicitly involves industrial-grade, rugged, low-power (remote) sensors.

Again, the human risk factors in IoT and IIoT are related to programming and the hardware design of IoT and IIoT devices themselves.[17] Furthermore, these devices are often manufactured by robots, which have their own human challenges (as mentioned earlier), leading to a cascade of human risk factors. One of the greatest human risk factors, though, is found in cybersecurity,[18] and people are recognized as “the weakest link in information security.”[19]

AI

Autonomous thinking machines have captured the human imagination for years, leading to scary stories about a world ruled by intelligent robots. However, because today’s digital society is based on software that is vulnerable to programming failure and cyberattack, this singularity—the point where AI exceeds human intelligence—is highly unlikely.[20]

AI is programmed by humans and, that again, is exactly where the issues creep in to create risk. AI is deployed in drones, robots, IoT and IIoT devices. Human errors are, therefore, amplified and added to the errors occurring in the integrated technology. However, there is a more subtle risk associated with AI, which stems from the fact that AI is rife with human bias.[21] Because AI needs humans to validate its outcomes,[22] at least initially, human error can creep in to impact outcomes. Another issue is the quality of the data used to train AI systems. Based on experience, data quality is almost never as good as it needs to be.

Augmented Reality/Virtual Reality

In one sense, virtual reality (VR) is a digital twin of the reality it models. Augmented reality (AR), by contrast, adds to the VR experience. For example, Google Lens provides additional information about the physical reality with which one is interacting.

Again, sensors pick up information, and its interpretation is determined by programming. Likewise, the quality of the augmentation is determined by the quality of the programming. If something observed in the physical reality is not in the VR "dictionary," it might not be depicted as intended in the virtual rendition. So the quality of the AR/VR experience depends on the quality of data it receives by means of the relevant sensors and by means of the data used to create the model for the recognition engine, the latter of which may be negatively influenced by human deficiencies during modeling and programming.

Next Wave Technologies on the Doorstep

Major new technologies will continue to change the way business is conducted. Cloud technology is already here, and others such as 5G, serverless computing and biometrics must be considered. Again, each emerging technology involves human risk factors that are worth analyzing as part of a diligent digital transformation strategy.

Human Risk Factors

Based on the previous discussion, the common human risk elements in all the digital transformation technologies can be linked to programming, design and data. In other words, the same human endeavors that produce digital transformation technologies are the same ones that put them at risk.

To extend the analysis, IT risk can be considered across seven subdisciplines: cybersecurity, resilience, vendors and third parties, projects and change, software development life cycle (SDLC), data, and compliance.[23] SDLC refers to the process of producing software, whether agile or waterfall; it starts with architectural approval and concludes with deployment and maintenance. Each of these subdisciplines have human risk components:

1. **Cybersecurity**—"Countering cyber threats requires a focus on people and behaviours, not just technology."[24]
2. **Resilience**—"Human risk is neglected in disaster plans."[25]
3. **Vendors**—Performing vendor due diligence is a human-intensive effort, and errors can and do occur.

> "HUMAN ERRORS IN DATA CAPTURE, DATA TRANSFORMATION AND DATA MIGRATION HAVE BEEN AROUND FOR AS LONG AS THE COMPUTER ITSELF."

4. **Projects**—Managing change is part of a successful deployment and, for the most part, that change demands an alteration in human behavior to ensure desirable outcomes.
5. **SDLC**—Humans assess the architectural implications of a new technology, design the programs (and devices), write the programs and, to a large extent, test the programs, especially in complex deployments. Wherever humans are involved, errors are bound to be made
6. **Data**—Human errors in data capture, data transformation and data migration have been around for as long as the computer itself.
7. **Compliance**—Many compliance requirements are met by a set of rules, but some are open to interpretation. It may be human nature for the interpretation to err on the side of the organization, rather than in terms of the spirit of the legislation.

When assessing the risk related to an organization's digital transformation technology, it may be meaningful to create a table summarizing the relevant risk areas and then capture the details of each cell in a typical risk management framework (e.g., identify, analyze, evaluate, control, monitor, report). **Figure 1** illustrates the human risk elements (X) at the intersection of the seven IT risk subdisciplines and the most significant digital transformation technologies identified earlier. The dark pink shaded cells represent topics discussed in text. The interpretation of these risk domains depends on the incremental risk profiles of the specific deployments of the digital transformation technologies.

In **figure 1, i**t can be noted that resilience is especially relevant to robotics and IoT/IIoT, given

Figure 1—Human Risk Elements Based on IT Risk in Digital Transformation Technologies

		Digital Transformation Technologies						
		Drones	Robotics	Blockchain	3D Printing	IoT and IIoT	AI	AR/VR
IT Risk Subdisciplines	Cybersecurity					X		
	Resilience		X		X	X		
	Vendors	X	X	X	X	X	X	X
	Projects	X	X	X	X	X	X	X
	SDLC	X	X	X	X	X	X	X
	Data	X	X	X	X	X	X	X
	Compliance	X	X					

how critical these technologies are to the manufacturing sector. There is an across-the-board impact in the vendors, projects, SDLC and data subdisciplines, especially in large organizations. In particular, the data category entails both a human input risk and an output risk—that is, the human risk related to analyzing, interpreting and acting upon the data produced by a digital transformation technology. In the compliance category, in addition to ANSI/HFES 100-2007, International Organization for Standardization (ISO) ISO 9000 *Quality management* is important for manufacturing in which robotics plays a part.

Taking Steps to Reduce Human Error

IT audits have traditionally focused on resources when considering technology risk, but from the preceding analysis, it is clear that the (human) resource implications are much more significant than previously thought. As a result, the goal should be to reduce the incidence of human error. There are three capabilities that can lead to a reduction in human error:[26]

1. **Detectability**—The ability to identify mistakes and prevent them from occurring
2. **Traceability**—The ability to identify the root cause of the mistake and institute corrective actions
3. **Dexterity**—The ability to perform a task without incurring error

Each of these capabilities can be reinforced by a culture that supports suitable training and processes. The question is whether the incremental costs required to implement these measures are considered worthwhile in the context of mitigating the potential costs of an error.

Ultimately, whatever steps are taken to reduce human error, auditors should "maintain sufficient professional skepticism when reviewing management's risk assessment for new systems"[27] by considering people as a driver (cause) of risk rather than merely reporting on its symptoms (e.g., "buggy" code).

> "IT AUDITS HAVE TRADITIONALLY FOCUSED ON RESOURCES WHEN CONSIDERING TECHNOLOGY RISK, BUT…IT IS CLEAR THAT THE (HUMAN) RESOURCE IMPLICATIONS ARE MUCH MORE SIGNIFICANT THAN PREVIOUSLY THOUGHT."

Conclusion

Figure 1 illustrates that the human risk element is pervasive in digital transformation technology. It is present in each of the digital transformation technologies discussed in this article and in each of the subdisciplines of IT risk. The scale of human risk in digital transformation is expansive, necessitating an intense focus on people and behavior (culture) when striving to implement a successful digital transformation strategy, including mechanisms that explicitly focus on reducing the incidence of human error.

Importantly, the cascading effect of human error occurring when the human risk in one technology (e.g., AI) is introduced into another technology that has its own human risk elements (e.g., drones) means that risk management becomes more complex. Urgent measures are needed to ensure the sustainability of not only the new technology, but also of the organization deploying the new technology and to guarantee the success of the digital transformation strategy.

Given the scale of the human risk elements identified in digital transformation technology, it should be obvious that merely performing some quick "change management" intervention after deployment will be insufficient (part of the "Projects" row in **figure 1**). The human factor is present in almost every element of digital transformation, meaning that special, extended attention is needed to mitigate the associated risk and, ultimately, to ensure the success and sustainability of the digital transformation initiative.

Endnotes

1 Pearce, G.; "Enhancing the Board's Readiness for Digital Transformation Governance," *ISACA® Journa*l, vol. 5, 2019, *https://www.isaca.org/archives*

2 Pearce, G.; "Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation," *ISACA Journal*, vol. 4, 2019, *https://www.isaca.org/archives*

3 Vyas, K.; "A Brief History of Drones: The Remote Controlled Unmanned Aerial Vehicles (UAVs)," *Interesting Engineering*, 2 January 2018, *https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs*

4 Atherton, K. D.; "What Causes So Many Drone Crashes?" *Popular Science*, 4 March 2013, *https://www.popsci.com/technology/article/2013-03/human-error-after-all/*

5 *Business Insider*, "Drone Accidents Are Due to Tech, Not Human Error," 25 August 2016, *https://www.businessinsider.com/drone-accidents-due-to-tech-not-human-error-2016-8*

6 King, T.; "Positive and Negative Effects of Drones," Positive Negative Impact, 8 July 2019, *https://positivenegativeimpact.com/drones*

7 Hockstein, N. N.; C. G. Gourin; R. A. Faust; D. J. Terris; "A History of Robots: From Science Fiction to Surgical Robotics," *Journal of Robotic Surgery*, 17 March 2007, *https://link.springer.com/article/10.1007/s11701-007-0021-2*

8 Matthews, K.; "Four Reasons You Still Need to Watch for Human Error When Working With Robotics," RobotIQ, 22 November 2018, *https://blog.robotiq.com/4-reasons-you-still-need-to-watch-for-human-error-when-working-with-robotics*

9 *Ibid*.

10 Huang, R.; "UN Pilot in Mongolia Uses Blockchain to Help Farmers Deliver Sustainable Cashmere," *Forbes*, 28 December 2019, *https://www.forbes.com/sites/rogerhuang/2019/12/28/un-pilot-in-mongolia-uses-blockchain-to-help-farmers-deliver-sustainable-cashmere/#60cedd8717d9*

11 Tanase, B.; "Human Error as a Limitation for Blockchain Adoption?" *Medium*, 21 December 2017, *https://medium.com/@biancatanase/human-error-as-a-limitation-for-blockchain-adoption-80f3da30e8be*

Enjoying this article?

- Read *The Future of IT Audit. www.isaca.org/Future-of-IT-Audit*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

12 Davies, C.; "Blockchain's Issues and Limitations," Cryptoboom, 9 December 2017, *https://cryptoboom.com/basics/blockchain/blockchains-issues-and-limitations*

13 Raman, R.; M. Mangnaik; "Blockchain Can Transform the World, but Is It Fool-Proof?" *Huffington Post*, 24 January 2017, *https://www.huffingtonpost.in/raja-raman/blockchain-can-transform-the-world-but-is-it-fool-proof_a_21660586/*

14 Wright, I.; "Human Error Is Worse in Manufacturing Compared to Other Sectors," *Engineering.com*, 8 November 2017, *https://www.engineering.com/AdvancedManufacturing/ArticleID/15974/Human-Error-is-Worse-in-Manufacturing-Compared-to-Other-Sectors.aspx*

15 Tractus3D, "3D Printing for Manufacturing," *https://tractus3d.com/industries/3d-printing-for-manufacturing/*

16 Wright, C.; "3D Printing in Healthcare," PreScouter, April 2017, *https://www.prescouter.com/2017/04/3d-printing-healthcare/*

17 Joyce, J.; "How the Internet of Things Is Affecting Laboratory Equipment," *Lab Manager*, 7 May 2018, *https://www.labmanager.com/laboratory-technology/2018/05/how-the-internet-of-things-is-affecting-laboratory-equipment*

18 *Ibid*.

19 Lineberry, S.; "The Human Element: The Weakest Link in Information Security," *Journal of Accountancy*, 1 November 2007, *https://www.journalofaccountancy.com/issues/2007/nov/thehumanelementtheweakestlinkininformationsecurity.html*

20 Thomas, M.; "Human Error, Not Artificial Intelligence, Poses the Greatest Threat," *The Guardian*, 3 April 2019, *https://www.theguardian.com/technology/2019/apr/03/human-error-not-artificial-intelligence-poses-the-greatest-threat*

21 *Op cit* Pearce, "Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation"

22 Kent, J.; "Artificial Intelligence Success Requires Human Validation, Good Data," *Health IT Analytics*, 26 November 2019, *https://healthitanalytics.com/news/artificial-intelligence-success-requires-human-validation-good-data*

23 McKinsey & Company, "'The Ghost in the Machine': Managing Technology Risk," July 2016, *https://www.mckinsey.com/business-functions/risk/our-insights/the-ghost-in-the-machine-managing-technology-risk*

24 Walker, E.; D. Witkowski; S. Benczik; P. Jarrin; "Cybersecurity—The Human Factor," Federal Information Systems Security Educator's Association, 2017, *https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf*

25 Ashford, W.; "Human Risk Is Neglected in Disaster Plans, Warns Study," *Computer Weekly*, 9 November 2007, *https://www.computerweekly.com/news/2240083858/Human-risk-is-neglected-in-disaster-plans-warns-study*

26 Nakata, T.; "Human Error Prevention," Slideshare, 19 December 2011, *https://www.slideshare.net/torunakata/human-error-prevention*

27 Lindsay, J. B.; A. Doutt; C. Ide; "Emerging Technologies, Risk, and the Auditor's Focus," Harvard Law School Forum on Corporate Governance, 8 July 2019, *https://corpgov.law.harvard.edu/2019/07/08/emerging-technologies-risk-and-the-auditors-focus/*

How to Balance Insider Threats and Employee Privacy

Recent headlines are replete with extremely costly and disruptive examples of insider threats playing a prominent role in high-profile data breaches.

For instance, in September 2019, an American Express employee accessed and stole copious amounts of customer data that he intended to use to perpetrate identity fraud. As a result, the financial services enterprise was forced to notify its customers of a self-inflicted wound that placed their personal information at risk.[1]

Meanwhile, a former Yahoo employee pled guilty to accessing and stealing sexual images from more than 6,000 customer accounts. The breach was a horrific invasion of privacy that included some of the employee's personal friends and colleagues.[2]

Of course, few insider threats are as costly as the one that compromised the data of 4.2 million members of Desjardins, the largest federation of credit unions in North America, ultimately costing the cooperative US$108 million.[3] The employee responsible for the breach was fired, but that retroactive response will not offset recovery costs or restore the enterprise's tarnished reputation.[4]

These events, when coupled with the thousands of incidents of accidental sharing, make it clear that, for many enterprises, the most significant cybersecurity threat is not an abstraction that exists outside the enterprise. It is most likely sitting in the cubicle next door.[5]

Given the dynamic nature of today's threat landscape and the increasing cost of failure when it comes to data security,[6] it is not surprising that 98 percent of enterprises monitor their employees' digital behavior.[7] However, these initiatives are coming to fruition at a time when data privacy is at the forefront for government regulators, legislators and employees. In short, although employee monitoring software can help prevent a costly data breach, its implementation can backfire if it is not handled correctly.

The following considerations can ensure a proper deployment of employee monitoring software, helping the organization achieve a privacy-friendly approach to insider threat prevention.

Pick a Purpose

With today's incredibly capable employee monitoring software, the insights an enterprise can glean are almost endless. While this expansive versatility makes software adoption simple, it can be a hindrance when trying to protect employee privacy.

For example, an enterprise deploying employee monitoring software to protect the enterprise's data may assess and evaluate data access points, data movement or unusual network activity. In contrast, an enterprise assessing productivity is likely to be more interested in knowing how much time employees spend on websites or using applications.

To ensure that employee privacy is an integral part of employee monitoring, the focus of monitoring can be narrowed by identifying its purpose. Once this priority has been established, an enterprise can

Isaac Kohen
Is vice president of research and development for Teramind, a leading global provider of employee monitoring, insider threat detection and data loss prevention solutions.

Enjoying this article?

- Read *Enforcing Data Privacy in the Digital World. www.isaca.org/enforcing-data-privacy*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

choose the right software with the most prescient configurations to promote a seamless rollout.

Align Process With Purpose

Clearly identifying the purpose of monitoring helps enterprises make decisions about how to achieve desired outcomes without compromising employee privacy.

When instituting employee monitoring to protect enterprise and customer data, executives should take the time to understand information flows. This can identify specific pain points and vulnerabilities that may contribute to a data breach.

As privacy regulations become more onerous and widespread, many enterprises have no choice but to ensure employee privacy when implementing any workplace monitoring initiatives. In the United Kingdom, the Information Commissioner's Office recommends that enterprises conduct data protection impact assessments to determine the efficacy of their initiatives.[8] These assessments promote critical thinking about employee monitoring so that adverse impacts and additional obligations can be evaluated before implementation.

In short, privacy-focused enterprises do not let monitoring programs run out of control. Instead, they align their processes with their purposes, while prioritizing intentionality at all times.

Communicate Standards

Secret monitoring is not the solution to data loss prevention. Indeed, there is little evidence that undisclosed monitoring is effective in protecting enterprise data. It can negatively impact employee morale and place enterprises in a dubious legal position.

Instead, open and clear communication with employees should be prioritized. Failure to communicate expectations sets employees up for failure and it can foster a negative workplace culture that offsets many of the gains derived from employee monitoring.

In general, employees need to know the following:

- Purpose of the new monitoring initiative
- Software used to collect their data
- Plan for managing, securing and evaluating their information
- Expectations for personal data management and accessibility

Ultimately, employee monitoring works best as a collaboration. All stakeholders can contribute to the process, and privacy-oriented enterprises can use the information obtained to determine best practices and propagate a culture of data security.

Choose the Best Technology

Enterprises have no shortage of options when it comes to employee monitoring. As employee monitoring becomes a new workplace standard, many new products provide in-demand features at an affordable price.[9]

Employee monitoring software can significantly reduce an enterprise's exposure to data loss events, but failing to secure this information at the expense of employee privacy is a nonstarter in today's business world. So, when choosing software, make privacy the first priority.

Specifically, features such as auto-redaction of personal information, time- or location-sensitive monitoring, or automated data access regulation can secure enterprise data without unnecessarily revealing employee information. The following are some of the other criteria to look for:

- **Features**—The features and benefits should be compared. Is it easy to use? Ask if the organization needs additional features like time tracking, productivity optimization and payroll management. Does it support anonymization, redaction/black-out, encryption, etc., to protect privacy?
- **Business case**—Can it deliver on the organization's business requirements? For example, if the organization has employees or customers in the European Union, organizations must check to see if the employee monitoring system supports EU General Data Protection Regulation (GDPR) compliance requirements such as data retention and erasure policies.
- **Flexibility**—How configurable is the solution? For example, does it allow the organization to create

segregated, role-based access control (RBAC) to reduce data exposure on a need-to-know basis? Can the monitoring objects be configured to allow employee privacy?

- **Price vs. value**—Does the product/price justify the return? Will it improve the productivity of employees by eliminating application overload, task-switching and idling? Are there any hidden costs such as maintenance, upgrades and support?
- **Deployment**—How fast can the organization get started? What are the deployment options? Can an enterprise, for example, deploy it on its own data center/on-premise to comply with border restrictions? If it is cloud based, can the vendor ensure business associate agreements (BAA) required by GDPR/US Health Insurance Portability and Accountability Act (HIPAA)-type regulations?
- **Vendor reputation**—Are they any good? Do they have great customer reviews? What is their experience in the organization's specific industry?
- **Support/service-level agreement**—Implementing an employee monitoring and data loss prevention solution can be complicated, especially if an organization does not have in-house resources. Will the enterprise get the help and ongoing support from the vendor?
- **Integration**—Is the software a monolithic product or can its usefulness be extended? For example, can it be connected to the existing security and incident security information and event management (SIEM) system to orchestrate a unified security system?
- **Compatibility**—Will it work well with IT systems? Is it compatible with the software employees use?

Conclusion

Data security is much more than an altruistic priority. Consumer sentiment is trending against enterprises that cannot protect their information, so enterprises need a way to protect their customers' data from malicious or accidental data leaks by its employees. Such threats have cascading consequences for enterprises of every size, yet organizations also need to uphold their employees' privacy right.

Fortunately, these imperatives are not mutually exclusive. It is possible to protect against insider threats while preserving employee privacy. It just requires an intentional effort to make it happen.

Endnotes

[1] Abrams, L.; "American Express Customer Info Accessed by Employee for Possible Fraud," Bleepingcomputer, 2 October 2019, *https://www.bleepingcomputer.com/news/security/american-express-customer-info-accessed-by-employee-for-possible-fraud/*

[2] Martin, A.; "Yahoo Engineer Admits Hacking Thousands of Accounts to Steal Sexual Images," News.sky, 1 October 2019, *https://news.sky.com/story/yahoo-engineer-admits-hacking-thousands-of-accounts-to-steal-sexual-images-11824338*

[3] The Canadian Press, "Desjardins Group Says 2019 Theft of 4.2 Million Members' Data Cost $108 Million," *Global News*, 26 February 2020, *https://globalnews.ca/news/6599224/desjardins-data-theft-cost-108-million/*

[4] Zurkus, K.; "Desjardins Insider Accessed Data of 2.9m Members," *Infosecurity*, 21 June 2019, *https://www.infosecurity-magazine.com/news/desjardins-insider-fired-for-1*

[5] Pepper, T.; "Alarming Statistics Show Human Error Remains Primary Cause of Personal Data Breaches," Realwire, 20 August 2019, *https://www.realwire.com/releases/alarming-statistics-show-human-error-remains-primary-cause-of-data-breaches*

[6] IBM, *2019 Cost of a Data Breach Report*, USA, 2019, *https://www.ibm.com/security/data-breach*

[7] Matyszczyk, C.; "In a Startling New Study, Companies Admit to Spying on Employees Far More Than Employees Realize," *Inc*, 19 February 2020, *https://www.inc.com/chris-matyszczyk/study-shows-how-much-companies-spy-on-employees.html*

[8] Information Commissioner's Office, "Data Protection Impact Assessments," UK, *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/*

[9] Krouse, S.; "The New Ways Your Boss Is Spying on You," *The Wall Street Journal*, 19 July 2019, *https://www.wsj.com/articles/the-new-ways-your-boss-is-spying-on-you-11563528604*

CASE STUDY

Building a Rock-Solid ERM Culture on FAIR

Rock Holdings, Inc., is a US-based holding company which owns several subsidiary companies including Quicken Loans, the US's largest mortgage lender. Due to strategic, operational and regulatory requirements, Rock Holdings has implemented quantitative risk analysis using Factor Analysis of Information Risk (FAIR). Over time, Rock Holdings' FAIR implementation transformed the business' enterprise risk management (ERM) program and risk culture. Along the way, Rock Holdings' Keith Weinbaum, an enterprise risk management architect and thought leader, has led the Rock Holdings enterprise risk team.

Introduction

A risk culture consists of the social and organizational backdrop for how an organization manages risk. In an effective culture, business risk owners are well informed about potential issues and are accountable for them. The owners are able to integrate considerations into managing value-producing business processes and strategies. They can express their risk appetite to technical and operational teams and, at a high level, direct the risk treatment strategies those teams take.

Risk Context

Many practitioners may be concerned primarily with information risk. However, organizations can benefit from creating an integrated risk management approach across information risk and ERM. The trick is to manage risk in the language of the business. That "language" is dollars, euros, yen or whatever local currency is used. The quantitatively oriented FAIR standard provides the analytical machinery to do this.

Risk Terminology

Risk (per FAIR)—The probable frequency and probable magnitude of future loss

FAIR—Factor Analysis of Information Risk

Information risk—Risk of business losses due to IT operational or cybersecurity events

Risk appetite—The level of risk an enterprise will take in an effort to accomplish its mission

Enterprise risk management—The methods and processes used by organizations to manage the business risk universe (e.g., financial, operational, market) and to seize opportunities related to the achievement of enterprise objectives

Dan Blum, CISSP, Open FAIR
Is an internationally recognized strategist in cybersecurity and risk management. His forthcoming book is *Rational Cybersecurity for the Business*. He was a Golden Quill Award-winning vice president and distinguished analyst at Gartner, Inc., has served as the security leader at several startups and consulting companies, and has advised hundreds of large corporations, universities and government organizations. Blum is a frequent speaker at industry events and participates in industry groups such as ISACA®, FAIR Institute, IDPro, ISSA, the Cloud Security Alliance and the Kantara Initiative.

Keith Weinbaum, CISSP, Open FAIR
Has worked at Quicken Loans for 20 years and is currently an enterprise risk architect. He built the information security function and led it for 10 years. From there, he built the enterprise risk management function which he led for six years. He oversaw the implementation of FAIR, which has been a centerpiece in how most risk is measured enterprisewide. As an architect, he now exclusively focuses on improving risk management-related processes and technologies.

The discipline used in the industry to manage risk culture at the enterprise level is called, appropriately enough, enterprise risk management (ERM). ERM processes plan, organize and lead activities to minimize risk impact on the business assets, revenues or earnings. ERM includes financial, strategic and operational risk and the risk of accidental losses.

Most organizations now operate as digital businesses with high reliance on IT. They can benefit by targeting overall risk reduction as a goal as opposed to focusing on meeting IT compliance obligations. Visibility into the overall security of the organization plays an important role in establishing this new dialog.

In recent years, investors and government regulators have begun to scrutinize the management policies and procedures of many different businesses. In some industries, boards of directors (BoDs) are now required to oversee and report on the adequacy of a business's risk management processes. In financial services, regulatory authorities such as the US Securities and Exchange Commission (SEC), US Federal Financial Institutions Examination Council (FFIEC), the US Consumer Financial Protection Bureau (CFPB) and their counterparts in other jurisdictions mandate a formal ERM-like approach to risk management.

Rock Holdings provides a unique risk culture case study with a:

- Financial services company that includes Quicken Loans (the US's largest mortgage lender)
- ERM program that started with information risk management using FAIR and evolved through three stages to become a valuable ERM program now in operation at most of Rock Holdings' subsidiaries

Company Background

Rock Holdings, Inc., is the parent company of several financial technology (fintech) businesses. These companies include:

- **Quicken Loans**—The US's largest mortgage lender, which created the first fully digital mortgage experience (Rocket Mortgage)
- **Quicken Loans Mortgage Services (QLMS)**—A tech-enabled mortgage origination platform and division of Quicken Loans serving independent mortgage brokers, community banks and credit unions across the United States
- **Rocket Homes**—A digital home search platform that can match clients with high-quality, prescreened real estate agents nationwide
- **Rocket Loans**—An online personal loan platform
- **Rock Connections**—A national strategic marketing company specializing in outbound and inbound client service for numerous online and technology-based businesses

Risk Management Pain Points and Timeline

Acquisitions, growth, digital business and financial services industry security challenges have driven an ongoing evolution of risk management at Quicken Loans and Rock Holdings over the past eight years. **Figure 1** shows the overall timeline for establishing ERM at Rock Holdings as it dealt with the following pain points:

- Inability to communicate information risk in business terms
- Increasing financial legal and regulatory requirements for risk management
- Information risk not integrated into ERM
- Increasing risk complexity

Figure 1—Quicken Loans' and Rock Holdings' Risk Management Timeline

Risk Management Program Development Stage	Scope	Timeline
Security program using qualitative risk management	Quicken Loans	Prior to 2012
Risk management program began using quantitative analysis with FAIR for information risk	Quicken Loans	2012–2014
ERM program established, also using quantitative risk management	Quicken Loans	2013–2014
ERM program expanded to additional Rock Holdings companies	Rock Holdings companies	2017–2020

> "DESPITE THE MAGNITUDE OF PROJECTS REQUIRING THAT MORE THAN 100 IT AND OTHER RESOURCES BE DIVERTED TO WORK ON CONFIDENTIALITY CONTROLS,…THE COMPANY ACCEPTED THE NEED ONCE IT WAS EXPRESSED THROUGH THE ERM PROCESS."

There were a number of stages to the effort and, in each stage, pain points were addressed.

Establishing Information Risk Management and ERM at Quicken Loans

At the beginning of the timeline in **figure 1**, Keith Weinbaum was the director of information security. In his operational role, Weinbaum requested budgets and resources from the Rock Holdings chief executive officer (CEO). However, there was not a proper process established to handle such requests.

Pain Point: Inability to Communicate Information Risk in Business Terms

Once a process was established, there was still dissonance between the information security team and leadership. Creating a dialog between the two teams, where both understood exactly what the other was talking about, took time. Although most security requests were approved, neither Weinbaum nor the CEO were satisfied with stock answers such as "Hackers might break in and wire themselves money or steal personal or financial information about our customers."

Weinbaum investigated multiple risk management methodologies and processes, such as COBIT®, the US National Institute of Standards (NIST) Special Publication (SP) 800-30 and OCTAVE. He concluded, "The best one for the quantitative analysis capabilities we knew we required was FAIR. It produced feedback that was easier to report back to leadership because it broke risk down to dollars and cents—a language both leadership and I understood completely." In 2012, Weinbaum received approval to hire two FAIR experts and began building an information risk management program.

Even at the early stages of Quicken Loans' risk management journey, quantitative risk management enabled security program evaluation and improvement. After establishing tools and methodologies, the team began an analysis to assess Quicken Loans' top information risk scenarios and the risk-reducing benefits of all major security projects. Before completing this exercise, the enterprise risk team pivoted to work on financial and operational risk for the ERM program, but the team eventually shared its prioritized recommendations for security projects. Weinbaum found that approximately 90 percent of the recommendations were for projects previously requested, but 10 percent were new projects. Also, 10 percent of existing projects were found to have insufficient risk reduction benefits and were then deprioritized.

Pain Point: Financial Legal and Regulatory Requirements for Risk Management

In parallel with the enterprise risk team's early efforts to quantify information risk, the legal and regulatory landscape was driving financial services companies such as Quicken Loans to provide better financial and operational risk management at the business level. As the CFPB pushed for formalized risk reporting and internal auditing, Quicken Loans' general counsel became a strong advocate for ERM.

However, when Quicken Loans launched an ERM project, Weinbaum and the team were concerned that the effort might adopt qualitative rather than quantitative risk management methodologies. In other words, a financial or operational risk scenario might be rated as "high risk" because it was assessed as a "4" on a scale of 1 to 5 rather than having a dollar value placed on it (i.e., annual loss expectancy of US$150 million and worst case loss estimate of US$450 million for a scenario despite a risk appetite of only US$100 million). After expressing these concerns to the CEO, Weinbaum's risk team was given the opportunity to lead a project working to create an ERM model for Quicken Loans based on FAIR.

From 2013 to 2014, the team instrumented risk analysis tools using FAIR methods for analyzing financial, operational and other business risk. The team found that working with executives on analyzing potential mortgage default rates and other financial risk scenarios they already understood quite well made it easier to get buy-in for using FAIR modeling terminology, calibrated estimation methods, Monte Carlo simulation and other features in the ERM context.

Pain Point: Information Risk Not Integrated Risk Into ERM
Only after working through the top business risk scenarios over a two-year period and getting the ERM to a steady state did the program turn its full attention to one of the major top information risk challenges with which every enterprise is familiar—the risk of a confidentiality data breach. Analysis showed that more work needed to be done to bring confidentiality risk down below the enterprise risk appetite. Despite the magnitude of projects requiring that more than 100 IT and other resources be diverted to work on confidentiality controls, such as reducing the volume of sensitive information stored within data repositories where data were not absolutely needed, the company accepted the need once it was expressed through the ERM process. "It was a major commitment for the company and there were many other things those resources could have been doing. I don't think we would have been able to get this level of buy-in without first having our methodology accepted by the executives for use on their turf, for financial risk challenges they already understood," says Weinbaum.

Expanding Rock Holdings' ERM Coverage
As Rock Holdings expanded and grew its stable of subsidiary companies and IT systems, it faced new management challenges.

> "WE SHOULD IMPLEMENT ERM SERVICES FOR ALL ROCK HOLDINGS COMPANIES."

Pain Point: Increasing Risk Complexity
Weinbaum explains the challenges Rock Holdings' executives faced in the mid-2010s: "Companies were getting more complex, stretching executives' knowledge and decision-making abilities. The CEO and general counsel saw the value of quantitative ERM and how it could enable Quicken Loans to make more informed risk decisions."

In 2017, Weinbaum's risk team was tasked with expanding the ERM program to the other subsidiary companies. The expectation was to utilize ERM to provide decision makers a better understanding of the risk in existing business processes and the business cases for new projects as well as improved confidence in risk-informed strategic decision-making. "We should implement ERM services for all Rock Holdings companies."

From this point, the Rock Holdings enterprise was truly on the road toward creating an enterprise risk culture.

How Rock Holdings' Risk Team Established Multi-Company ERM

Once given the go-ahead for the Rock Holdings ERM project, Weinbaum began rolling out ERM to each of the (then) six companies. Rollouts started with the CEO for each company, as follows:

- Meet with the company CEO for a 90-minute session, including a demonstration of ERM processes and quantitative risk management.
- Identify a risk champion to work with from each company.
- Conduct a 25-question survey with each company CEO and report results to the Rock Holdings CEO.
- Work with the champion and other stakeholders to list the core business processes, assess each process's key risk factors, and update company-specific policies or procedures as necessary to create a repeatable assessment process.
- Build support for working with any specialized company processes into Rock Holdings' governance, risk and compliance (GRC) systems' risk management functions.

Prior to beginning the rollout, the enterprise risk team prepared a high-quality ERM demonstration to gain company CEO buy-in and to show that the effort was worthwhile and would yield valuable results. The team showcased policy management, compliance management, audit management, vendor risk management and issue management in the GRC tool. The demonstration concluded by showing how quantitative risk management could tie all the other GRC elements together to provide visibility of future loss exposure (in US dollars).

The risk team operationalized and instrumented ERM for each company during six overlapping four- to six-month periods. Including the company-level champions and ERM or FAIR specialists already on staff, the core risk team grew to approximately 10

Enjoying this article?

- Learn more about, discuss and collaborate on risk management and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

people. Internal auditors and other stakeholders were also engaged. The team sent monthly email updates to the list of stakeholders from all companies.

Scoping the Risk

The Rock Holdings risk team utilized a concept called the Scoping Triangle to create a generic risk matrix for business processes:

- **Assets**—Business processes, information, applications, services, facilities
- **Threats**—External cyberattacks, physical attacks, internal abuse, errors, etc.
- **Effects**—Process completed incorrectly or in an untimely manner, experienced breach of confidentiality, etc.

As the team analyzed risk scenarios, it leveraged information from the Rock Holdings business continuity management (BCM) process; however, it needed to go deeper. For each company, the team assessed business processes' data in the GRC system from business impact assessments (BIAs), which included dependency maps and availability risk assessments for the most important IT systems. However, the risk team needed to perform additional deeper analyses using the Scoping Triangle criteria.

Overall Risk Assessment Process

The risk team employed the following risk and control assessment methodology to analyze business-process-related risk for key risk scenarios:

- High-level inventory and scoping
- Key risk and control identification
- Key control documentation and testing
- Risk analysis, evaluation and treatment
- Risk monitoring

Risk Analysis Process

During the analysis process, the risk team took careful steps to ensure that key risk areas identified were both:

- **Comprehensively exhaustive**—Avoiding missing any key risk areas
- **Mutually exclusive**—Avoiding double dipping

Working with information from BCM teams and other stakeholders, the risk team mapped company functions to processes. It met with process owners seeking a deeper understanding of interprocess dependencies, applications or third parties used, success factors, failure modes, incident histories, known risk and performance metrics.

The team worked with the stakeholders and risk champions to decide which processes to measure first and, in some cases, to chain risk scenarios together (i.e., an effect on one asset is a threat to another) and identify potential root causes of risk in each scenario. The team endeavored to minimize its time demands on the business. Often, rather than scheduling meetings, risk specialists would temporarily embed themselves within a business process team and observe the team running its process.

The risk team employed a business process modeling notation (BPMN) tool and trained many stakeholders and business analysts in the tool's language. The team loosely measured risk to see if they appeared likely to exceed significant inherent quantitative thresholds and labeled those that did as "key" risk factors.

> "OFTEN, RATHER THAN SCHEDULING MEETINGS, RISK SPECIALISTS WOULD TEMPORARILY EMBED THEMSELVES WITHIN A BUSINESS PROCESS TEAM AND OBSERVE THE TEAM RUNNING ITS PROCESS."

Current State

As of Q1 2020, the ERM process at Rock Holdings, Inc.:

- Fully integrates Rock Holding's fintech companies into the ERM process
- Covers financial, market, credit, operational and information risk categories
- Documents all key risk areas in the multicompany GRC system
- Analyzes key risk scenarios using a customized quantitative risk analysis tool inspired by FAIR

- Reports key risk analyses to executives via periodic meetings and risk reports
- Provides monthly status updates to most Rock Holdings executives via the audit and risk team (ART)

Executive decision-making at Rock Holdings is benefiting from the ERM process. Through the monthly ART process, company executives can review risk exposure with senior leaders of operational functions such as mortgages, finance, human resources (HR) and IT. The enterprise risk team works with operational leaders in advance to prepare risk measurements. At the ART meetings, ERM facilitates risk decisions in discussions with executives and senior leaders.

Weinbaum also references Rock Holdings' Epic Ideas process for strategic decision-making as a proof point of ERM's success. The Epic Ideas process evaluates any large project involving IT. When submitting an Epic Idea, each project team can choose cost reduction, risk reduction or revenue generation as the project's primary theme. Risk reduction projects undergo a quantitative risk assessment. In a few cases, such projects were found not to reduce risk enough and were changed or cancelled.

Not all Epic Ideas currently undergo quantitative risk analysis. ERM has a seat at the table for all the projects and performs less formal quantitative analysis on some revenue-increasing or cost-reducing projects on a case-by-case basis. As the Epic Ideas process continues to mature, Rock Holdings will likely want quantitative risk analyses performed on any proposed effort, regardless of its primary theme.

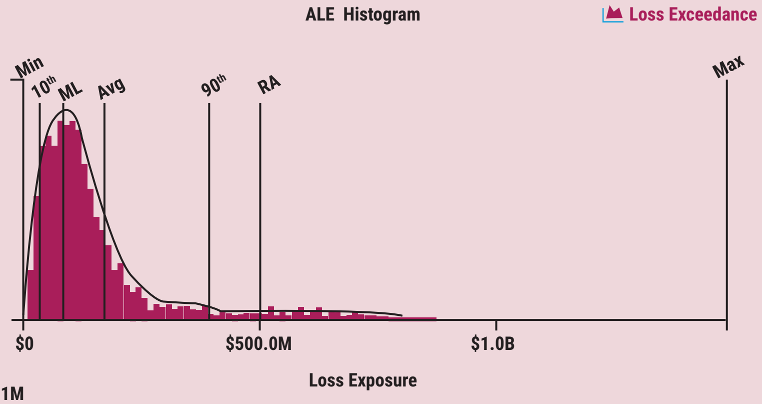
> “IN GENERAL, PROVIDING THE QUANTIFIED RISK INFORMATION IMPROVES DECISION-MAKING AND COMMUNICATION BETWEEN EXECUTIVES AND OPERATIONAL TEAMS IN THE BUSINESS.”

In general, providing the quantified risk information improves decision-making and communication between executives and operational teams in the business. As noted earlier, risk appetite can be difficult to quantify or it may change based on business events or contexts. Having a number for the current risk at any given time enables executives to initiate a more informed conversation with operational teams.

Figure 2 provides a diagram representative of the risk measurements that Rock Holdings' enterprise risk team and other organizations' teams using FAIR can bring to the table. Risk analysts prepare calibrated estimates for more than a dozen FAIR model risk components including (at a high level) Threat Event Frequency, Vulnerability, Difficulty, Primary Stakeholder Impact and Secondary Stakeholder Impact. For each component, the model expresses estimates as a range with minimum, maximum and most likely data points. The risk measurement process performs Monte Carlo simulations on all these components using the ranges. It feeds them into a loss exceedance curve, as shown in **figure 2**, depicting aggregate minimum, maximum, average and, most likely, annual loss expectancy.

Figure 2—Sample Annual Loss Exposure (ALE) in US Dollars Histogram

Maximum	$1B
90 percent	$385M
Most Likely (ML)	$90M
Average	$175M
10th percent	$48M
Risk Appetite (RA)	$43M
Minimum	$500M



All numbers rounded to the nearest $1M

Metrics

Although Rock Holdings has not reached the point of tracking formal metrics yet, Weinbaum is able to provide data or estimates on many of the following metrics (**figure 3**) recommended for customers who use ERM projects**.**

Lessons Learned

It is instructive to review lessons learned—what went well, what could have been done differently—after reaching risk program milestones.

What went well:

- **Closely engaged with stakeholders on areas of the risk universe that are familiar to them.** Because the risk team met with each company CEO and other stakeholders multiple times, executives were well-prepared for the ERM process. Because the team began by surfacing deeper analyses of business process risk areas that executives were familiar with, such as mortgage underwriting, the team found it relatively easy to get buy-in for the quantitative methodology.
- **Worked with one company or business unit at a time.** To enable a small team to cover multiple companies (or business units), Rock Holdings introduced the ERM program to one company at a time and focused exclusively on risk areas at the business process level. "Don't boil the ocean," says Weinbaum.

What could have been done differently:

- **Provide just-in-time training, or refresher training at critical points in the transformation process.** Stakeholders were trained once and bought into the methodology, but training was not repeated before ERM reports were exposed at the group level. By that time, some stakeholders had forgotten key concepts and became confused. In hindsight, Weinbaum advises periodically refreshing or reorienting stakeholders on key quantitative risk management concepts from time to time if they have not been involved recently.
- **Use off-the-shelf quantitative risk management tools.** When Rock Holdings began Open FAIR implementation in 2013, the discipline was at a very early stage. Commercially available tools, training and implementation support are now more widely available from vendors and consultants. Weinbaum believes that if he were starting the project now, Rock Holdings would be better off not to build its own risk analysis tool.

Figure 3—High-Level Metrics Recommended for Quantitative Risk Management Programs

Metric	Rock Holdings Results Representative of the Metric
Percent of corporate divisions covered by ERM process	Approximately 60 percent (this number was higher prior to acquisitions)
Percent of IT projects undergoing risk assessment	100 percent of large IT projects that are focused on reducing risk undergo a quantitative risk
Percent of security projects undergoing risk assessment	80 percent of security projects that get worked on are now validated by quantitative risk assessments
Percent of stakeholders satisfied with ERM process	90 percent stakeholder agreement with risk treatments recommended after assessments
(Yes/No) Complies with regulatory requirements	Y
Dollar value of inherent risk exposure reduction due to risk program	Rock Holdings has reduced millions of dollars of loss exposure by its own measurements
Cost savings (dollar value)	Saved on canceled security projects or Epic Ideas
Number of trained risk specialists	10
Number of trained stakeholders, conversant with the methodology	Enterprise risk team and stakeholders are able to perform "on the fly" quick assessments using the FAIR model
Average time required to perform quantified assessment	Typical risk assessment takes two to four weeks depending on the scenario's scope

Benefits

Rock Holdings acknowledges the benefits from the ERM program to be that executives and senior leaders can:

- Focus primarily on revenue generation
- Always know their future loss exposure and what is being done about it
- Compare different types of risk on an apples-to-apples basis
- Gain efficiencies from implementing consistent risk processes across the organization

Conclusion and Next Steps

In a constantly changing environment with multiple business units, processes and systems, ERM will never be perfect. Likewise, the work of evaluating risk scenarios will never be "done." ERM is an ongoing process. Rock Holdings' goal is to expand it to all companies and to measure all key risk scenarios. The enterprise risk team will continue to implement each component of the ERM process consistently, find best practices and spread them to all the companies. It is also a team goal to perform risk management through a more automated, real-time process so that risk owners can see loss exposure estimates based on current data values rather than only through point-in-time briefings.

Although Rock Holdings will continue to require specialists to operate its risk assessment tools and to fully understand FAIR and related quantitative analysis methodologies, the company plans to better train additional staff outside of the ERM group in basic risk analysis skills. This training will raise the general level of knowledge about the methodology and processes to reduce biases, improve staffs' ability to provide calibrated estimates and enable the risk process to operate more efficiently.

Train, Certify
Then Apply a World Leading Cybersecurity Framework

Explore the steps needed to implement NIST's Cybersecurity Framework (CSF) using ISACA®'s comprehensive COBIT® information and technology governance framework. Secure your organization and your future with the **Implementing the NIST Cybersecurity Framework Using COBIT 2019** program.

www.isaca.org/CobitNist-jv3

ISACA®

FEATURE

Addressing Key Pain Points to Develop a Mature Third-Party Risk Management Program

Third-party risk management is high on the boardroom's agenda. The business ecosystem is heavily dependent on third-party relationships, and with this dependence comes a responsibility to manage risk. There is a growing need to implement robust third-party risk management frameworks or improve and update existing programs.

The third-party landscape is evolving at a rapid pace, with on-demand service providers and fourth parties playing a significant role and work being moved to enterprises' global capability centers (another kind of third-party relationship). This supports the need for a strong third-party risk management framework.

Regulators are continuing to emphasize third-party oversight.[1] Although some industries have regulatory guidance to define their approaches to third-party risk management, others are solely dependent on internal requirements driven by the enterprise's risk framework. Regulatory-driven initiatives generally yield better results, but for those industries that lack regulatory mandates, other requirements such as the US Sarbanes-Oxley Act (SOX), the EU General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) can help improve and mature programs.

There is an inherent dichotomy when it comes to managing third parties. Business units that deal with third parties prefer seamless relationships; they want third parties to be quickly brought on board so they can start receiving services. Any risk management initiatives are seen as barriers to that relationship. Risk teams, in contrast, want to consider the risk factors in the relationship and take appropriate measures before third parties commence service delivery.

Cataloging third parties, tiering based on criticality, oversight commensurate with risk exposure, and improved reporting and governance are areas that typically require constant improvement for enterprises seeking a mature third-party risk management program.

Visveshwar Ramasubramaniam, CISA, CISM, CISSP, CCSP
Is an information security professional with more than 12 years of experience in information security, information assurance and third-party risk management. He has worked on multiple projects related to developing third-party risk management programs and conducted third-party assessments for organizations across banking, financial services, insurance; technology; and oil and gas industries.

Anil Kumar Singh
Is an information security professional with more than seven years of experience in information security, data privacy and third-party risk management. He has predominately worked for healthcare, IT, banking and insurance organizations. He has been involved in developing, establishing and streamlining privacy and third-party risk management frameworks for various organizations.

Typical Pain Points in Today's Third-Party Risk Management Program

Figure 1 illustrates the common pain points in a third-party risk management program.

Lack of a Holistic Third-Party Risk Management Program

In most cases, third-party risk management is synonymous with assessment. However, other aspects of third-party risk management include risk profiling, ensuring the use of appropriate language or requirements in contracts, and managing problems identified by assessments.

Some regulations provide directions for setting up a third-party risk management (TPRM) framework. Taking guidance from the regulations, a high-level framework can be developed, as shown in **figure 2**. Further, many add-ons or improvements are available that can enhance an existing third-party risk management program. These include:

- **Governance, risk management and compliance (GRC) tools**—The last decade saw the emergence of GRC tools to manage risk and compliance within an enterprise. This can be extended to third-party risk management. For instance, GRC tools can be leveraged to maintain inventories of third parties, conduct assessments, track issues to closure and so forth.
- **Dashboarding and reporting**—Multiple reports are required to be prepared and distributed to internal stakeholders, regulators, clients and others. Hence, it is critical to define and manage reporting parameters. Also, an analytical perspective that lists trends can be very useful.
- **Risk intelligence**—Risk intelligence on third parties is readily available. It is important to obtain the risk intelligence published by various sources and act on it. This is helpful in establishing continuous monitoring.[2]

Lack of Comprehensive Third-Party Coverage

Defining "third party" is essential to the success of a program. In less mature third-party risk management programs, the scope of third parties is restricted to typical IT service providers. In some cases, the scope is extended to include business process outsourcing arrangements. Therefore, it is critical to define what constitutes a third-party

Figure 1—Third-Party Risk Management Pain Points

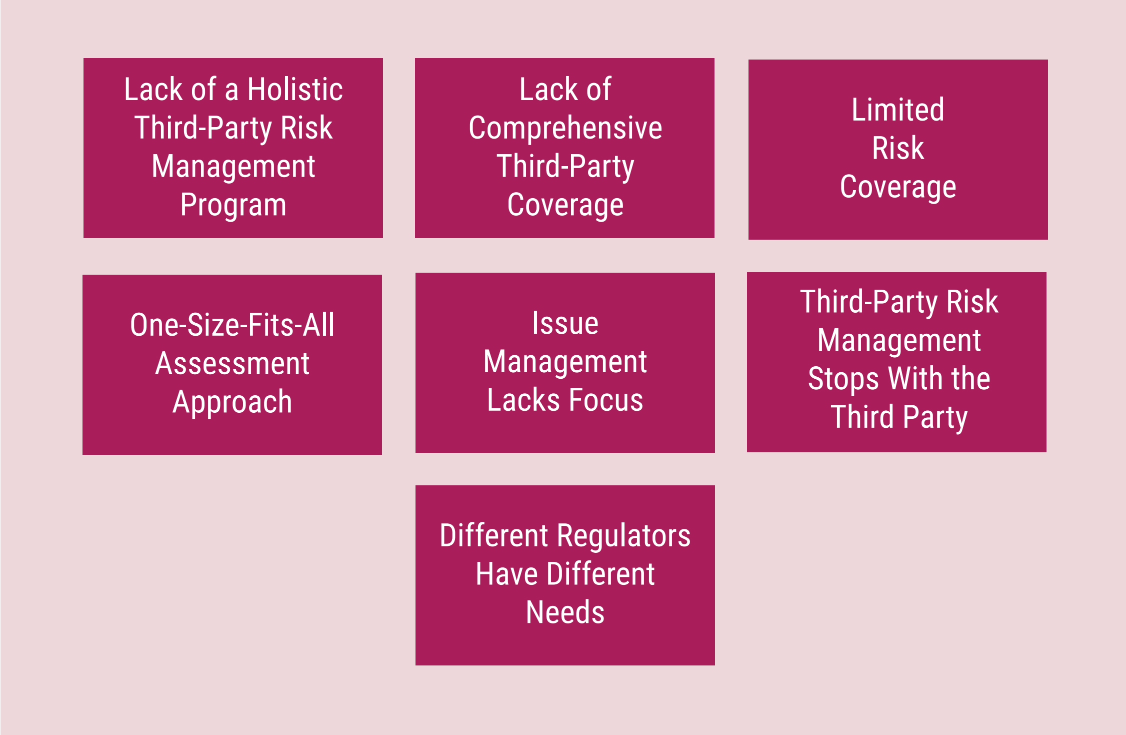
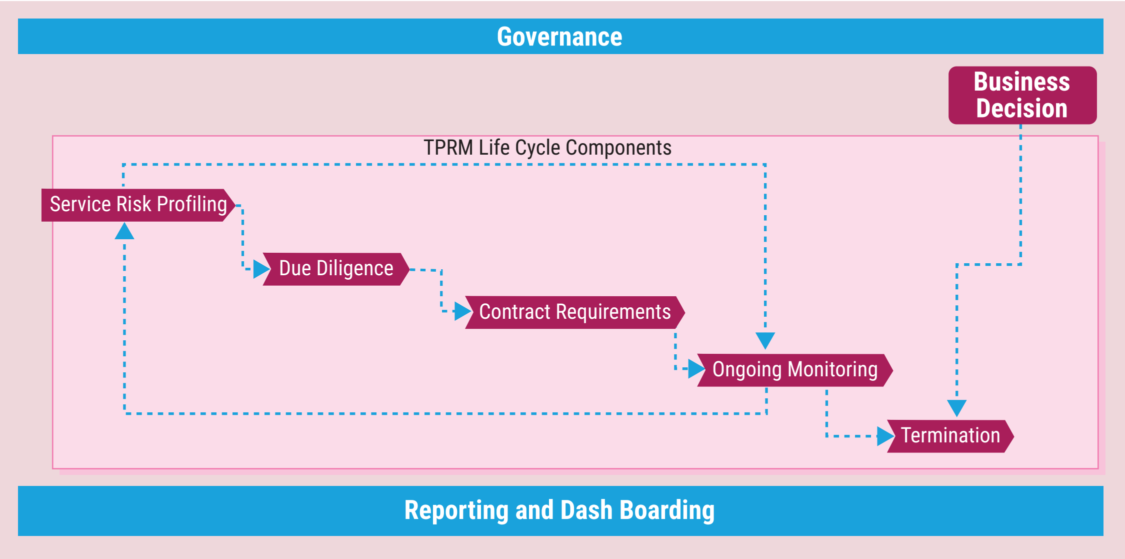

Lack of a Holistic Third-Party Risk Management Program
Lack of Comprehensive Third-Party Coverage
Limited Risk Coverage
One-Size-Fits-All Assessment Approach
Issue Management Lacks Focus
Third-Party Risk Management Stops With the Third Party
Different Regulators Have Different Needs

Figure 2—High-Level Risk Management Framework



arrangement. Ideally, all entities that have a contractual obligation to deliver services to the enterprise should be considered third parties.[3] Some examples of third parties are IT suppliers, business partners, affiliates, subsidiary enterprises, business process outsourcing/knowledge process outsourcing (BPO/KPO) service providers, subcontractors, distributors, brokers and dealerships.

A mature third-party risk management program has processes that can constantly scan and catalog third parties throughout the enterprise. This is more easily said than done. It is not uncommon for business units to enter into contracts with or procure services directly from third parties (e.g., shadow IT), which might lead to the skipping of essential steps in risk mitigation.

Different third parties pose different risk to an enterprise, so it is critical to profile third parties based on the appropriate parameters, which include:

- Volume of data accessed, processed or stored
- Type of data accessed, processed or stored
- Location from which services are provided
- Annual spending on the third party
- Business units or processes impacted by services provided by third party

One way of defining third parties is to classify them as mission critical, business essential or noncritical.

Limited Risk Coverage

Information and data privacy issues are top concerns when developing a third-party risk management program.[4] This is not surprising, as these are obvious risk factors in any third-party arrangement. However, third-party risk management involves much more. For instance, do third parties follow a responsible supply chain? Some of the broader risk domains that should be considered include concentration risk, geopolitical risk, credit risk and strategic risk.

If a third-party risk management program is heavily focused on a handful of risk factors and ignorant of other requirements, it might not identify the actual risk a third-party arrangement poses to the enterprise.

> “A MATURE THIRD-PARTY RISK MANAGEMENT PROGRAM HAS PROCESSES THAT CAN CONSTANTLY SCAN AND CATALOG THIRD PARTIES THROUGHOUT THE ENTERPRISE.”

Not all risk factors are relevant to all third-party arrangements, but it is essential to consider different risk domains across different third-party types and different phases of the program's life cycle.

A mature third-party risk management program provides for multiple risk domains that are mapped to different third parties based on their applicability, and it determines appropriate actions to mitigate the risk.

One-Size-Fits-All Assessment Approach

Although third-party risk management is evolving at a rapid pace, the assessment of third parties is still vital. This critical component can provide a snapshot of the third party's compliance posture.

Assessment must be efficient and commensurate with the risk exposure of the third party. Less mature third-party risk management programs use a single questionnaire or set of controls to assess all third parties. Such an approach is ineffective.

A mature third-party risk management program has a healthy mix of remote and on-site assessments and relies on service auditor reports (SARs) conducted at specified frequencies and covering relevant areas. The assessment program should define three parameters: frequency, mode and scope (**figure 3**).

Frequency

Third parties require assessment at different intervals. It might make sense to assess mission-critical third parties every year and noncritical third parties every two years. A mature third-party risk management program should also provide for *ad hoc* assessments in response to data breaches or any global threat.

Mode

It is also important to define the method of conducting the assessment. Common methods include:

- **SAR review**—Technically, this cannot be considered a mode of assessment; however, under certain third-party arrangements, the third party might be required to provide only attestation reports for the enterprise's consumption. It is, therefore, essential to understand what is available in these reports and how they line up with control requirements. It may be difficult to follow up on any identified problems, but it is important to ensure that they are addressed (see the later discussion of issue management).
- **Self-assessment**—This is the easiest method and requires little interaction. Typically, a questionnaire is sent to the third party to complete, and no additional clarifications are requested. Although this is easy to accomplish, it lacks comprehensiveness and relies completely on the third party's responses.
- **Remote assessment**—This mode is slightly more comprehensive than self-assessment. Enterprises conduct remote interviews and discussions and ascertain responses by the third party. This mode is especially effective when third parties are located around the globe, and it helps reduce costs. The downside is that multiple remote discussions might be required, extending the assessment schedule.
- **On-site assessment**—This is the most comprehensive assessment mode. Dedicated assessors visit third-party sites and conduct the assessment within a defined period. Although this method provides a high level of confidence in the assessment, it is costly.

> “A MATURE THIRD-PARTY RISK MANAGEMENT PROGRAM HAS A HEALTHY MIX OF REMOTE AND ON-SITE ASSESSMENTS AND RELIES ON SARS CONDUCTED AT SPECIFIED FREQUENCIES AND COVERING RELEVANT AREAS.”

Figure 3—Assessment Parameters

Third-Party Criticality	Frequency	Mode	Scope
Mission critical	Annually	On-site	Baseline controls plus focused control domains
Business essential	Biannually	Remote	Baseline controls

> “MOST ENTERPRISES OVERLOOK THE RISK ASSOCIATED WITH FOURTH PARTIES BECAUSE THEY RELY ON THEIR CONTRACTUAL ARRANGEMENTS WITH THIRD PARTIES TO MANAGE FOURTH PARTIES.”

All the preceding are viable options, as long as the assessments are well planned and executed. Some enterprises create two- or three-year assessment calendars, with adequate buffers for any ad hoc assessment requests.

Most important, all third-party contracts should include “right to audit (or) inspect” clauses. Third parties should be actively involved in the planning phase, and appropriate agreements should cover scope, logistics, evidence sharing and follow-up.

Scope

The most important element of an assessment is its scope. As discussed earlier, the risk assessment allows an enterprise to determine the various risk factors to which it is exposed through the third-party arrangement. So, it is essential to base the scope of the assessment on the characteristics of the third-party arrangement. One way to achieve this is to develop a baseline set of controls for assessment and then add other controls as needed.

Issue Management Lacks Focus

When problematic issues are identified by risk assessments, it can be a challenge to manage them. Some key challenges related to issue management include:

- Lack of defined ownership of identified issues
- No defined timelines for managing issues
- Lack of support from third parties for remediating identified issues

It is important to have a defined process that clearly identifies roles and responsibilities for managing problematic issues (**figure 4**). It is important to recognize that the issue management process is not the sole responsibility of the third party’s risk management team. It is a collaborative effort that includes multiple stakeholders such as business, senior management, suppliers and the like.

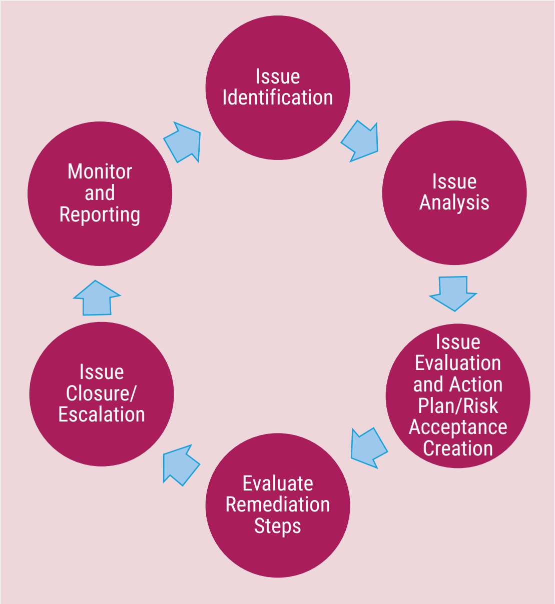
Third-Party Risk Management Stops With the Third Party

Risk management goes beyond third parties. Fourth (or nth) parties provide services to support the operations of third parties, which, in turn, provide services to the primary enterprise. Therefore, these fourth parties may be directly involved with the services delivered to the primary enterprise, exposing it to various risk factors.

Fourth parties or subcontractors may also have access to data owned by the primary enterprise, and any risk to these data while held by the fourth party remains the responsibility of the primary enterprise, from the perspective of both regulators and customers. Thus, the significance of fourth parties and the risk associated with them should be addressed by enterprises and regulators.

Interestingly, most enterprises overlook the risk associated with fourth parties because they rely on their contractual arrangements with third parties to manage fourth parties. Their primary focus continues to be oversight and monitoring of third parties.

Figure 4—Issue Management Process


Issue Identification
Issue Analysis
Issue Evaluation and Action Plan/Risk Acceptance Creation
Evaluate Remediation Steps
Issue Closure/ Escalation
Monitor and Reporting

Regulators, however, emphasize fourth-party management, encouraging primary enterprises to establish inventories of fourth parties and independently assess them, especially when the fourth party accesses, stores, processes, or hosts confidential or sensitive data.[5, 6]

A mature third-party risk management program should include provisions related to the fourth-party relationship commensurate with the fourth party's level of involvement.

> “ENTERPRISES SHOULD FOCUS ON IDENTIFYING LOOPHOLES IN THEIR CURRENT PROGRAMS AND IMPROVING THEIR MATURITY.”

Different Regulators Have Different Needs
Globally, there are many regulatory requirements related to outsourcing or third parties. Enterprises operating in multiple geographic locations must comply with multiple regulations. This can be a daunting task, and the consequences of failing to comply can be significant.

It might make sense to identify the common requirements and build an all-inclusive framework. In fact, it is fairly easy to extract the common trends in regulations, as they tend to follow a similar pattern. Regulatory requirements can be broadly divided into two types:

1. **Framework requirements**—Regulations mandate that certain components be included in the overall third-party risk management framework. These requirements tend to cover the full life cycle of the third-party arrangement from sourcing to termination.
2. **Risk requirements**—Regulations require that certain risk factors be addressed. For example, the US Federal Reserve requires a financial institution to focus on compliance, concentration and reputational risk when entering into and managing a third-party arrangement.

A mature third-party risk management program identifies and includes the set of common requirements contained in multiple regulations, and it keeps a constant watch for any new regulations that might be applicable.

Conclusion

A balanced and risk-driven approach to third-party risk management that continuously monitors and adjusts to the changing risk posture is vital today. Enterprises should focus on identifying loopholes in their current programs and improving their maturity.

Recent exposure incidents reiterate the need for a holistic third-party risk management framework and continuous improvements to ensure mature third-party risk management programs.

The following recommendations can greatly help improve the overall maturity of a third-party risk management program:

- Having a holistic third-party risk management program covering the entire third-party relationship life cycle
- Extending the third-party coverage to include various types of third parties
- Extending the risk domains to cover different types of risk that a third-party arrangement can bring to the enterprise
- Working on the assessment approach and tweaking it to make it commensurate to the risk a third-party arrangement brings to the table
- Ensuring all identified issues are taken to their logical conclusion
- Including fourth parties in the third-party risk management program
- Considering all common requirements from different regulations while developing the overall third-party risk management framework

Enjoying this article?

- Read *Managing Third Party Risk. www.isaca.org/managing-third-party-risk*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Endnotes

[1] Venminder, “State of Third Party Risk Management 2019,” *www.venminder.com*

[2] Aravo, “The Growing Need to Infuse Third-Party Risk Intelligence Into Your TPRM Program,” 5 June 2019, *https://www.aravo.com/blog/the-growing-need-to-infuse-third-party-risk-intelligence-into-your-tprm-program/*

[3] Board of Governors of the Federal Reserve, “Guidelines on Outsourcing Risk Management,” USA, 5 December 2013, *https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf*

[4] Pymnts, “Third-Party Data Breaches Rise to 61 Pct in US,” 15 November 2018, *https://www.pymnts.com/news/security-and-risk/2018/third-party-data-breaches-cybersecurity-risk/*

[5] Monetary Authority of Singapore (MAS), “Risk Management/Outsourcing Guidelines,” 5 October 2018, *https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf*

[6] *Op cit* Board of Governors of the Federal Reserve

Stay Connected to the World Around You

Without leaving home...

Start conversations, seek guidance and network with professionals across the globe through ISACA®’s Engage community.

www.isaca.org/EngageNow-jv3

ISACA®

Managing Technology Risk to Protect Privacy and Confidentiality

Enterprises must deal with a large and constantly growing volume of data, and they require the capacity to manipulate and process this information while protecting data sources. Key stakeholders such as clients, regulators, investors and the public are affected by how enterprises manage the risk related to collecting, storing and sharing information. For example, personally identifiable information (PII) such as name, email address and Internet Protocol (IP) address is expected to be protected in the context of its use, access, location and confidentiality.[1]

Enterprises must understand how to adopt a risk management process focused on both data protection and mitigation strategies to address security risk related to privacy and confidentiality.

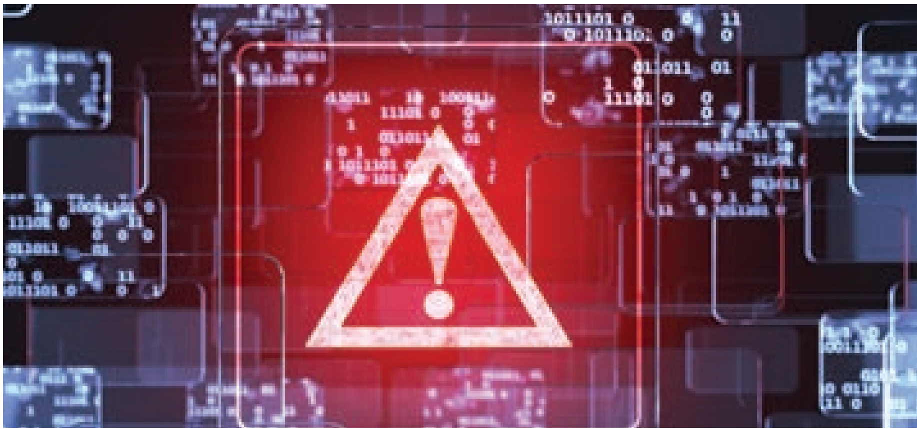
Privacy and Confidentiality

In recent years, privacy and confidentiality and their impact on enterprises have become relevant topics. Privacy can be understood as the freedom from intrusion into an individual's private life or affairs when that intrusion results from undue or illegal gathering and use of data about that individual.[2] Similarly, confidentiality aims to preserve authorized restrictions on information access and disclosure, including the means of protecting personal privacy and proprietary information and distinguishing authorized and unauthorized users through access levels.[3] In sum, there is an expectation that information in a trusted environment will not be disclosed and that security mechanisms will be implemented to make this information unusable by unintended parties or adversaries.

Risk Assessment and Mitigation

So why do enterprises need to invest in mechanisms for data protection and IT security? As Richard Clarke, cybersecurity special advisor to the US President, observed, "If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked."[4] Investments in technology are intended, among other objectives, to reduce the security risk related to privacy and confidentiality breaches. Enterprises need to align business objectives with risk and understand which threats need to be controlled. The results may be a better alignment of growth and risk, compliance with legal and regulatory requirements, and increased resilience.

A security risk assessment provides the basis for an enterprise to identify, protect against, detect, respond to and recover from security threats. This assessment can also be useful when prioritizing areas of investment. For instance, an enterprise with a centralized IT environment with only local staff has a different security risk profile than an enterprise with decentralized activities and a mobile workforce. A 2019 study conducted in Canada shows that Canadian enterprises are deploying more security layers to increase their protection,



Thiago de Oliveira Teodoro, CISA
Is a consultant in governance, risk and compliance (GRC). He has 10 years of professional experience in the areas of auditing and internal controls in both the public and private sectors.

> ENTERPRISES SHOULD UNDERSTAND THE LIKELIHOOD OF A SECURITY RISK AND ITS POTENTIAL IMPACT TO DETERMINE WHICH TECHNOLOGY SECURITY FEATURES ARE REQUIRED TO MAINTAIN OPERATIONS ON A CONTINUOUS BASIS.

including Domain Name System (DNS) firewalls (57 percent), password managers (51 percent), penetration testing (39 percent) and cybersecurity insurance (25 percent).[5] These results indicate that enterprises are considering several aspects of security. However, it is difficult to determine whether the implementation of these measures is aligned with risk-based strategies that ultimately protect privacy and confidentiality at critical endpoints or whether these measures are a reaction to the occurrence of security-related incidents. An enterprise can benchmark its security against the general industry, and it should be able to identify the measures that best fit its own security needs.

Enterprises should understand the likelihood of a security risk and its potential impact to determine which technology security features are required to maintain operations on a continuous basis. This can be achieved by understanding the common types of cybersecurity attack vectors that can deliver malware such as email, corrupted Internet traffic, stolen credentials and malicious code.[6] Organizations must also determine the level of risk they are willing to assume to achieve a desired result (risk tolerance).[7] For example, an enterprise may concentrate on addressing the risk of denial-of-service attack (e.g., web application firewall) but, because of budgetary constraints, may have only limited resources to defend against phishing attempts (e.g., predictive email security).

How can data security mitigate risk related to privacy and confidentiality? A risk mitigation plan involves recognizing how a single control or suite of controls can address multiple, related risk factors.[8] For instance, a risk mitigation plan to protect personal privacy and proprietary information relies on measures to protect data or prevent their further use if acquired by unauthorized parties. The mitigation plan can be considered an additional layer of security in a defense-in-depth strategy: If one control turns out to be inadequate or even fails, the additional layer prevents a more harmful outcome.

More specifically, data security to protect PII and proprietary information commonly uses the following methods:

- **Encryption**—The process of converting plaintext information to ciphertext using a cryptographic algorithm (e.g., Advanced Encryption Standard [AES]) and a password key
- **Anonymization (or de-identification)**—A process that removes the association between the identifying data set and the data subject[9]
- **Tokenization**—A technique that replaces the original value with a token value and in which centralized data tokenization stores both the data and the tokens, allowing the tokenizing and de-tokenizing of data

An illustration of this is a sample data set of four users whose first names, last names, zip codes, email accounts and credit card numbers have been collected in comma-separated values (.csv) files (**figure 1**). In this case, one can observe the results when encryption, anonymization and tokenization are applied (**figure 2**) to prevent an adversary from accessing these data.

Figure 1—Sample Data Set

Original Data

First_Name;Last_Name;Zip_Code;Email_Account;Credit_Card;
User1;Last1;11523;user1@hotmail.com;4555635915326950;
User2;Last2;10235;user2@yahoo.com;5236985123675980;
User3;Last3;16588;user3@gmail.com;4552326874523650;
User4;Last4;14323;user4@business.com;5489362598561580;

Approximately 80 countries worldwide have enacted policies and regulations regarding privacy and confidentiality, illustrating the importance of adopting a risk management strategy to protect the collection, storage and sharing of sensitive data.

Figure 2—Application of Data Security Measures

Technique	Description	Result
Encryption[*]	Use of AES-256 with Cipher Blocker Chaining (CBC) for all original data (ciphertext).	Salted__VËãBAêÍPÏˆÃ'"‡üOÅniDþG
Anonymization[**]	Secure Hash Algorithm (SHA)-256 Cryptographic Hash Algorithm was applied to the email account records only. To protect all the original data, this process would need to be repeated for the remaining fields with similar results (plaintext).	“612e41a6de3e37eba776ae87ee009d11c14110d31f31e9d687eae06b62580613” “f0ff7031943d99d1aee9f5e8560a448c0071319ce8e82f2e49e38916072f5cda” “278626d11fb466bfe6ad81bc0b75b147f1d8260e93c53d575d1aaeaac001c942” “3cb5aa0235e315a05f5cb70adfe8b6a102ec745491fa7958de661c2e23fdb088”
Tokenization[***]	The tokenization of all original data results in token objects that have been documented with the token type and additional information extracted from the token, such as credit card details associated with the number 5 (plaintext).	6,”First”,”” 17,”_”,”” 6,”Name”,”” 1,”;”,”;” 6,”Last”,”” 17,”_”,”” 6,”Name”,”” 1,”;”,”;” 6,”Zip”,”” 17,”_”,”” 6,”Code”,”” 1,”;”,”;” 6,”Email”,”” 17,”_”,”” 6,”Account”,”” 1,”;”,”;” 6,”Credit”,”” 17,”_”,”” 6,”Card”,”” 1,”;”,”;” 15,”User1;Last1;11523;user1@hotmail.com”,”” 1,”;”,”;” 5,”4555635915326950”,4555635915326950 1,”;”,”;” 15,”User2;Last2;10235;user2@yahoo.com”,”” 1,”;”,”;” 5,”5236985123675980”,5236985123675980 1,”;”,”;” 15,”User3;Last3;16588;user3@gmail.com”,”” 1,”;”,”;” 5,”4552326874523650”,4552326874523650 1,”;”,”;” 15,”User4;Last4;14323;user4@business.com”,”” 1,”;”,”;” 5,”5489362598561580”,5489362598561580 1,”;”,”;” 0,””,””

[*] Keller, J.; “Cryptr,” Github, *https://github.com/nodesocket/cryptr*

[**] Hendricks, P.; “Anonymizer,” Github, *https://github.com/paulhendricks/anonymizer*

[***] Porsteinsson, V.; “Tokenizer,” PyPI, *https://pypi.org/project/tokenizer/*

Enjoying this article?

- Read *Conducting an IT Security Risk Assessment. www.isaca.org/conducting-an-ITsecurity-risk-assessment*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums.

  https://engage.isaca.org/onlineforums

Understanding the principles of data classification, defining privileges and access controls at the time of data creation, and protecting the data-at-rest and data-in-transit environments are essential to meeting privacy and confidentiality requirements. Among the security methods discussed, encryption offers the highest level of data protection because it results in ciphertext—an unreadable mix of letters and symbols.[10] However, it is important to understand that each method has advantages and disadvantages under specific circumstances.

It is recommended that enterprises establish security risk assessment as a permanent process to ensure an understanding of the technological environment and to support the management of security vulnerabilities that could affect data privacy and confidentiality.

Get Noticed

Advertise in the ISACA® Journal

ISACA Journal

Endnotes

[1] McCallister, E.; T. Grance; K. Scarfone; “ Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” *Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology Special Publication (SP) 800-122, USA, April 2010, *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf*

[2] Garfinkel, S. L.; “De-Identification of Personal Information,” National Institute of Standards and Technology Internal Report (IR) 8053, USA, October 2015, *https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf*

[3] Joint Task Force Transformation Initiative, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations,” *Building Effective Assessment Plans*, National Institute of Standards and Technology Special Publication (SP) 800-53A, revision 4, USA, December 2014, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf*

[4] Lemos, R.; “Security Guru: Let's Secure the Net,” *ZD Net*, 19 February 2002, *https://www.zdnet.com/article/security-guru-lets-secure-the-net/*

[5] Canadian Internet Registration Authority (CIRA), “2019 CIRA Cybersecurity Survey,” *https://cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey*

[6] Rapid7, “Common Types of Cybersecurity Attacks,” *https://www.rapid7.com/fundamentals/types-of-attacks/*

[7] Kissel, R.; “Glossary of Key Information Security Terms,” National Institute of Standards and Technology Internal Report (IR) 7298, USA, 25 April 2006, *https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7298.pdf*

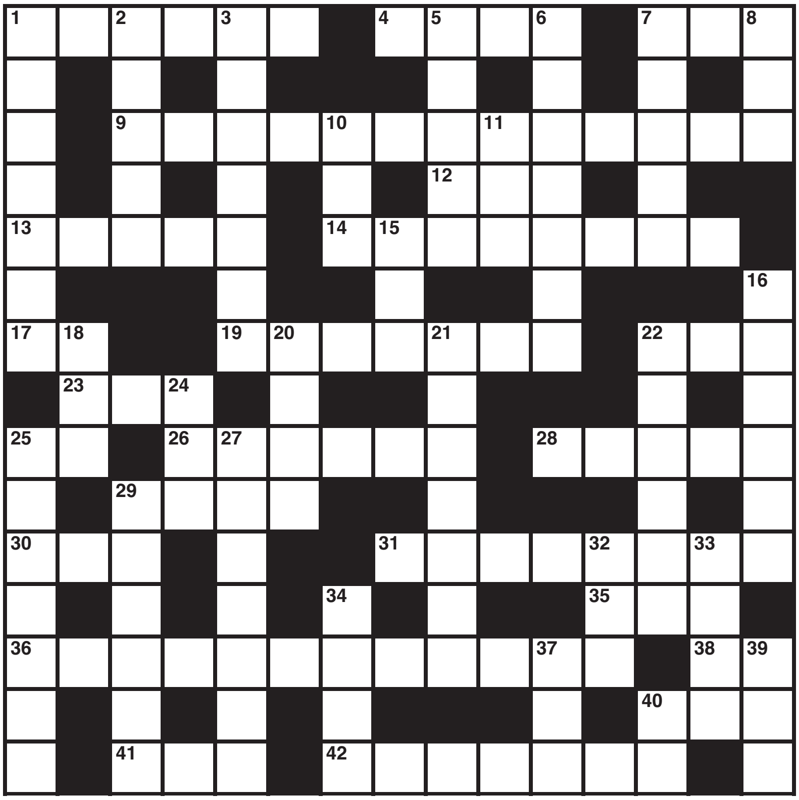
[8] Nicholson, F.; C. Baker; *Certification in Risk Management Assurance, 1st Edition*, Institute of Internal Auditors Research Foundation (IIARF), USA, 2013

[9] *Op cit* Garfinkel

[10] US Department of Health and Human Services, “Health Information Privacy,” *https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html*

CROSSWORD PUZZLE

By Myles Mellor
www.themecrosswords.com



ACROSS

1 AWS view security and compliance as a ____ responsibility between AWS and the customer

4 A key function of this role is cloud vendor selection

7 Get data secretly

9 Proposed privacy design practice which would minimize the risk of unauthorized use of personal data

12 Storage capacity measurement, abbr.

13 Easy to comprehend

14 What a futurist does, as best he or she can

17 Complete metric system of measurements for scientists

19 Results

22 Reduced, as a budget

23 Not quite right

25 Domain name, abbr.

26 Copy on a separate storage device

28 "To err is ___"

29 Section taken out of a whole

30 Watchdog's warning

31 Set up processes which run without human intervention

35 Bothered (with "at")

36 Key concern relating to data collection, how it's collected and how it is used

38 Branch of computer technology relating to writing programs that can then evolve their own knowledge and functions

40 Global currency org.

41 Tint

42 Author of The Mathematical Theory of Communication, Claude ____

DOWN

1 Causes

2 Microsoft's cloud service offering

3 Increase the size of

5 Reputation

6 Inceptions

7 Avoid

8 Shout of excitement

10 Little bite

11 Proposal in response to an RFP

15 Road map abbr.

16 Point of view

18 Tiny charged particle

20 Confront

21 Obtain information and transfer it to a storage device

22 Fight against

24 US crime solvers

25 Available electronically

27 Under debate, 2 words

29 Result of a successful cyberattack

32 Spring month

33 People working toward a common purpose

34 Part of Einstein's equation

37 Word of optimism

39. "No __, ands or buts"

40. Enclosed inside

Answers on page 58

CPE QUIZ #190

Take the quiz online.

https://bit.ly/2UBLKkp

Based on Volume 1, 2020—Technology on the Edge
Value—1 Hour of CISA/CRISC/CISM/CGEIT Continuing Professional Education (CPE) Credit

TRUE/FALSE

BLUM ARTICLE

1. Privileged access management (PAM) lacks the deep knowledge of roles, entitlements and identities needed to manage access via an automated, risk-based decision. Instead, this is in the identity governance and administration (IGA) component of identity and access management (IAM). Fortunately, PAM integration with IGA is both deep and wide.

2. IGA/PAM must support bringing DevOps under a risk-based identity governance model, matching relevant risk criteria before granting elevated, function-specific privileges to DevOps user accounts for sensitive applications.

KOHNKE ARTICLE

3. To date, no privacy risk factors have been identified for augmented reality (AR)/virtual reality (VR) technologies.

4. Physical risk associated with AR/VR includes immersion distraction and loss of spatial awareness, which must be managed by careful design of the spaces in which the AR/VR devices are used.

5. Logical and data security risk related to AR/VR technologies includes unapproved (including remote) activation and access. Appropriate controls for this risk include multifactor authentication, PIN entry and restrictions outlined in security policies.

WILLIAMS ARTICLE

6. Normalization and merging of data help ensure that processes are based on a comprehensive and accurate data set without blind spots.

7. Even with an offline model regularly updated via application programming interface (API) connections, security and operations teams must maintain administrative access to cloud platforms; performance of their processes is likely to disrupt the cloud deployment.

EFE ARTICLE

8. Qbit can enable an algorithm to generate random numbers, which can support generating data encryption keys, simulating and modeling complex phenomena, and selecting random samples from data sets.

9. Quantum computers will constitute a massive leap forward in a short time, necessitating specific transition activities, which already exist, to adopt the new technology.

10. As with any new technology, organizations seeking to implement quantum computing should identify business areas in which the technology can create strategic advantages and quantify the value of the new solutions.

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. Take the quiz online at *www.isaca.org/cpequiz*, where it is graded automatically. 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.

PEARCE ARTICLE

11. Digital transformation is only about technology; other considerations, such as the operating model, are tangential.

12. A survey of 1,988 business and technology executives revealed that inflexible/slow processes, technology integration and ineffective third-party partners were the top three barriers to executing a digital strategy.

13. Culture—often evidenced in user detachment, ambiguous communication and/or subverted processes—is a critical success factor in the IT risk management pillar of the enterprise governance of IT (EGIT).

WLOSINSKI ARTICLE

14. Compartmentalization calls for separating business and personal applications (apps) using technological techniques. This limits artificial intelligence (AI) programs' access to data, thus reducing the impact if attackers gain access to an app.

15. Data encryption and data masking are effective protective controls, but they do not protect data from exposure arising from AI searching, gathering, correlation and malicious usage.

16. AI can predict cyberattacks by reviewing data and detecting suspicious activity by clustering the data into meaningful patterns, without the need for human intervention or analysis.

AXELROD ARTICLE

17. Understanding how individuals/groups weigh motives, motivation, intent, risk and consequences against the value and benefits of committing crimes can help protect systems and data from attacks committed by attackers who are in league with victims and defenders.

18. Persons with privileged access should have regular background checks—preferably every three years, especially if they have experienced a substantial change in their role/responsibilities or in the systems/data available to them.

Answers: Crossword by Myles Mellor
See page 57 for the puzzle.

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

ISACA Member and Certification Holder Compliance

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

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

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

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

IS Audit and Assurance Standards

The standards are divided into three categories:

- General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

General

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

Performance

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

Reporting

1401	Reporting
1402	Follow-Up Activities

IS Audit and Assurance Guidelines

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

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

General

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

Performance

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

Reporting

2401	Reporting
2402	Follow-Up Activities

IS Audit and Assurance Tools and Techniques

These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programs, reference books and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf*.

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

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

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

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

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

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

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

© 2020 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC) (*www.copyright.com*), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1944-1967), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

ISSN 1944-1967

Subscription Rates:

US:
one year (6 issues) $85

All international orders:
one year (6 issues) $100

Remittance must be made in US funds.

https://bit.ly/2NzLpM3

ADVERTISERS/
WEBSITES

leaders and supporters

Editor

Jennifer Hajigeorgiou
publication@isaca.org

Managing Editor

Maurita Jasper

Assistant Editor

Safia Kazi

Contributing Editors

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Dustin Brewer, CSX-P, CCSP, CEH,CHFI
Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CIPM, CIPP/E, CPTE, DipFM, FIP, ITIL Foundation, Six Sigma Green Belt
K. Brian Kelly, CISA, CSPO, MCSE, Security+
Vasant Raval, DBA, CISA
Steven J. Ross, CISA, CBCP, CISSP

Advertising

media@isaca.org

Media Relations

news@isaca.org

Reviewers

Matt Altman, CISA, CRISC, CISM, CGEIT
Sanjiv Agarwala, CISA, CISM, CGEIT, CISSP, ITIL, MBCI
Vikrant Arora, CISM, CISSP
Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Brian Barnier, CRISC, CGEIT
Ronald Bas, CISSP
Pascal A. Bizarro, CISA
Joyce Chua, CISA, CISM, PMP, ITILv3
Ashwin K. Chaudary, CISA, CRISC, CISM, CGEIT
Ken Doughty, CISA, CRISC, CBCP
Nikesh L. Dubey, CISA, CRISC, CISM, CISSP
Robert Findlay
Jack Freund, Ph.D., CISA, CRISC, CISM, CIPP, CISSP, PMP
Sailesh Gadia, CISA
Durgesh Gaitonde, CISM, CRISC, COBIT 5 Foundation, CEng, CIPM
Robin Generous, CISA, CPA
Tushar Gokhale, CISA, CISM, CISSP, ISO 27001 LA
Miguel Angel Gonzalez, CISA, ISO 27032 Lead Cybersecurity Manager, ITIL v3
Tanja Grivicic
Manish Gupta, Ph.D., CISA, CRISC, CISM, CISSP
Jeffrey Hare, CISA, CPA, CIA
Sherry G. Holland
Jocelyn Howard, CISA, CISMP, CISSP
Khawaja Faisal Javed, CISA, CRISC, CBCP, ISMS LA
Mohammed J. Khan, CISA, CRISC, CIPM
Abbas Kudrati, CISA, CISM, CGEIT, COBIT 5 Foundation, CBE, CCEH, CCISO, CCNA, CCSK, CHFI, EDRP, ISO 27001 LA, ITIL Foundation, MCSE+, Microsoft Certified Azure Fundamentals, PRINCE2, SABSA Foundation, TOGAF CEA
Shruti Kulkarni, CISA, CRISC, CCSK, ITIL
Bhanu Kumar
Hiu Sing (Vincent) Lam, CISA, CPIT(BA), ITIL, PMP
Edward A. Lane, CISA, CCP, PMP
Romulo Lomparte, CISA, CRISC, CISM, CGEIT, COBIT 5 Foundation, CRMA, IATCA, IRCA, ISO 27002, PMP
Larry Marks, CISA, CRISC, CGEIT
Luis Martinez
Tamer Marzouk, CISA, ABCP, CBAP
Brian McSweeney
Irina Medvinskaya, CISM, CGEIT, FINRA, Series 99
Rubal Mehta
David Earl Mills, CISA, CRISC, CGEIT, MCSE
David Moffatt, CISA, PCI-P
Donald Morgan, CISA
Eswar Muthukrishnan, CISA, ITIL Manager, Six Sigma
Jonathan Neel, CISA
Jacky Y. K. Ng, CISM, COBIT Assessor, AgilePM, CEng, CMgr, FCMI, ISO 9001 and ISO/IEC 27001 LA, ITIL Expert, MHKIE, MIET, PRINCE2, RPE
Nnamdi Nwosu, CISA, CRISC, CISM, CGEIT, PfMP, PMP
Ganiyu Babatunde Oladimeji, CISA, CRISC, CISM
Daniel Olaniran, CISA, CRISC, CISM, PMP
Anas Olateju Oyewole, CISA, CRISC, CISM, CISSP, CSOE, ITIL
Daniel Paula, CISA, CRISC, CISSP, PMP
Pak Lok Poon, Ph.D., CISA, CSQA, MIEEE
John Pouey, CISA, CRISC, CISM, CIA
Parvathi Ramesh, CISA, CA
Ron Roy, CISA, CRP
Louisa Saunier, CISSP, PMP, Six Sigma Green Belt
Abdulmajid Suleman, CISA, CISM, CGEIT, COBIT Foundation, CISSP, ISO 27001 LA, ITIL, MCSE, PMP
Nancy Thompson, CISA, CISM, CGEIT, PMP
Smita Totade, Ph.D., CISA, CRISC, CISM, CGEIT
Satyajit Turumella
Sadir Vanderloot Sr., CISA, CISM, CCNA, CCSA, NCSA
Rajat Ravinder Varuni, CEH, DOP, DVA, GPEN, SAA, SAP, SCS, SOA
Juan Gantiva Vergara
Varun Vohra, CISA, CISM
Manoj Wadhwa, CISA, CISM, CISSP, ISO 27000, SABSA
Kevin Wegryn, PMP, Security+, PfMP
Tashi Williamson
Ellis Wong, CISA, CRISC, CFE, CISSP

ISACA Board of Directors (2019-2020)

Chair
Brennan P. Baybeck, CISA, CRISC, CISM, CISSP

Vice-Chair
Rolf von Roessing, CISA, CISM, CGEIT, CISSP, FBCI

Director
Tracey Dedrick

Director
Pam Nigro, CISA, CRISC, CGEIT, CRMA

Director
R. V. Raghu, CISA, CRISC

Director
Gabriela Reynaga, CISA, CRISC, COBIT 5 Foundation, GRCP

Director
Gregory Touhill, CISM, CISSP, Brigadier General United States Air Force (ret.)

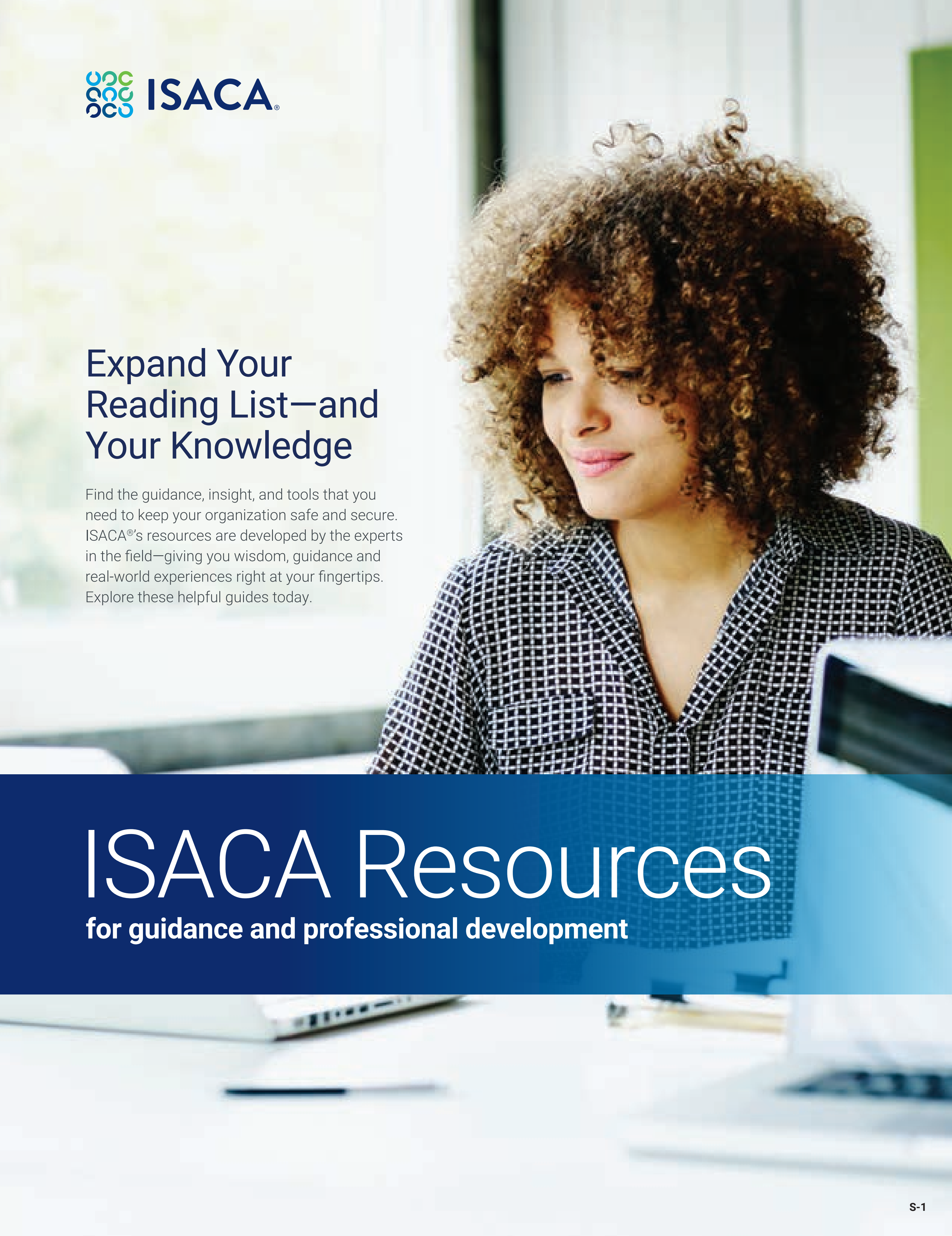
Director
Asaf Weisberg, CISA, CRISC, CISM, CGEIT

Director and Chief Executive Officer
David Samuelson

Director and ISACA Board Chair 2018-2019
Rob Clyde, CISM

Director and ISACA Board Chair 2015-2017
Chris Dimitriadis, Ph.D., CISA, CRISC, CISM

Director and ISACA Board Chair 2012-2013
Greg Grocholski, CISA



ISACA

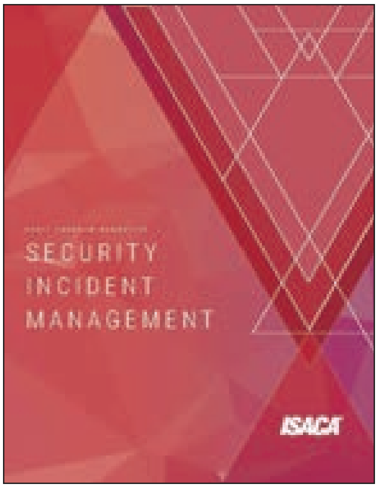
Expand Your Reading List—and Your Knowledge

Find the guidance, insight, and tools that you need to keep your organization safe and secure. ISACA®'s resources are developed by the experts in the field—giving you wisdom, guidance and real-world experiences right at your fingertips. Explore these helpful guides today.

ISACA Resources

for guidance and professional development

FEATURED RESOUCES



Security Incident Management Audit Program

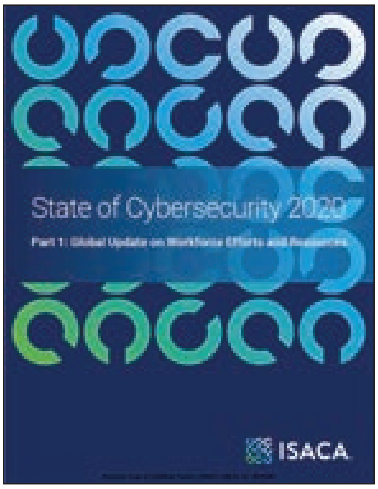
Web Download Product Code: WAPIM2 | Member: $25 | Non-member: $49

Unplanned incident preparation for many enterprises includes business continuity programs, disaster recovery plans and information security strategies. While looking at some of the same elements as these incident preparation tactics—namely the security triad of confidentiality, integrity, and availability—security incident management differs in that it poises enterprises for the identification and analysis of threats or incidents. In the current landscape, the combined focus on security incidents from both regulatory and operational perspectives put enterprises in positions where the effectiveness of their Security Incident Management programs is not optional.

To assist IT auditors as they assess the effectiveness of security incident management programs, ISACA has created a *Security Incident Management Audit Program*. The audit objective is to provide management with an independent assessment relating to the effectiveness of security incident management governance and operational procedures. Specifically, the audit program takes into consideration assurance around:

- Program design and implementation, from information security management, awareness and training, to insurance and third-party due diligence.
- Tools and technologies, inclusive of software and server and workstation configuration.
- Reporting best practices, giving consideration to the balance of incident details and potentially sensitive information.
- Lessons learned, ensuring protocols that include input from all stakeholders.

In addition to the operational areas above, the audit program also provides testing of applicable legal and regulatory compliance requirements related to security incidents.



State of Cybersecurity 2020
Part 1: Global Update on Workforce Efforts and Resources
ISACA

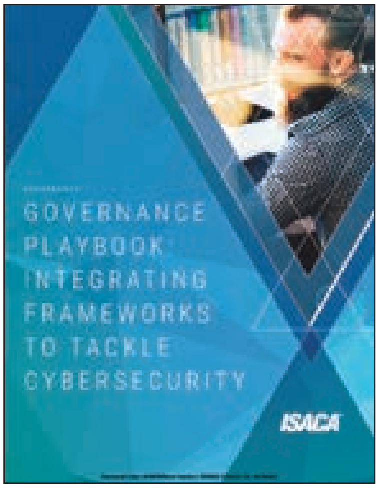
State of Cybersecurity 2020, Part 1: Global Update on Workforce Efforts and Resources

White Paper Product Code: WHPSC201 | Member/Non-member: FREE

State of Cybersecurity 2020 reports the results of the annual ISACA global State of Cybersecurity Survey, conducted in the fourth quarter of 2019.

This is the first report based on the survey, which focuses on the current trends in cybersecurity workforce development, staffing, budget and gender diversity. The survey findings are similar to past findings in which respondents indicated they are short-staffed, have difficulty finding sufficient talent for open positions and cybersecurity budgets are expected to grow.

This year's survey also finds that slight progress was made towards increasing the number of women in cybersecurity work roles, and also finds that almost half of all enterprises have specific diversity programs in place.


GOVERNANCE PLAYBOOK: INTEGRATING FRAMEWORKS TO TACKLE CYBERSECURITY
ISACA

Governance Playbook: Integrating Frameworks to Tackle Cybersecurity

White Paper Product Code: WHPGPIF | Member/Non-member: FREE

Get a head start on implementing NIST's CSF in your enterprise using ISACA's COBIT® 2019. Download ISACA's white paper: *Governance Playbook: Integrating Frameworks to Tackle Cybersecurity.*

No enterprise—regardless of its industry, type, size, or geographic location—is exempt from cyberthreats. As the need to move information in today's economy is vital to success, we have to recognize that cybersecurity is no longer simply an IT issue and consider it in the larger picture of enterprise governance. Leaders should ensure that their enterprise develops or adopts and implements a cybersecurity/risk framework. The cybersecurity framework (CSF) created by the National Institute of Standards and Technology (NIST) is globally recognized as just such a framework.

Since no two enterprises are the same, implementing the NIST CSF in isolation can be challenging. Applying that same CSF in harmony with COBIT 2019 as a comprehensive information and technology (I&T) governance and management framework approach can be a valuable combination.

The NIST CSF pairs well with COBIT 2019 because COBIT 2019:

- Employs a principles-based structure.
- Provides a holistic approach.
- Has a phased, iterative implementation methodology.
- Is an informative reference for NIST CSF as it includes an assessment program based on industry standards.

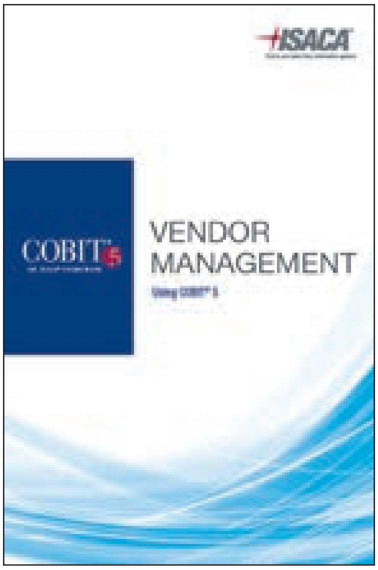
This white paper outlines a game plan for implementing the NIST Cybersecurity Framework using COBIT 2019, which in turn will reduce enterprise cybersecurity risk and more.

CSX Cybersecurity Fundamentals Study Guide, 2nd Edition

eBook Product Code: EPUB_CSXG2 | Member Price: $60 | Non-member Price: $65
Web Download Product Code: WCSXG2 | Member price: $50 | Non-member price: $55

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 cybersecurity concepts, such as ransomware, policies and cybersecurity 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, big data, artificial intelligence and social media.



Vendor Management: Using COBIT 5

Print Product Code: CB5VM | Member Price: $35 | Non-member Price: $70
Web Download Product Code: WCB5VM | Member price: $25 | Non-member price: $60

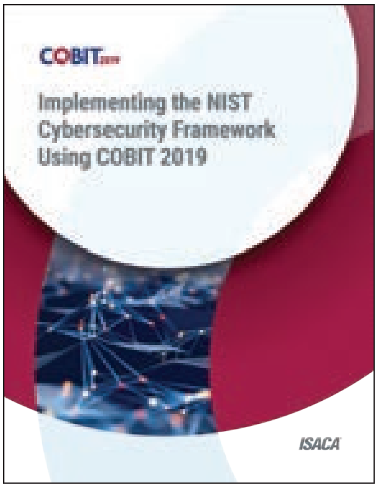
Vendors constitute an important part of an enterprise's external environment. The increased use of outsourcing and cloud computing implies that vendors are taking on an increasingly fundamental role in the operations of an enterprise.

As the scope, scale and complexity of vendor relationships and services increase, the risk related to them and the importance of effective vendor management increase proportionately. Managing external vendors should be a key competency for every enterprise and can lead to optimally mitigated risk and significant benefits.

This publication describes the vendor management process and its activities and then presents the most common threats, risk and mitigation actions. A detailed case study is provided to show the potential consequences of faulty vendor management. Practical sample templates and checklists are also provided to help during implementation of the concepts presented in this publication.

Who should use this guide? The vendor management process involves many stakeholder functions within the enterprise, including:

- The legal function (validate contracts).
- The compliance, legal and audit functions (consulted during the review of service agreements).
- The risk function (analyzes vendor-related risk).
- The board (budget approvals).
- The procurement function (oversees the overall selection and management process).



Implementing the NIST Cybersecurity Framework Using COBIT 2019

Print Product Code: CB19NIST | Member Price: $35 | Non-member Price: $65
Web Download Product Code: WCB5NIST | Member price: $25 | Non-member price: $60

Many enterprises lack an approach to integrate cybersecurity standards and enterprise governance of Information & Technology (EGIT). This lack of approach leaves them unable to establish systematic—yet flexible and achievable—governance and management objectives, processes, and capability levels to make measured improvements toward cybersecurity goals.

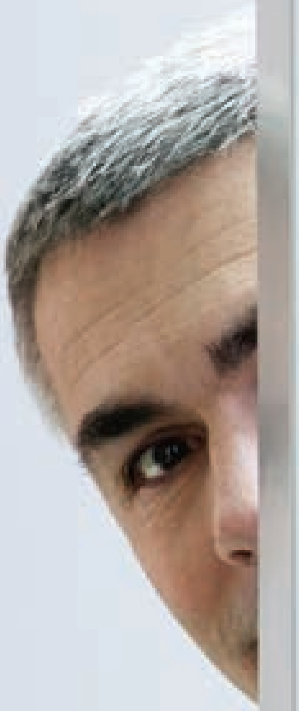
Created to support critical infrastructure, the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) continues to evolve based on feedback from diverse stakeholders and use cases. Today, the NIST CSF is a useful guide to help any enterprise address its cyberrisk.

Explore proven practices to anticipate, understand and optimize I&T risk by implementing the NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1 using COBIT 2019. Features include:

- NIST CSF Implementation.
- Correlating CSF guidance with measurable governance and management practices.
- Mapping of CSF steps and activities to COBIT 2019.
- Appendices for quick reference and further considerations.

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®



Stop Hiding Your Technical Privacy Expertise

Let everyone know you're a privacy pro with CDPSE, ISACA®'s newest certification. Confirm you have the technical skills and knowledge it takes to assess, build and implement a comprehensive privacy solution.

www.isaca.org/CDPSE-jv3

CDPSE™ Certified Data Privacy Solutions Engineer™
An ISACA® Certification

ISACA®

Transform Perspectives

with ISACA's CGEIT Certification

Be the game-changer for elevating IT from cost center to the greatest value creator. Leverage ISACA®'s **Certified in the Governance of Enterprise IT® (CGEIT®)** certification to transform business competitiveness—and the way your organization sees you.

CGEIT Job Practice Change Coming Soon! The last day to take the current exam is June 28. The new exam goes into effect on July 2, 2020. Register today at **www.isaca.org/NewCGEIT-jv3**

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