VOLUME 5, 2020

ISACA Journal

THE ALWAYS-ON CONTINUUM

THE DARK SIDE OF ROBOTIC PROCESS AUTOMATION

BUILDING A CULTURE OF SECURITY

PANDEMIC-DRIVEN REMOTE WORKING AND RISK MANAGEMENT STRATEGIES

ISACA.ORG

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 September and October.

Auditing the Cloud: Microsoft Azure
Adam Kohnke, CISA, CISSP, eJPT

Common Sense Authentication
Paul C. Schauer, Ph.D.

Next-Generation Security Intelligence
Louisa Saunier, CISA, CISM, CISSP, PMP, and Kemal A. Delic

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

Lessons for the IT Community From the Pandemic

As I write this piece in June 2020, the world has been facing the COVID-19 outbreak for nearly seven months. Millions have been infected; hundreds of thousands have died.[1] Millions more people have lost their livelihoods, at least in the short term. In discussing the successes of information technology in ameliorating the impact of the disease on society at large, we must never let those statistics be far from front-of-mind.

With a little distance now from the onset of the pandemic, there are a number of trends made more obvious by the IT community's response to this pandemic. We need to absorb the lessons learned to be prepared for a recurrence of this global disaster or the arrival of another one.

Work From Home

Perhaps the most important trend has been the shift in the way many people work.

Information technology has enabled a semblance of normal operations during the pandemic[2] by eliminating the necessity for people to travel to their offices[3] and work in close proximity. They do their jobs in their homes, made possible by portable computers, cell phones, virtual private networks (VPNs), high-speed connection to the Internet and, of course, the Internet itself. Indeed the acronym "WFH," or work from home, has entered the popular vocabulary.[4]

It seems obvious in retrospect; of course people would distance themselves from others and work remotely. But it was not obvious in prospect.[5] It is not so many years ago that the technologies that have enabled WFH either did not exist or were not so widely utilized that we could rely on them. For example, although Zoom Video Communications was founded in 2011,[6] it feels as though Zoom exploded on the Internet for every businessperson and student just in time for the pandemic. When was it that everyone had a personal computer, a cell phone and WiFi? Or does everyone have them, even now?

At Home at Work

As working from home has changed the nature of work, so it has also changed the nature of home. It may be someone's castle, but for many, home was never designed to be their workplace. Perhaps those who have a suburban house, with a room set aside to be an office, have sufficient space for an at-home office. The residents might work at the kitchen table or they may have a desk, a high-speed Internet connection, a printer and a storage area for paper files (remember paper files?). But urban folks living in a one-bedroom apartment, with Internet connectivity designed for games and movies, find it more difficult. And, if that bedroom is shared with a significant other? Is the apartment sizable enough to allow two people to work both productively and amicably?

The IT community needs to be cognizant of the realities of those people who are not equipped for residential toil in the age of WFH. There is quite a bit of evidence that working at home may outlast the pandemic. Some have given precedence to

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.

equipping their homes for child rearing, not the daily nine-to-five (remember nine-to-five?). Others have just graduated and joined the workforce. Still more—too many more—simply do not earn enough to afford a suitable office in their homes. The IT community cannot in conscience simply assume that the cost of working from home will be borne by the workers.

> “THE IT COMMUNITY CANNOT IN CONSCIENCE SIMPLY ASSUME THAT THE COST OF WORKING FROM HOME WILL BE BORNE BY THE WORKERS.”

The Internet and the Data Center

The Internet was designed not to break,[7] and it did not. But it did bend. Speeds got slower; connections became less reliable, and faces and voices disappeared from online meetings. Sometimes, those working from home lost access to the Internet altogether because, though the Internet itself does not fail, the last mile from the Internet service provider (ISP) to the home sometimes does. If WFH is to become the contingency plan for pandemics and other serious disruptions, then the IT community must consider end-to-end connectivity so that workers can maintain productivity. It is not enough to keep the enterprise's data center up and running; users must be able to reach it and use it reliably over time.

Notably, the pandemic has emphasized several trends that were ongoing well before COVID-19 had ever been encountered. Those who operate organizations' data centers and keep their infrastructures running have no need to be physically near the systems they support. So during lockdowns, the techs work at home, too. Instead of being down the hall from the data center, they are across town or even further away.

Nonetheless, there is always a need for so-called "touch labor." A circuit pack has to be replaced, a power blip investigated, a switch flipped. Before the pandemic, I had not heard of this need as a rationale for movement of systems to the cloud. But the value of having a faraway staff available for these sorts of tasks became much more apparent.[8] In these disastrous times, public cloud providers have already made the hurried travel to a disaster recovery (DR) site unnecessary for many.[9] In the difficult days we are living through, the IT community should focus on accelerating the trend toward migration to the cloud.

Cybersecurity in the Pandemic

Since this is the Information Security Matters column, I should note that as I see it, cybersecurity seems to be effective through the pandemic. Or more properly, *serious* cyberattacks seem no worse than before,10 faint comfort indeed. Before COVID-19, there were more than enough reasons to fear that there would be a significant increase in cyberattacks.11 With everyone working remotely, the guardrails provided by the employers' workplaces (whatever they were) have been taken away.

Why, then, hasn't the incidence of cyberattacks exploded? A few thoughts: For those using VPNs, the threat of an attack is no greater than if they were on an ethernet connection in an office building. Maybe attackers can target central enterprisewide systems more easily than lots of individual personal computers. Perhaps there is more end-point protection installed than we realize. Or it just might be that the bad guys are as frightened of COVID-19 as we are and are taking time off. Whatever the case, we cannot be confident that the relative calm will continue.

The IT Community

Throughout this article I have referred to the "IT community." Who exactly am I talking about? In general, I mean anyone who makes a living in developing, implementing, operating or controlling applications and infrastructure. That is a lot of people, to be sure, and it is difficult to prescribe how any group that large should think, much less act. And yet, we who have made information technology such an intrinsic part of the world we live in owe it to ourselves and our fellow citizens to begin the conversation about IT during and (we dearly hope) after the pandemic.

At the risk of sounding too rah-rah for the home team (remember home teams?), I would like to suggest that ISACA® and everything/everyone it represents is the proper forum for that conversation. Let us all raise it in our publications, training, chapter meetings and research. Then, bring the rest of the world into the discussion.

Endnotes

1 Coronavirus Research Center, COVID-19 Case Tracker, Johns Hopkins University, Baltimore, Maryland, USA, *https://coronavirus.jhu.edu/*

2 I should temper my statement a bit. I bring to this discussion the perspective of a US citizen who lives in New York City, which, for a time, was the global epicenter of the outbreak. There may well be other locations with greater disruption and less capacity for information technology to reduce the impact.

3 Note that those whose jobs require them to work in places other than offices were not so fortunate. I am not sure if information technology could change the lot of waiters, gardeners and taxidermists, but an IT community that has made the world safe for cute kitty pictures must have some ingenuity to spare to improve the lives of factory, meat processing and transportation workers.

4 If a pop culture term has reached the *Harvard Business Review*, then everyone must be using it. Giurge, L. M.; V. K. Bohns; "Three Tips to Avoid WFH Burnout," *Harvard Business Review*, 3 April 2020, *https://hbr.org/2020/04/3-tips-to-avoid-wfh-burnout*

5 To cite one example among hundreds: Alba, D.; C. Kang; "So We're Working From Home. Can the Internet Handle It?" *The New YorkTimes*, 16 March 2020, *https://www.nytimes.com/2020/03/16/technology/coronavirus-working-from-home-internet.html*

6 US Securities and Exchange Commission, Zoom Video Communications, Inc., registration, *https://www.sec.gov/Archives/edgar/data/1585521/000119312519107178/d642624ds1a.htm*

7 Fishman, C.; "The System That Actually Worked," *The Atlantic*, 6 May 2020, *https://www.theatlantic.com/ideas/archive/2020/05/miracle-internet-not-breaking/611212/*. This is an excellent, nontechnical overview of the way the Internet has been operated during the pandemic.

8 Miller, R.; "In Spite of Pandemic (or Maybe Because of It), Cloud Infrastructure Revenue Soars," *TechCrunch*, 1 May 2020, *https://techcrunch.com/2020/05/01/in-spite-of-pandemic-or-maybe-because-of-it-cloud-infrastructure-revenue-soars/*

9 Ross, S.; "Do You Need a Disaster Recovery Plan,?" *ISACA® Journal*, vol. 2, 2017, *https://www.isaca.org/archives*

10 Center for Strategic and International Studies, Significant Cyber Incidents, *https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents*, undated but incidents from May 2020 are listed. Unsurprisingly depressing reading. See *inter alia*.

11 Mooney, G.; "The Cybersecurity Risks of Remote Employees Working From Home," Progress, 17 March 2020, *https://blog.ipswitch.com/the-cybersecurity-risks-of-remote-employees-working-from-home*

Enjoying this article?

- Read *Privacy: Beyond Compliance*. *www.isaca.org/privacy_beyond_compliance_2020/*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

IS AUDIT
BASICS

Defining Targets for Continuous IT Auditing Using COBIT 2019

I have previously discussed sitting and passing my Certified Information Systems Auditor® (CISA®) exam back in 2005.[1] I tend to remember that one of the hot topics at that time was continuous online auditing. The approach allowed IT auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.[2] However, the focus then was very much on auditing the transactional data from applications. One of the key perceived benefits was the change from periodic reviews of a sample of transactions to ongoing audit testing of 100 percent of transactions.[3]

Although some practitioners had adopted continuous auditing for IT audit purposes,[4, 5] it took the second edition of the Institute of Internal Auditor's *Global Technology Audit Guide (GTAG) 3: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition* to popularize a focus expansion to include not only transactional data, but also other data sources such as security levels, logging, incidents, unstructured data, and changes to IT configurations, application controls, and segregation of duty (SoD) controls.[6] So what is continuous auditing and how can it be used by auditors to audit IT processes?

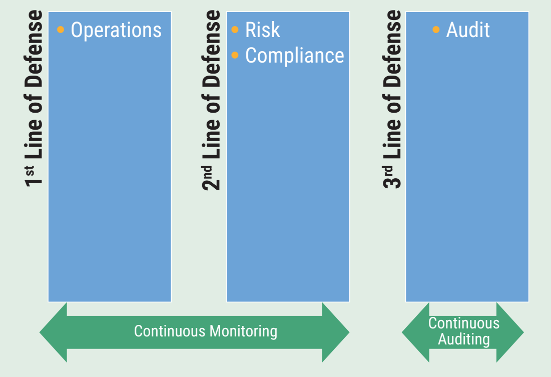
Ian Cooke, CISA, CRISC, CGEIT, COBIT 5 Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, FIP, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt

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 both ISACA's CISA® and CRISC™ Online Review Course. 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.

Defining Continuous Auditing

Continuous auditing is not the same as continuous monitoring. There may very well be instances (e.g., in different enterprises) where both are performing the same function and utilizing the same underlying code, but the key difference is the owner of the process. Continuous monitoring is a management process that monitors whether internal controls are operating effectively on an ongoing basis.[7] In other words, it is performed by the first or second line. Continuous auditing is performed by audit and is designed to enable the internal auditor to report on subject matter within a much shorter time frame than under the traditional retrospective approach (**figure 1**).[8]

Figure 1—Continuous Monitoring vs. Continuous Auditing



Continuous auditing is achieved through ongoing risk and control assessments enabled by technology-based audit techniques such as generalized audit software, spreadsheet software or scripts developed using audit-specific software, specialized audit utilities, computer-aided audit tools (CAATs), commercially packaged solutions and custom-developed production systems.[9] In short, continuous auditing is about using technology to measure and report on risk indicators.

> “THE KEY TO IDENTIFYING THE USEFUL METRICS IS TO ASCERTAIN WHETHER THERE ARE TWO OR MORE SOURCES OF INFORMATION THAT CAN BE CLASHED TO PRODUCE RELIABLE FIGURES.”

Identifying Risk Indicators

A risk indicator is a metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.[10] Identification of quality risk indicators is, therefore, critical to performing continuous auditing over IT processes.

In COBIT®, a management objective always relates to one process (with an identical or similar name) and a series of related components of other types to help achieve the objective.[11] These processes are, in turn, broken down into management practices, each of which has defined sample metrics (**figures 2, 3** and **4**).

I am proposing that many of these metrics can be used as risk indicators for continuous IT auditing purposes. The key to identifying the useful metrics is to ascertain whether there are two or more sources of information that can be clashed to produce reliable figures.

For our first example, to measure the number of emergency changes not authorized after the incident, this might involve, for instance, clashing the data from a release management application with the data from a change management application. Having a common identifier between these applications is key.

For our second example, to measure the average downtime per critical asset, clashing the data from the asset register with the data from an incident management system would produce the desired result, most likely matching the asset ID.

For our third example, to measure the average time between change and update of accounts might involve, for instance, clashing the data from a service desk application with data from, say, the

Figure 2—Sample COBIT Management Practice 1

Management Practice	Example Information Security-Specific Metrics
BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimize further incidents. Ensure the emergency change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorized after the change.	a. Number of emergency changes not authorized after the incident b. Percent of total changes that are emergency fixes

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018

Figure 3—Sample COBIT Management Practice 2

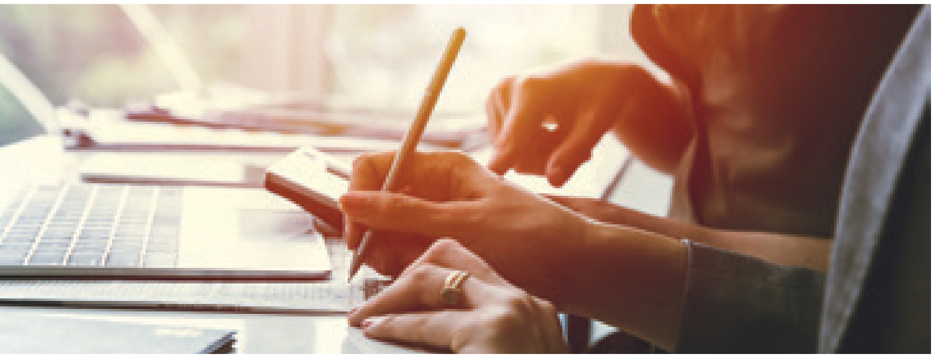
Management Practice	Example Information Security-Specific Metrics
BAI09.02 Manage critical assets. Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs.	a. Number of critical assets b. Average downtime per critical asset c. Number of incident trends identified

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018

Figure 4—Sample COBIT Management Practice 3

Management Practice	Example Information Security-Specific Metrics
DSS05.04 Manage user identity and logical access. Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.	a. Average time between change and update of accounts b. Number of accounts (vs. number of authorized users/staff) c. Number of incidents relating to unauthorized access to information

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018



Microsoft Active Directory (AD). Again, having a common identifier, likely the user ID, is key.

Further, many of the COBIT-defined metrics may be key risk indicators (KRIs), a subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk[12] or, where risk is not measured, key performance indicators (KPIs), a measure that determines how well the process is performing in enabling the goal to be reached in the enterprise under review. These will also add value to any continuous audit program.

In addition, ongoing control assessments need not run in real time. The frequency of analysis should be determined by the level of risk, the business process cycle and the degree to which management is monitoring the controls.[13]

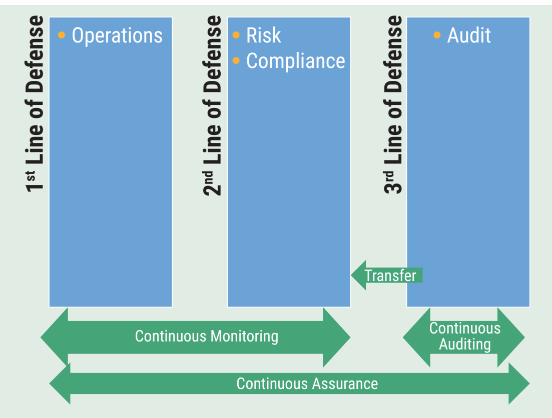
Improving the Control Environment

When a continuous auditing program is working well for a period of time, it may be possible to transfer the workload from audit to management. In this case, continuous auditing becomes continuous monitoring. Audit will now provide continuous assurance, a combination of continuous auditing and testing of first and second lines of defense continuous monitoring (**figure 5**).[14] In this manner, audit can focus on new metrics, which, in turn, can be transferred to management, continuously improving the control environment.

Conclusion

Audit is always under pressure to prove its value to the business. This can be achieved in the first instance by identifying, measuring and reporting upon risk indicators. Further value can be added by transferring these newly defined controls to the first and second lines while developing new metrics. Finally, where these risk indicators relate to management practices and, in turn, management objectives, an audit's value can be demonstrated clearly.

Figure 5—Continuous Assurance



Endnotes

1 Cooke, I.; "Backup and Recovery," *ISACA® Journal,* vol. 1, 2018, *https://www.isaca.org/archives*
2 ISACA®, *CISA Review Manual 2005*, USA, 2004
3 The Institute of Internal Auditors (IIA), *Global Technology Audit Guide (GTAG) 3, Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, USA, 2005
4 Cooke, I.; "Auditing Oracle Databases Using CAATs," *ISACA Journal,* vol. 2, 2014
5 Cooke, I.; "Auditing SQL Server Databases Using CAATs," *ISACA Journal,* vol. 1, 2015, *https://www.isaca.org/archives*
6 The Institute of Internal Auditors (IIA), *Global Technology Audit Guide (GTAG) 3, Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition*, USA, 2015, *https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG3.aspx*
7 *Ibid.*
8 *Ibid.*
9 *Ibid.*
10 ISACA Glossary, "Risk Indicator," *https://www.isaca.org/resources/glossary*
11 ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*
12 ISACA Glossary, "Key Risk Indicator," *https://www.isaca.org/resources/glossary*
13 *Op cit* IIA, 2015
14 *Ibid.*

Why the Bleeding Edge Is So Bloody

Those of us who have been in this industry for a while have seen amazing accomplishments and growth within the technology sector. We have also seen security breaches happen, usually paired with quick knee-jerk reactions and a “slap-a-Band-Aid-on-it” mentality as a response. We read about a data breach that was caused by unpatched software, review our own patching policies, append them if needed, and move on to the next issue and repeat this process. We constantly teeter between secure computing and just plain old computing, depending on whether the security part is convenient or within budget.

The Spine

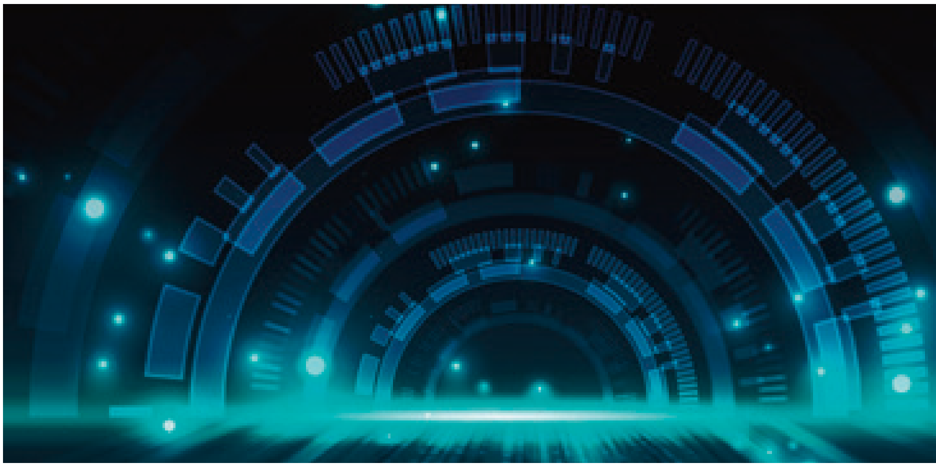
To me, one of the most fascinating vulnerabilities out there is the buffer overflow attack. This attack is executed by taking a vulnerability in software, breaking it and attempting to make the processor run code that was never intended to be there in the first place by overwriting memory. There is an elegance to this epic ballet of hardware and software variables that have to be in perfect alignment for these amazingly intricate exploits to work. I was curious as to the first time this exploit was used and I found a white paper titled *Computer Security Technology Planning Study, Volume II*,[1] published in 1972.

The paper not only theorized about the possibility of buffer overflow attacks, but also postulated theories on access controls, data integrity and physical device security. Many of these original thoughts are still used in security to this day, and it is a fascinating read, mostly because it was written 48 years ago and the ideas still ring true. For example, the most recent published buffer overflow attack was identified in January of this year (as of this writing).[2]

The Blade

Since 1972, we have made leaps and bounds in processing speed, communications, storage capacity and many more aspects of computing, but it was a bit surprising to learn that we have known about the possibility of this exploit for almost 50 years and we still continue to have the same problem. Buffer overflows are, of course, just one example; however, we find the same types of attacks (e.g., social engineering, unauthorized hardware, programming issues) are used over and over again to gain unauthorized access. Trends in attack vectors change to match what is working at the time.

According to ISACA’s *State of Cybersecurity 2019, Part 2: Current Trend in Attacks, Awareness and Governance*, the top three attack types are phishing, malware and social engineering.[3] The first known mention of a phishing attack can be traced back as far as 1996.[4] It can be argued that malware has been around since software was introduced, but the first rumblings of such a concept were around the 1970s.[5] Attempting to find the first social engineering attack is almost impossible because since humans have been able to communicate, there are those who have clandestinely tried to get more information from someone than that individual wanted to give. The same attacks that have worked for decades are still working. What are we missing?



Dustin Brewer, CISM, CSX-P, CDPSE, CEH
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.

Enjoying this article?

- Read *State of Cybersecurity 2020 Part 2: Threat Landscape and Security Practices. www.isaca.org/state-of-cybersecurity-2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The Tip

One of the best predictors of future human behavior is past behavior. Technology behavior and trends seem to have no immunity to this adage. Current trends continue to see more data breeches and cyberattacks every year, with a growing technology skills gap. As consumers, we not only want our technology to work flawlessly but also to have innovation with every release, all while expecting technology to remain secure. However, we are building all of this on a foundation that is not secure or necessarily stable.

In order to secure the future, we need to better secure the present, which means understanding how the technology of our past works. Do you have to know how to program in x86 assembly off the top of your head? Absolutely not. But if you understand the basics and know what payloads and shellcode for certain attacks look like, it may help with incident response and possible future mitigation. Do you have to memorize all of the flag combinations of an IPv4 packet? Again, no. But knowing how to use a protocol analyzer and read packet traffic to find patterns and possible anomalies may give you a deeper understanding of not only what an attacker was doing but also their tactics, techniques and procedures. This all depends on your current job role and responsibilities, but if you are in cybersecurity, policy, frameworks and standards are only half the battle. Attackers have these technical skills and know their vulnerabilities or at least how to test a system for them. As a bonus, having a good foundational knowledge of information technology helps when learning about emerging tech. As cybersecurity practitioners, we have to be jacks-of-all-trades and masters of some.

> “AS CYBERSECURITY PRACTITIONERS, WE HAVE TO BE JACKS-OF-ALL-TRADES AND MASTERS OF SOME.”

The Bleeding Edge

Insanity is popularly defined as doing the same thing over and over again and expecting different results. While not a clinical definition, this expression may be onto something when it comes to evolving in our practices as professionals linked to the IT field and our practices as human beings. If something is not working, it is time to try something else while not forgetting our principles and where we are heading.

The bleeding edge of technology is still deeply intertwined with the technology of the past. As we continue to use the blade of technology to solve problems, the deeper into the artery we get and, at this point, it is not just the edge that is bloody, but the whole knife. As the incision has become deeper, we have only applied patches, sutures and made minor course adjustments to compensate for the mistakes caused by prior innovation. To compound the problem, we have also forgotten (or never properly learned) the technologies that we are currently building on, leaving room for the proverbial needle of a vulnerability in the haystack for someone to find, study, exploit, and grab any and all data that they can.

With the exception of quantum computing, the majority of computing is still done using the same processor type we were using in the 70s. And while many practitioners are excited about the prospects of a totally new computing capability and architecture with quantum, can we be worthy of such a gift in our future without first mastering the technology of the past and meeting the demands of the present?

Endnotes

[1] Anderson, J. P.; *Computer Security Technology Planning Study, Volume II*, USA, October 1972, *http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf*

[2] Exploit Database, Torrent 3GP Converter 1.51 - Stack Overflow (SEH), *https://www.exploit-db.com/exploits/47965*

[3] ISACA®, *State of Cybersecurity 2019, Part 2: Current Trend in Attacks, Awareness and Governance*, USA, 2020, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc192*

[4] Phishing.org, History of Phishing, *https://www.phishing.org/history-of-phishing*

[5] Love, J.; “A Brief History of Malware—Its Evolution and Impact,” Lastline, 5 April 2018, *https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/*

Working From Home: Reassessing Risk and Opportunities

The technology for remote communication through distributed networks existed in rudimentary form during the 1990s,[1] but sophisticated applications for distance learning, video teleconferencing, online chat and telemedicine developed modest acceptance in the early 21st century. Expanded bandwidth and network development partially explain this trajectory, but several other factors—particularly, human factors—must align well for the adoption of new technology.[2]

Habits and routines sometimes require an exogenous nudge to initiate change. The coronavirus pandemic prompted changes in behavior that have contributed to the ubiquity of telecommuting and remote conferencing. Survival depended on keeping distance and limiting face-to-face interaction. For many workers, technology became a lifeline to salvage the disrupted routines of business and society following lockdowns intended to slow the spread of the virus. Comparing today's pandemic to the influenza pandemic of 1918, one could surmise that the ability to resume essential activities—even with an acceptable sacrifice of effectiveness—provides a distinct advantage that allowed toleration of public health policies without even greater disruption of the economy.

For a change to occur, it seems one needs to be "in a pinch." Even when the technology is rough around the edges and the end user seems unprepared or unwilling, pressing needs produce efforts to accommodate new technology. Online teaching is better than no teaching; committee meetings on Zoom or Teams are better than no meetings (although we all prefer fewer, more impactful meetings). Everyone had to invest new energy to adapt to new technology, and this investment appears to be paying off. Not everyone has developed the required proficiency for online work and some even hate it, but the technology has allowed us to accomplish more today than in the past.

But our journey into the future continues, leaving us with questions. How much of this virtual world will remain part of our lives after the pandemic has passed? Will the technological shift leave lasting changes in the habits and practices of business and society? For auditors, navigating through this future requires an examination of the changing risk environment and our ability to identify and mitigate these risk areas. We should examine these questions further.

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.

Edward A. Morse, CPA
Is a professor of law at Creighton University and holds the McGrath North Endowed Chair in Business Law. He is the incoming vice-chair of the American Bar Association (ABA) Cyberspace Law Committee. He can be reached at morse@creighton.edu.

Enjoying this article?

- Read *Supply Chain Resilience and Continuity: Closing Gaps Exposed in a Global Pandemic. www.isaca.org/supply-chain-continuity-2020*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

How Did We Fare?

Balancing healthcare benefits from lockdowns with the negative impact on the economy has been a challenge around the globe. While Denmark locked down the economy, Sweden did not. The outcomes are quite different in each country and it is too soon to say which approach proved superior. South Korea avoided the lockdown, but it tested people extensively and followed the test results by isolating infected individuals and contact tracing others who were likely at risk. Such measures may be effective, but they may not be compatible with privacy expectations (and laws) in other countries.

Variations in these approaches permit the study and assessment of outcomes, with possible benefits to future efforts to address pandemic conditions. Preliminary information suggests that targeted measures aligned to the risk of each community could have fared better than a blanket shutdown.[3] Problems of overreach from regional edicts tend to disparately impact some communities with lower demographic risk. The US federal system mitigates those risk areas to some extent, but variations within the US states remain: Rural Virginia, for example, differs from areas within the state bordering the District of Columbia (DC).

Workplaces experienced differential impacts based on "essential" and "nonessential" designations by governments. For those with compatible work requirements, remote officing increased dramatically compared to pre-COVID times.[4] These workers faced new challenges, including technology issues, increased (and perhaps different types of) distractions, reduced team cohesion and difficulties with communication.[5] But offsetting benefits were also realized from avoiding the time and costs of commuting, not to mention eating meals at home and reduced wardrobe costs.

Other workers did not have the option of performing remotely but instead had to adapt to the restricted environment. Retail grocers focused on maintaining customer loyalty while assisting employees with staying healthy.[6] Curbside pickup, home delivery of online orders and special shopping hours for seniors were among the steps taken by stores to adjust to the new conditions. Restaurants and bars offered takeout menus, adapting to online orders and pick-up or delivery options. The privately held office supply distributor W.B. Mason, recognizing that people away from the office still need supplies wherever they work, began delivering products such as coffee, paper towels and bathroom cleaners directly to consumers at their homes.[7]

Most schools and universities were not prepared for a mid-semester transition to remote learning. The amount of effort was overwhelming for teachers and students; even parents had to go through the frustrations of taking on new ways of doing things. Despite all these efforts, preliminary research on school-age students suggests only 70 percent of normal school year reading skills learning and approximately half of math learning was achieved.[8] This presents a potentially lasting detrimental impact on the educational system, which will have to adapt to lower achievement in future years.

> GETTING BACK TO NORMAL MAY ENTAIL A NEW NORMAL.

From Crunch Time to Calm

Getting back to normal may entail a new normal. The benefits of remote officing may attract some workers who prefer to continue this arrangement. We Company, a space renting firm, may find lesser demand for its services from organizations whose workers choose to remain at home. But other remote workers may find temporary office space attractive to provide options for in-person meetings or to get away from the distractions of the home environment. The net effect of these preferences is difficult to gauge, as tremendous variations exist across the world. Workers residing in low-cost housing environments are presented with economical alternatives to acquire and develop home-office space, while high-rent locales present greater pressure from multipurpose use of smaller living spaces. Employers will also be looking at their own space needs—if more of their workers prefer remote officing, dedicated offices may be inefficient. Meeting spaces and temporary workspaces may become the new normal in commercial real estate configurations. Demands for convenient access by workers may also change the location of these spaces, shifting them away from current headquarters and closer to where most employees are living.

The ability to work remotely may create a new demographic division within the workforce. Rather than white-collar and blue-collar labor, we may see a division based on those who work in the IT space (haves) and those who need to be physically present at work to add value (have nots). Workers in manufacturing, construction and other production work will continue to commute to their workspaces, along with many intermediaries dealing with moving material goods. However, the breakdown of labor needs within this space may shift. Personal customer contacts may become more limited if organizations shift to remote delivery instead of in-person contact, affecting the demand for fulfillment staff and telephonic or Internet contact instead of cashiers. As technology-leveraged skill sets become more demanding, it is possible that more jobs might be lost for those who are already in the have-nots category, while the haves gain even greater importance.

Although it may be too early to judge, the expectation is that the share of remote work in the total workspace will increase over time.[9] Facebook Chief Executive Officer (CEO) Mark Zuckerberg asserts that in the long run, the company will permanently reconfigure its operations so that about half of its employees work from home (WFH). Twitter has announced that most of its employees will be allowed to keep working from home even after the pandemic passes. Unfortunately, job losses resulting from the pandemic have fallen disproportionately on those workers who cannot perform their work from home.[10] Empty offices do not need cleaning crews; those lunching at home do not generate work for restaurant workers; and even Uber drivers may see fewer customers as people choose to stay close to their home bases.

Lasting Changes That Stick

While more organizations and workers are embracing the benefits of remote work during the pandemic, there are indications that the long-term value of WFH may not hold in all cases. A report on LinkedIn indicates that some experts believe extended remote work threatens a “decay in culture” as out-of-office workers face increased isolation, distractions and blurred lines between work and home life. The report also asserts that short-term success of WFH amid the pandemic has largely been rooted in established relationships, which are harder to build and maintain online.[11] People lose touch when they are not personally present with some degree of frequency, and existing relationships may end, for example, due to retirement. It has been said that innovation and creativity can be built only with good rapport, which stems from personal contact, not a remote connection. While these are not proven assertions, the possibilities of human factors derailing a technological solution deserve consideration.

> “AS TECHNOLOGY-LEVERAGED SKILL SETS BECOME MORE DEMANDING, IT IS POSSIBLE THAT MORE JOBS MIGHT BE LOST”

Economic benefits from working at home can be expected to continue beyond the pandemic, when lockdowns have been lifted. Savings measured by avoided costs for commuting, reduced office space, and reduced friction in remote conferencing with others will tend to incentivize business leaders and their employees to keep the gains they managed to achieve while fighting the virus. If work role expectations stabilize, some employees may even consider moving to a more remote residential area, reducing congestion and improving quality of life. At a macro level, environmental protection and energy savings could show visible improvements.

But the shifts will have proven detrimental to some workers and in some environments. For example, educators involved in kindergarten, elementary, or middle school, where face-to-face interaction is extremely important for the development of young people, are likely to find the WFH option to be unsustainable. The in-school vs. out-of-school options do not appear to present comparable achievement of the end goal of a student’s personal development. Health counselors may also find that remote sessions fail to deliver the same progress with their patients. When you cannot achieve your goals, preferences for comfort and convenience are insufficient to sustain remote work practices.

Changing Risk Landscape and the Auditor

Fellow *ISACA® Journal* columnist Steven J. Ross aptly puts it, “(C)hanging the definition of work necessitates a corresponding redefinition of security over the information with which we work.”[12]

> BECAUSE THOSE WHO WFH ARE MOSTLY KNOWLEDGE WORKERS, ISSUES OF DATA PROTECTION, SYSTEMS SECURITY, INCIDENT MANAGEMENT AND PRIVACY REQUIRE CAREFUL RECONSIDERATION.

The growing acceptance of WFH qualifies as the redefinition of work, bringing along new challenges of information security. Because those who WFH are mostly knowledge workers, issues of data protection, systems security, incident management and privacy require careful reconsideration. Risk mitigation in the context of WFH requires a thorough and careful exercise in risk assessment; without it, the organization and its stakeholders could be vulnerable to new or heightened risk.

The single most important source of new or elevated risk is that remote work extends the boundaries of the formal information system of the entity. An elevated level of remote engagement calls attention to a comparatively porous system having more windows and gates than the wall protecting the traditional business edifice.[13] Diverse communication carriers, varied end-user hardware and generous authentication protocols all lead to greater risk from increasing the porousness of the system.

Disaffected, disengaged or depressed employees also present organizational risk. Are those working remotely maintaining positive mental attitudes about their work and their employer? Organizations may need to invest additional resources to help affected employees with their needs. Current tax and economic conditions present challenges for employee self-help when it comes to technology investment, which employees must make with after-tax dollars. Enhanced employer investments to equip employees to function effectively and efficiently in a WFH environment, including access to technical support, may be required. Providing regular opportunities for feedback and finding new ways to measure the effectiveness of remote work may be needed to avoid productivity losses and potential risk scenarios from careless or thoughtless behavior. Efforts to provide regular opportunities for interaction and avenues for accessing assistance may be more important than ever.

Remote work arrangements can present new tax consequences for both enterprises and employees,[14] presenting compliance and fiscal demands that had previously not been considered. Activities by employees in remote locations may also trigger new regulatory responsibilities, affecting not only those employees, but the entire business enterprise. Where will firms get the resources to devote to these new compliance efforts? Perhaps some resources will come from travel budgets, which have been widely slashed after the pandemic.[15]

Organizations with staff working remotely should consider their policies governing that work. Such policies provide anchors to identify and develop measures to mitigate related risk. An ISACA® blog post lists specific areas organizations should address:[16]

- Switch to cloud-based storage.
- Require regular password changes.
- Limit access.
- Provide for remote support systems.
- Keep software and programs up to date.

Other factors to consider might include responsibilities for ownership, access, maintenance, and acquisition of hardware and software tools needed to function effectively in a remote role. For such a significant development in the life of an organization's information systems, a disciplined approach to meeting these requirements, such as resources (including training), applications or procedures, and documentation, will be necessary to produce consistent and coherent standards that permit management to measure and assess employee and organizational progress.

The COBIT® framework naturally suits in this case, although other frameworks may also be effective in achieving the goal of systematically incorporating control risk factors of WFH. The application of COBIT to remote work was well illustrated in a recent article.[17] The article emphasizes these areas of the COBIT framework:

- Manage critical assets.
- Manage network and connectivity security.
- Manage endpoint security.
- Manage business resilience.

Whether one likes it or hates it, the new normal that incorporates WFH in a significant way is here. It is important for every organization to develop an impact analysis for WFH and consider putting in place a plan to suitably address its impact.

> “IT IS IMPORTANT FOR EVERY ORGANIZATION TO DEVELOP AN IMPACT ANALYSIS FOR WFH AND CONSIDER PUTTING IN PLACE A PLAN TO SUITABLY ADDRESS ITS IMPACT.”

Endnotes

1 For an early experiment in distance learning, see Raval, V.; *Videotex in Education: An Empirical Study*, USWEST Foundation, 1992

2 Raval, V.; “Window on the World: About the Future…,” *Information Strategy: The Executive’s Journal*, Fall 2000, p. 39–45

3 Ip, G.; “Lockdown or No? A New Look at the Costs,” *The Wall Street Journal*, 6–7 June 2020

4 Ozimek, A.; “The Future of Remote Work,” Upwork, June 2020, *https://content-static.upwork.com/blog/uploads/sites/6/2020/05/26131624/Upwork_EconomistReport_FWR_052020.pdf*

5 *Ibid.*

6 Kang, J.; “Wegman Pampered Its Shoppers, Now It Has to Protect Them,” *The Wall Street Journal*, 30–31 May 2020, *https://www.wsj.com/articles/shoppers-were-pampered-at-wegmans-now-they-are-the-grocers-biggest-risk-11590811211?mod=searchresults&page=1&pos=1*

7 FitzGerald, D.; “Office-Supply Company Pivots to the Home,” *The Wall Street Journal*, 29 May 2020, *https://www.wsj.com/articles/office-supply-company-makes-a-pivotto-your-home-office-11590667219?mod=searchresults&page=1&pos=4*

8 Hobbs, T. D.; L. Hawkins; “America’s Grand Learning Experiment in Remote Learning Fails,” *The Wall Street Journal*, 6–7 June 2020, *https://www.wsj.com/articles/schools-coronavirus-remote-learning-lockdown-tech-11591375078?mod=searchresults&page=1&pos=1*

9 *Op cit* Ozimek

10 Torrey, H.; “Many Want to Keep Working From Home,” *The Wall Street Journal*, 28 May 2020

11 LinkedIn, “Beware of Permanent WFH,” *https://www.linkedin.com/feed/news/beware-of-permanent-wfh-4852268/*

12 Ross, S. J.; “I Left My Security in the Office,” *ISACA® Journal*, vol. 4, 2018, *https://www.isaca.org/archives*

13 Raval, V.; “Window on the World: The Borderless World,” *Information Strategy: The Executive’s Journal*, Fall 2001, p. 44–48

14 Saunders, L.; “Working Out of State? Beware of Surprises,” *The Wall Street Journal*, 30–31 May 2020, *https://www.wsj.com/articles/remote-working-from-a-different-state-beware-of-a-tax-surprise-11590744601?mod=searchresults&page=1&pos=1*

15 The Audit Executive Center Knowledge Brief, *COVID-19: Longer-Term Impact on Internal Audit*, The Institute of Internal Auditors, USA, 2020, *https://dl.theiia.org/Documents/COVID-19-Longer-Term-Impact-on-Internal-Audit.pdf*

16 Johannson, A.; “Here’s How Leading Organizations Keep Remote Workers Safe and Secure,” ISACA Now, 29 March 2018, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/heres-how-leading-organizations-keep-remote-workers-safe-and-secure*

17 Villanueva, L; D. Brewer; “Managing Remote Environments With COBIT 2019,” *COBIT Focus*, 30 March 2020, *https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2020/managing-remote-work-environments-with-cobit-2019*

FEATURE

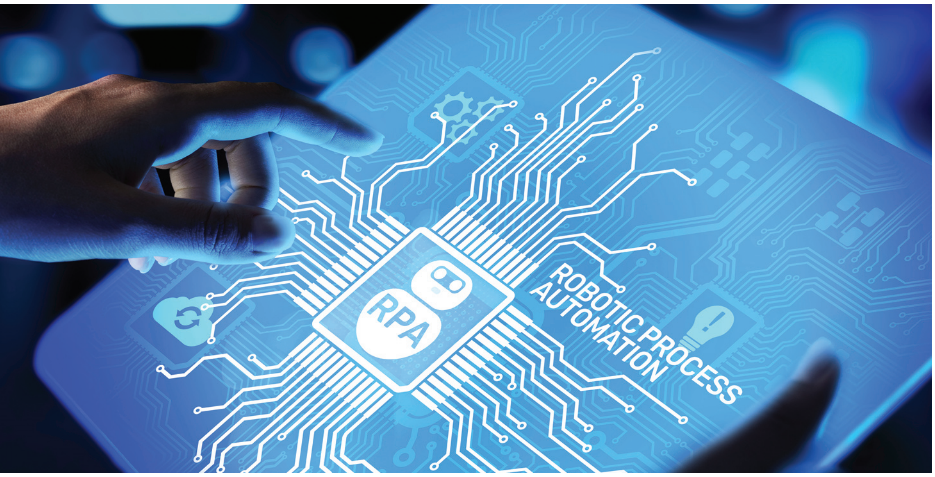
The Dark Side of Robotic Process Automation

日本語版も入手可能

www.isaca.org/currentissue

Business processes involve performing a sequence of tasks, such as registering a sale, computing value-added tax, sending an invoice, packaging and sending the product, updating the inventory and accounts receivables, etc. These tasks have traditionally been carried out by one or more human operators, with associated issues being a description of duties of each operator, information shared or processed, possible operator errors such as typos or transcription errors, labor costs, and speed of the process. With the emergence of computers, more and more of these traditionally human tasks were automated, i.e., computers were programmed to perform them.

Robotic process automation (RPA) refers to using a virtual robot (more affectionately called "bot" in industry jargon) to perform the tasks that human operators perform by following simple predefined rules such as opening a file, reading a record and sending an email.



Spiros Alexiou, Ph.D., CISA, CSX-F, CIA
Has been an IT auditor for a large company for the last 12 years. He has more than 24 years of experience in IT systems and he has written a number of sophisticated computer programs. He can be reached at spiralexiou@gmail.com.

Partially driven by the existence of bots that perform these tasks, RPA is currently in vogue. Literature suggests that audit use RPA for its own tasks, although some shortcomings are cited.[1] In other words, RPA interest is twofold:

- Enterprises ask audit to evaluate whether a place for bots exists in its own internal practice such as continuous auditing activities where a bot produces a list of exceptions to predefined criteria.
- Enterprises task audit with evaluating RPA risk given its adoption. At the same time, audit must deliver the message that sometimes RPA is used to fix poor planning and, in so doing, creates further risk that would not exist if the whole process had been planned properly.

As alluded to previously, (non-RPA) automation, i.e., software to perform a sequence of tasks, was introduced in the 1970s, if not before. For example, a program could check for a notification in the form of a file, read this file and act on the information. Such an action on the information might involve starting or stopping another task. Such standalone automated programs, often called demons, would run in the background and could, for example, check a directory every minute, discover a new file, open and read that file, and insert selected contents into another program such as a database; or they could take a backup every day at a specified time, using, for instance, the Unix cron command. Applications also communicate in other demonless ways without human involvement or knowledge of the actions, although the human operator is the one who started the application. For instance, when a user uses Hypertext Transfer Protocol Secure (HTTPS) for web browsing, the browser and server negotiate the parameters necessary for a secure connection automatically, i.e., without the user being involved or necessarily aware of any details. The point is that automation has been successfully employed for nearly half a century before RPA. So why is RPA needed? To answer this question, it is important to look at how RPA works and how it differs from plain old automation.

RPA sometimes works analogously to plain old automation and adds new functionality such as reading and deciphering a web page Hypertext Markup Language (HTML), locating data and buttons, reading the data from the web page HTML code, processing data and, ultimately, exporting/presenting results. This works similarly to the former demons, has the same effect a human operator would have, and typically works well (e.g., open a file, read a record, copy or make a decision based on a rule, and process it by sending an email or opening a browser and typing). However, as a result:

- Human operators must store any passwords needed either in cleartext or reversibly decryptable form in the RPA. Unless the application in question works with hash injections (in which case the encrypted password is enough), anyone with access to the RPA can retrieve the passwords. This, of course, is no different in principle than the former demons.
- Particularly for non-web-based applications, RPA may use "screen scraping," which is considered a last-resort measure and rightly so.[2] Screen scraping uses Optical Character Recognition (OCR) to read the screen output just as humans do,[3] but does this make sense? Data originally exist in digital form, but RPA requires printing them on the screen and reading them back to digital form. What if the OCR misses a decimal in a US$1000.00 invoice figure and reads one million instead? Or maybe a dust particle sitting on the screen is misread for a decimal point in an accounts receivable form. Human operators cannot easily read digital signals, so visual representations are warranted for humans. However, reading digital signals is the computer's most natural function. Some vendors claim[4] 100 percent OCR accuracy and, indeed, sophisticated algorithms using artificial intelligence (AI) are used to improve OCR robustness,[5] but this poses risk, especially to audit: Nothing works forever unattended error-free, and vendors typically do not insure against errors or cover possible losses. Indeed, research cites arguments against OCR, finding that "barely imperceptible altercations to images can easily fool a trained deep neural network."[6] Moreover, OCR typically focuses on recognizing characters; it is not always clear if insurers protect against missed or misread decimal points. Could a bad pixel on the screen, dust or lighting issues result in such an error? The literature also lists choosing to automate via RPA, a process where errors are "disproportionately costly," as an RPA pitfall.[7] It is also understood that protection against errors and fallback solutions are not generally available for (screen-scraping) RPA solutions.[8]

The correct solution is to automate the entire process. Instead of printing on the screen and then reading the original digital data, what could be simpler than automatically reading the digital data? Not only is this less error prone, but it is also much faster and more efficient.

> " IF HUMANS WANT TO DO A THOROUGH JOB OF CHECKING, THIS PRACTICALLY MEANS REPERFORMING THE TASKS COMPLETED BY THE BOT, HENCE NEGATING ALL ITS ADVANTAGES. "

Why is screen-scraping RPA even discussed as a viable solution? The answer is for a variety of reasons, such as closed proprietary systems with poor or no Application Programming Interfaces (APIs) or interfaces, legacy systems with code written in obsolete programming languages, and/or poor design of these systems. RPA appears as the lesser evil. The system is often designed to employ human operators for routine tasks from the start or the needs evolved and were extended, again using human operators for routine tasks. Of course, the correct solution is to automate routine tasks in the first place, with data available to automated routines that perform these rule-based tasks without the need for humans or screen output. In addition, source code is often unavailable or unmodifiable for either ownership, budgetary or readability reasons, so that automation cannot be built on top or as an extension

Enjoying this article?

- Watch CPE on Demand: *Audit Outlook: Intelligent Automation*. *www.isaca.org/Audit-Outlook-Intelligent-Automation*
- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

of the existing system. To be fair, RPA limits dependence on the coder (but increases dependence on the RPA solution).

To address issues such as the misreading of decimals, further human controls are introduced, which is problematic because humans tend to agree with bots, especially when the probability of bot error is low. If humans want to do a thorough job of checking, this practically means reperforming the tasks completed by the bot, hence negating all its advantages. If the task and risk are significant enough to require the attention of humans with questioning mindsets, the task should have been assigned to a human in the first place; better yet, the risk of such errors caused by the bot itself should be eliminated.

All this is not to say that risk associated with any IT system are nonexistent or should be downplayed. Such risk scenarios cover the entire lifetime of RPAs, but are not fundamentally different from those of any IT system from development, operation, ownership, security, logging, monitoring, business continuity, change management, incident management (yes, bots can fail and crash) to retirement.

> “WHAT AUDIT NEEDS TO KNOW AND DO IS TO BE AWARE OF THE RISK AND MAKE SURE RPA IS USED BECAUSE OF NEED AND NOT POOR PLANNING.”

Conclusion

RPA is likely to remain in vogue, mostly due to the cost-cutting attraction of replacing humans with machines. What audit needs to know and do is to be aware of the risk and make sure RPA is used because of need and not poor planning. New systems should not be designed with RPA in mind; they should be automated by design. Access to open source code combined with the knowledge and skill to extend the code are significant advantages. RPA is automation, and automation is, in general, desirable, but screen-scraping RPA is an inefficient and insecure automation that introduces potentially significant risk factors that proper automation eliminates. Because many decision makers do not understand how RPA works, audit must indicate that screen-scraping RPA is a poor substitute for full automation and should be a last, not first, resort solution. To design a new system that automates with RPA makes no sense at all. Instead of looking for a magical action that will somehow fix all problems, the correct way is to think about the process and how to optimize it.

Additional RPA pitfalls exist and, indeed, a number of articles discuss RPA “failures.”[9, 10, 11, 12, 13] These mostly focus on their application, not on the technology itself. Currently, RPAs are programmed to do repetitive, nonintelligent (i.e., rule-based) tasks that do not change; in general, they cannot handle unexpected scenarios such as a change in an application's screen layout; nor do they work out-of-the-box, as customization to the relevant process is, in general, needed. Similarly, processes and tasks do not exist in isolation but typically require input and give output to other tasks and processes. These interdependencies are also important. However, if RPA is a hammer, the world is not a nail, and often better, safer and more efficient ways exist to accomplish the same ultimate goal.

Endnotes

1 Struthers-Kennedy, A.; A. Poulikakos; “RPA: First Steps to Greater Internal Audit Efficiency,” Corporate Compliance Insights, 16 November 2018, *https://www.corporatecomplianceinsights.com/rpa-first-steps-to-greater-internal-audit-efficiency/*

2 KPMG, “Internal Audit and Robotic Process 2 Automation: Considerations for Assessing and Leveraging Intelligent Automation,” *https://assets.kpmg/content/dam/kpmg/nl/pdf/2018/advisory/internal-audit-and-robotic-process-automation.pdf*

3 Techopedia, “Screen Scraping,” *https://www.techopedia.com/definition/16597/screen-scraping*

[4] UiPath, "Screen Scraping Software for Desktop and Web-Screen Scraping that Works Everywhere," *https://www.uipath.com/solutions/technology/screen-scraping*

[5] Sporici, D.; "Evaluating the Robustness of OCR Systems," Coding.Vision, 7 September 2019, *https://codingvision.net/ai/evaluating-the-robustness-of-ocr-systems*

[6] Qian, S.; "Adversarial Robustness of Optical Character Recognition (OCR)," *Medium*, 19 September 2019, *https://medium.com/@sharon.qian.10/adversarial-robustness-of-optical-character-recognition-ocr-91eedc36ef6*

[7] AIMultiple, "20 RPA Pitfalls and the Checklist for Avoiding Them [2020 update]," 1 January 2020, *https://blog.aimultiple.com/rpa-pitfalls/*

[8] Morphy, E.; "Why RPA Implementation Projects Fail," CMSWire, 5 March 2019, *https://www.cmswire.com/information-management/why-rpa-implementation-projects-fail/*

[9] Casey, K.; "Why Robotic Process Automation (RPA) Projects Fail: Four Factors," Enterprisers Project, 18 June 2019, *https://enterprisersproject.com/article/2019/6/rpa-robotic-process-automation-why-projects-fail*

[10] Hewlett, G.; "Five Most Critical Points of Failure in RPA Implementation," *Assurity*, 12 November 2019, *https://assurity.nz/insights/five-most-critical-points-of-failure-in-rpa-implementation/*

[11] Iluri, S.; "Top 10 Reasons Why Automation Efforts Fail," Skan, *https://skan.ai/top-ten-reasons-why-automation-efforts-fail/*

[12] Trefler, A.; "The Big RPA Bubble," *Forbes*, 2 December 2018, *https://www.forbes.com/sites/cognitiveworld/2018/12/02/the-big-rpa-bubble/*

[13] Leonards, A.; "What Can We Learn From RPA Failures?" *Raconteur*, 9 September 2019, *https://www.raconteur.net/technology/rpa-failures*

FEATURE

Building a Culture of Security

A cybersecurity culture is more than physical barriers of entry into a building, multifactor authentication system access or least privilege authorization. It is a collective mindset of the people in the organization working every day to protect the enterprise. A robust security culture can reduce risk and save enterprises millions of dollars by offsetting the impact of corrupted or lost data, decreased revenue, regulatory fines, and protect the enterprise's reputation.

Before the personal computer (PC) and the Internet, cybersecurity was relatively easy. Most machines were green screen terminals that connected directly to a mainframe in the basement. Security was the easy task of not letting strangers access the building. Even with a stolen credential, hacking the system required physical presence. However, with the introduction of the PC and later the Internet, intrusion happens halfway around the globe.

Paul Frenken, ACP, FAIR, PMP, PMS1
Is an independent consultant focusing on bringing value by implementing emerging technology and best business practices for his clients. He brings more than 20 years of experience in IT infrastructure, development, change management, customer and consulting services. With a varied background from startup dot-coms to Fortune 50 organizations, Frenken applies business best practices and cutting-edge technology to improve profit margins.

Security now means more than physical enforcement. Protecting enterprise assets requires a culture of security throughout an enterprise.

Why Is Cybersecurity Culture So Important?

A strong cybersecurity culture helps protect the enterprise's most important asset: its data. Physical assets such as equipment, buildings and even people can be replaced; however, data are difficult to replace. Most organizations spend years and countless resources to acquire and create their enterprise's data assets. Many enterprises that lose data may become insolvent. Thus, organizations need to value protecting their data and cybersecurity at all levels. Reports about enterprises targeted because of inadequate security riddle the media. Simple security standards that all employees follow can address most security issues. Human error or behavior causes 90 percent of all cyberattacks.[1] Employees losing their laptops or cell phones, inserting flash drives into their computers, or opening mysterious emails compromise more enterprises than malicious criminal hacks from external adversaries.

Organizations spend millions of dollars on hardware and software such as firewalls, virus protection and physical barriers. However, enterprises economize on employee training and fail to value security culture enough to invest resources in building and enforcing standards that provide protection from human behavior.

What Is a Security Culture?

A security culture constitutes more than just cyberawareness. It must:

- Incorporate a broader corporate culture of day-to-day actions encouraging employees to make thoughtful decisions that align with security policies.
- Require the workforce to know the security risk and the processes for avoiding that risk.

- Build and enforce an operating process of tasks that keeps the enterprise safe.

A security culture includes a healthy combination of knowledge and follow-through of daily work tasks.

Cybersecurity best practices start with building a security culture. Intuitively, most cybersecurity professionals agree that spending resources on workforce training about the importance of cybersecurity is best for an enterprise's security efforts. Teaching employees to recognize threats, curb poor behavior and follow basic security habits is the best return on investment (ROI). However, measuring and justifying the expense proves challenging. Persuading upper management with an ROI number based on employee training and changing the organization's culture requires aggressive, high-pressure sales.

The probability of employees starting a fire in the enterprise either by accident or design is lower than them opening an avenue for a cyberattack. Employee education, behavior and culture focused on cybersecurity best practices and standards are as important as the annual fire drill. It is the cybersecurity professional's responsibility to persist in building a security culture to change how employees view cyberprotection. Whether it is senior management, human resources or the employee in the cube next door, everyone needs to continuously sell cyberstandards and best practices. When a cyberattack impacts the enterprise's systems, everyone will look at the cyberprofessional to answer the question, "How could this happen?"

How to Change to a Security-Conscious Culture

Most IT teams value security business practices and standards. The biggest challenge with developing a security-conscious culture occurs with enterprise middle to senior management supporting solid security practices and building the culture to support it. These levels can look upon building a security culture as another expense to the business with little quantitative ROI to the organization.

> “EVEN BY CITING NUMEROUS HIGH-PROFILE AND COSTLY BREACHES, PERSUADING MANAGEMENT TO INVEST IN A BEHAVIORAL CHANGE WITHIN THE ORGANIZATION STILL PROVES CHALLENGING.”

To mitigate enterprise indifference, cybersecurity professionals may follow a few steps to build a solid foundation for a security culture. First, publish statistics on the number of times hackers probed enterprise systems. Most employees, especially senior management, will be astonished by the sheer volume. Second, track and publish statistics on the number of phishing and junk emails that come into the enterprise's mail servers. It should be noted that email is one of the top avenues for hackers to gain access to enterprise systems.[2] Although most employees believe they know how to recognize a phishing email and avoid responding to the email's request, 30 percent of all phishing email is opened, and 12 percent overall have links that are clicked.[3]

Obtaining Senior Leadership

Once the hacking data are shared, the next step involves obtaining buy-in from senior leadership. Numbers, ROI, revenue and shareholder value motivate senior leadership. Cybersecurity risk proves challenging to assign an ROI number. However, hard data of potential attacks help management realize that a breach has a higher potential of happening than a fire in the office. Sharing a breach's cost to a similar organization's profit margins assists management in viewing the investment in a security-conscious culture as a pseudo insurance policy. However, even by citing numerous high-profile and costly breaches, persuading management to invest in a behavioral change within the organization still proves challenging.

The chief information officer (CIO), chief technology officer (CTO) or chief information security officer (CISO) must assume the role of cybersecurity champions on the leadership team. These IT leaders need to garner the leadership team's confidence to help explain the threat, risk and impact of failing to develop a secure mindset. These security champions are key in building and maintaining a cybersecurity culture.

Enjoying this article?

- Read *COBIT® Focus Area: Information Security*. *www.isaca.org/COBIT-Focus-Area-Information-Security*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Cybersecurity Culture as an Insurance Policy?

Cybersecurity professionals sell the cybersecurity culture investment to management as an insurance policy like any other business insurance. Most enterprises carry insurance to protect against liability, fire and theft on their capital equipment and employees. To justify this expense, senior management asks the question, "Can a business continue if the building or inventory is lost due to fire, flood or theft?" The answer is usually no, so management makes the business decision to purchase insurance to protect against the potential of a disaster.

Most enterprise managers value fire, flood or theft insurance. However, according to the US National Fire Protection Association, there are an average of 3,340 office fires in the US each year.[4] *DarkReading* reported 6,500 enterprise data breaches in 2018.[5] That is only the ones that were reported or even the ones the enterprise knew about. How many times has an enterprise stated it recently discovered a breach that occurred a few years ago? Or worse, they never realize they were breached at all. Statistically speaking, enterprises are more likely to experience a monetary loss from a cyberincident than a fire or flood, yet management is more likely to invest in fire and flood insurance than building a quality cybersecurity culture.

Framing a cybersecurity culture as an insurance policy is more likely to motivate senior management to support the initial expense of building a security culture. Cybersecurity professionals know that the biggest ROI is training enterprise team members on safe cyberbehavior.

Workforce Buy-In and Training

After garnering management support, security professionals must persuade the workforce to change its behavior. To do this, one must survey the enterprise's associates for suggestions. Nothing helps to build cultural change more than involving employees in the process and solution. If the workforce understands the threat and helps with the solution, then the culture has a good foothold to grow into a standard operating procedure.

Once security professionals have employees invested, they must create training programs. Although a robust cybersecurity training program requires labor-intensive work, it proves invaluable in engendering the culture. Thirty-seven percent of organizations' staff cite insufficient cybersecurity training in the workplace.[6] Training warrants more than one workshop or online course. An efficacious training program needs to repeat key concepts more than once a year. For example, some enterprises publish monthly IT newsletters to facilitate communication with other divisions. These newsletters cover various security topics, and each month, IT team members discuss these topics with their colleagues outside of IT. Some even require employees to add the monthly topic to their internal email tagline to reinforce it. This may help persuade colleagues to recognize cybersecurity as a serious matter.

> "FRAMING A CYBERSECURITY CULTURE AS AN INSURANCE POLICY IS MORE LIKELY TO MOTIVATE SENIOR MANAGEMENT TO SUPPORT THE INITIAL EXPENSE OF BUILDING A SECURITY CULTURE."

Build Security Policies

Well-documented policies form the cornerstone of a security culture. Cybersecurity policies must cover the daily operating procedures of using enterprise assets and accessing data resources. The IT security team develops the official security policies, and stakeholders approve them. These policies outline the rules and procedures that everyone with access to enterprise assets must follow. Some human resources (HR) departments create additional employee security behavior documents that cover expectations and outline the consequences of noncompliance. During new employee onboarding, both the hiring manager and HR must ensure that the recruit has completed the security training requirement.

Report an Incident

The last step in building a cybersecurity culture is to encourage employees to report incidents. Some enterprises even build systems to recognize associates who detect problems, loopholes or inconsistencies in human and equipment cyberbehavior. Cybersecurity professionals must provide easy avenues such as a group cybersecurity mailbox, website form or phone number for incident reports. When employees understand the risk and have an easy avenue to report issues, they will likely use it, especially if they gain some recognition for identifying an issue.

Addressing the Naysayers

Identifying the number of potential intrusions, garnering management support, building workforce buy-in, creating clear policies and building an easy avenue to report incidents all set the foundation for a cybersecurity culture. Any effective cultural change requires labor-intensive work from everyone. Thus, with change comes resistance. Despite a cybersecurity culture's positive impact, there will be naysayers who resist any change. Peer pressure impacts the behavior of those few employees who resist the change. In most cases, the lollygaggers will conform after their fellow employees press them. Finally, a cybersecurity culture requires HR to create policies that support the security culture and procedures to correct or even terminate noncompliant employees. Building a cybersecurity culture empowers team members to be proactive and vigilant in their daily tasks. Every employee's unwritten job description includes cybersecurity.

Behavioral Change Takes Time

Hackers often use phishing emails to enter enterprise systems. To test a security training's efficacy, cybersecurity professionals may send a test phishing email to employees who completed the training. What do the results indicate about security culture? It takes time for policies to become an embedded culture.

For example, a colleague recently shared a story of one experience building a security culture. The goal of the initiative was to teach team members to lock their systems when away from their desks. First, approximately 3,000 employees completed security training. To reinforce this training, the IT team printed 1,000 yellow business cards stating: "You are away from your desk but your computer is not locked." The IT team would walk the halls and place cards on team members' computers who were away from their desks but had not locked their computers. In three months, the IT team finished disseminating all 1,000 cards. The reminder cards' second printing was on an orange background, and they were disseminated in approximately nine months. The third printing was on red cards, and 18 months into the third printing cycle, the IT team still had approximately 600 cards. A few older cards were still circulating. This means that colleagues had taken cybersecurity to heart and were using older cards to remind their coworkers about the importance of computer security. This successful security culture campaign required a minimal investment, but had a major impact on building a cybersecurity culture.

> “WHEN EMPLOYEES UNDERSTAND THE RISK AND HAVE AN EASY AVENUE TO REPORT ISSUES, THEY WILL LIKELY USE IT, ESPECIALLY IF THEY GAIN SOME RECOGNITION FOR IDENTIFYING AN ISSUE.”

Excessive Cybersecurity

Based on firsthand experience, one large top-five financial services enterprise took a draconian approach to cybersecurity. For example, it replaced all laptops with virtualized desktops, initially turned off all Universal Serial Bus (USB) ports, locked out the Internet and did not allow emailing out of the enterprise. These excessive cybersecurity approaches made work challenging and simultaneously introduced new risk to the environment. First, the enterprise required traveling employees to use their personal laptops or the hotel's business center computer. Neither option presented a good choice. Employees may not upgrade and patch their personal machines often enough, and who knows who last used the business center machine.

The enterprise wanted to limit the possibility of an intrusion from a USB device. However, this policy made modern office tasks challenging. It is difficult to use Personal System/2 (PS/2) keyboards or mice and forget about any wireless input devices when

> “THE GOAL IS TO WORK WITH BUSINESS AND BUILD A CULTURE THAT PROVIDES THE ABILITY TO COMPLETE WORK AND SECURE THE ENTERPRISE’S ASSETS.”

all the USB ports are disabled. The Internet was so locked up that conducting any research was difficult.

However, prohibiting sending external email and stripping incoming email attachments were the most excessive policies that made it difficult to communicate with vendors. In fact, traveling employees had to use their personal email accounts on their phones to communicate with vendors and use their personal printers to print attachments such as requests for proposals (RFPs) and statements of work (SOWs). Management waited three weeks to revoke some of the most stringent controls and almost six months to finally achieve a balance between security and business. This exemplifies what not to do. This security culture became excessive, angering many employees and introducing new threats. Enterprises must avoid stringent policies that make it too difficult for employees to do their jobs. The goal is to work with business and build a culture that provides the ability to complete work and secure the enterprise’s assets.

Conclusion

Building a security culture needs to have a balance between business activity and business security. Encouraging employees to participate in building a cybersecurity culture will go a long way in embedding the culture in the everyday tasks of the employee. Employees will learn to understand their role in keeping the organization safe and accept responsibility to help remove threats. The human factor is the weakest link in security practices, but with a cybersecurity culture, organizations can turn the weakest link into the strongest asset.

Endnotes

1 Spadafora, A.; “90 Percent of Data Breaches Are Caused by Human Error,” *Techradar*, 8 May 2019, *https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error*

2 Data Insider, “91% of Cyber Attacks Start With a Phishing Email,” Digital Guardian, 26 July 2017, *https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing*

3 Verizon, *2019 Data Breach Investigations Report*, USA, 2019, *https://enterprise.verizon.com/resources/reports/dbir/*

4 Campbell, R.; “U.S. Structure Fires in Office Properties,” National Fire Protection Association, August 2013, *https://www.nfpa.org/News-and-Research/Data-research-and-tools/Building-and-Life-Safety/US-Structure-in-Office-Properties*

5 Vijayan, J.; “2018 Was Second-Most Active Year for Data Breaches,” *Dark Reading*, 13 February 2019, *https://www.darkreading.com/threat-intelligence/2018-was-second-most-active-year-for-data-breaches/d/d-id/1333875*

6 Netwrix, *2018 IT Risks Report*, USA, 2018, *https://www.netwrix.com/2018itrisksreport.html*

Pandemic-Driven Remote Working and Risk Management Strategies

日本語版も入手可能

www.isaca.org/currentissue

One of the most visible results of the 2020 COVID-19 pandemic has been the mainstream transition from traditional office-based work to remote work-at-home arrangements. Government officials worldwide mandated that nonessential employees stay home. Enterprise leaders followed the government mandates by directing employees to isolate at home to keep the virus from spreading throughout employee populations. A primary lesson from that experience is that employees and the critical functions they perform can be protected and maintained by initiating secure remote teleworking operations. Unfortunately, as **figure 1** depicts, remote working introduces new IT-related threats that require unique threat mitigation countermeasures.

These countermeasures can be organized under five categories:

1. Employee security
2. Endpoint security

Figure 1—Remote Work Threats and Countermeasures

Threat	Countermeasures
Theft of teleworking endpoints and devices	Work-from-home policy, endpoint encryption, identity and access management (IAM) and, preferably, multifactor authentication (MFA), endpoint management technology (e.g., mobile device management [MDM], mobile application management [MAM])
Unauthorized monitoring, collection or modification of traffic passing over teleworking networks	Work-from-home policy, hardened virtual private network (VPN) infrastructure, enhanced logging of VPN infrastructure, IAM and preferably MFA, encryption, backup and restore
Telecommuting-specific increases in endpoint malware infection	Work-from-home policy, antimalware services, endpoint and remote access system vulnerability management, network access control (NAC), application security, security information and event management (SIEM)
Pandemic-specific phishing attacks	Employee training, email antiphishing services, SIEM
Pandemic-specific malicious website infections	Employee training, web content filtering, SIEM
Remote teleworker outages and service request management	Enhanced technical support, hardened high-availability remote access systems and VPNs
Theft or destruction of enterprise intellectual property by temporarily furloughed or laid-off employees	IAM and preferably MFA, MDM, MAM, SIEM, cloud access security broker (CASB)

Brett Bonin, CISA
Is a successful cybersecurity executive with extensive experience leading world-class corporate security transformation and optimization programs. Bonin currently directs global security strategy and operations as the deputy chief information security officer of Omnicom Group, a Fortune 100 international marketing company with five major subsidiary networks: DAS Group of Companies, DDB, BBDO, Omnicom Media Group and TBWA. He leads the organization in securing both corporate IT and the intellectual property of more than 5,000 business clients in more than 100 countries, including brands such as Apple, AT&T, Cisco, Hewlett Packard, Microsoft, Nike, PepsiCo and the US Army. Bonin honed his security and business leadership practices through 25 years of mentoring from the best global executive leaders, and he has diverse senior-level experiences in private- and public-sector roles. He is a retired US military officer with 25 years of decorated service in cyber, engineering and intelligence.

3. Network security
4. Security monitoring
5. Security reporting

Each of these categories contains security areas that, if ignored, could result in serious risk both during the transition and longer term operational approach to predominantly working remotely. Enterprise leaders should evaluate each one for applicability to their unique environments.

Employee Security

Employee security is one of the five categories that require unique countermeasures. Employees are often the weakest link in enterprise security because they have countless opportunities to make decisions that could lead to a security breach. Employee security focal points include teleworking policy, training, antiphishing, and identity and access management (IAM):

- **Teleworking policy**—A solid work-from-home policy that accounts for pandemic-related threats is an essential starting point for maintaining safe and continuous business and IT operations. The work-from-home policy should specify what enterprise leaders expect from employees who are working remotely. It should emphasize cybersecurity considerations, such as safe remote computing, acceptable use and sanctioned applications. Acceptable use is a general concept that may have been in effect before the pandemic, so enterprises should create an exception to policy and procedure to enable users with special-case scenarios to perform functions that would otherwise be restricted as unacceptable. The policy should provide information such as who to contact in the case of lost or stolen devices, phishing, or the observation of suspicious computing events. The teleworking policy should also intersect with enterprise training and provide a list of mandatory training courses aimed at mitigating the threats specific to telecommuting. Critical to a safe remote work environment is the virtual private network (VPN) that provides connectivity from home offices to enterprise systems. Remote workers should have access to all the how-to information they need to connect remotely over the VPN.
- **Employee training**—Training managers should consider creating specialized training content to empower employees with the knowledge to manage the unique threats they will face while teleworking. Training should include policies governing work-from-home computing rules and tutorials that prepare end users for potential threats, such as laptop thieves or pandemic-specific phishing emails.
- **Email antiphishing services**—Enterprise leaders should prepare for new pandemic-specific phishing tactics. For example, hackers may send malicious emails to employees under the guise of pandemic-related subjects to make them seem more relevant and to trigger an emotional impulse to click on the malicious link or file attachment. The enterprise should implement or fine-tune antiphishing platforms to account for messages with pandemic signatures coming from external sources.
- **IAM**—IAM teams need to both grant new access and remove existing access based on unique pandemic-specific considerations. Onboarding and offboarding employees remotely will require IAM actions to create, temporarily disable and delete employee IAM credentials and underlying authorizations. Multifactor authentication (MFA) is also imperative, particularly for anyone connecting from remote locations to perform elevated administrator and high-risk functions. Certain industries and job functions that involve sensitive data should ensure that all systems that store, process and transmit sensitive data are hardened through enhanced IAM security measures such as centralized log correlation,

> “BY DIRECTING THE ENCRYPTION OF ENDPOINT HARD DRIVES AND SENSITIVE FILES, ENTERPRISE LEADERS CAN BE ASSURED THAT LAPTOP AND MOBILE DEVICE THIEVES WILL NOT BE ABLE TO ACCESS DATA.”

monitoring and retention of user login attempts and access. MFA is wise for users performing job functions involving high-risk sensitive data.

Endpoint Security

The endpoint security category is the second of five categories that require unique countermeasures. Weaknesses in endpoint and device security can provide an abundance of opportunities for threat actors to gain unauthorized access and damage the integrity and availability of data. Endpoint and device security focus areas include endpoint encryption, endpoint management services, antivirus services, endpoint vulnerability and patch management, backup and restore, web content filtering, application security, and cloud access security broker (CASB):

- **Endpoint encryption**—With so many employees working remotely, many more laptops will be used outside the office in remote locations without physical security protection. By directing the encryption of endpoint hard drives and sensitive files, enterprise leaders can be assured that laptop and mobile device thieves will not be able to access data.
- **Endpoint management services**—Managing laptops and devices remotely over the Internet is more important when the majority of employees are teleworking. For example, existing patching platforms may double as mobile device management (MDM) platforms. Windows System Center Configuration Manager (SCCM) and Apple Jamf have remote wiping and locking capabilities that IT and security leaders can use to maintain the confidentiality of data, intellectual property and trade secrets. These platforms can also be used to partition and ultimately wipe, if necessary, enterprise data without impacting personal data on personal mobile devices if the enterprise has a bring-your-own-device (BYOD) program.
- **Antivirus services**—Next-generation antivirus services inhibit the execution of malicious logic on endpoints, servers and devices. These types of preventive security tools do not rely on static malware signatures alone, but block the execution of malicious logic based on artificial intelligence (AI) and machine learning to protect against zero-day exploits. Next-generation antivirus services provide better protection than legacy signature-based services.
- **Endpoint vulnerability and patch management**—More remote teleworking translates into more scanning and patching and greater exposure to threats. Remote workers connecting to insecure home and public networks, particularly those bypassing centralized enterprise IT security services, are much more vulnerable than typical in-office workers. Patching endpoint vulnerabilities is part of basic computing hygiene that becomes more important during teleworking.
- **Backup and restore**—The ability to restore data from backup is essential to any operating environment exposed to threats that can alter the integrity and availability of enterprise data. If user data are backed up, enterprise leaders can mitigate threats such as ransomware viruses and stolen laptops and other devices by ensuring that lost data can be recovered and restored.
- **Web content filtering**—Hackers may create malicious pandemic-related websites containing malware that could compromise remote user endpoints and, ultimately, allow hackers to enter the enterprise network or steal data from the end user. Content filtering services can be tuned to filter out malicious pandemic content.
- **Application security**—Employees may use their enterprise endpoints to access consumer cloud applications (e.g., messaging, video) that can expose the enterprise to significant risk. Enterprise IT leaders should identify and patch these third-party applications or remove them from employee endpoints.

- **Cloud access security broker (CASB)**—CASB services can provide enterprise leaders with insight into what types of applications employees are using and what types of data they are uploading and downloading. The CASB also allows the enterprise to control risky cloud activities.

> “MORE REMOTE TELEWORKING TRANSLATES INTO MORE SCANNING AND PATCHING AND GREATER EXPOSURE TO THREATS.”

Network Security

Network security is the third out of the five overall categories that require unique countermeasures. A network is the “highway in” and should be both resilient and robust while also serving as a “checkpoint” into restricted areas with restricted data. Network security countermeasures include high-availability remote access infrastructure, network access control (NAC) and enhanced technical support:

- **Hardened high-availability remote access infrastructure**—With a shift to remote teleworking, VPN system security and resilience become more important. Without hardened, strong encryption, attackers can exploit weaknesses in remote connectivity systems to either gain unauthorized system access or collect and/or modify data in transit. Network staff can harden VPN systems by requiring MFA to augment the simple stand-alone username and password, making it much more difficult to exploit and gain access. Scanning for VPN infrastructure vulnerabilities and then patching and configuring them to a hardened and secure state are critical when work is performed remotely over VPNs. The VPN system should be resilient and implemented in a redundant, high-availability architecture to ensure that there are no single points of failure. The network team must also provision the VPN to support large increases in remote user traffic, making centralized Internet capacity and circuit redundancy more critical as well.
- **Network access control (NAC)**—NAC services perform a gatekeeper function by not allowing users and their laptops or devices to connect to enterprise services without passing system checks. NAC systems also provide an actionable compliance status for each endpoint based on a set of enterprise security policy requirements. Managers can designate which segments and resources VPN-connected users can access in accordance with the principle of least privilege based on compliance status and employee identity. Security leaders can effectively cordon off endpoints that might be susceptible to threats based on the NAC system-generated risk profile for each endpoint prior to connecting to the network.
- **Enhanced technical support**—Technical support processes, which would typically include physically bringing laptops and other devices to work for repair and inspection, need to be updated to conform to constrained pandemic operations when only remote access is feasible. Technical support teams will require secure remote desktop applications. IT leaders should evaluate all remote management applications and ensure that staffers harden them to the fullest.

Security Monitoring

Security monitoring is the fourth out of five overall categories that require unique countermeasures. Every node on the network produces event logs that security professionals can leverage when piecing together clues during an investigation. Security practitioners can deploy security information and event management (SIEM) platforms to centrally correlate and store event logs for future analysis during investigations. A shift to remote teleworking involves specific systems that produce unique logs that need to be a new focus.

SIEM includes central correlation and monitoring of events from security platforms that indicate potential compromise from pandemic-related threats. The monitoring team should ensure that specific events from the following types of sources are being monitored for malicious activity:

- Security system availability
- Endpoint malware infections
- VPN
- Identity and access authentication requests and failures
- MDM
- Email antiphishing services

> "ENTERPRISE SECURITY LEADERS SHOULD CONSIDER CREATING SPECIALIZED REPORTING CAPABILITIES THAT PROVIDE THE STATUS OF SECURITY SERVICES AIMED AT MITIGATING PANDEMIC-RELATED THREATS."

Security Reporting

Security reporting is the fifth and final category that requires unique countermeasures for a shift to remote teleworking. Enterprise security leaders should consider creating specialized reporting capabilities that provide the status of security services aimed at mitigating pandemic-related threats. The following are examples of specialized reporting:

- Number, type, purpose and criticality of remote user endpoints not reachable by endpoint management systems such as patching, antivirus, MDM and encryption
- Access logging and monitoring of privileged administrative access to high-risk systems and functions
- Employee and system compliance reports with current vulnerabilities, prioritized by the most critical vulnerabilities
- VPN-specific indicators and metrics, such as availability, employee logins and data specifics
- Remote user backup status
- CASB reports on risky remote user cloud data transfers and risky public cloud application use
- Remote worker policy exceptions
- Remote worker acceptable Internet usage

Conclusion

When pandemics such as the COVID-19 outbreak lead to a widespread, rapid shift to remote working in home offices, the enterprise threat landscape changes, and enterprise IT security leaders must deploy specific enhanced threat mitigation countermeasures. By implementing enhanced IT security countermeasures in employee security, endpoint security, network security, monitoring and reporting, enterprises can ensure that business systems will continue to operate in an unimpeded, secure manner.

Enjoying this article?

- Read *Getting Started with Risk Management. www.isaca.org/Getting-Started-With-Risk-Management*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Applying Agile to Digital Audit Transformation

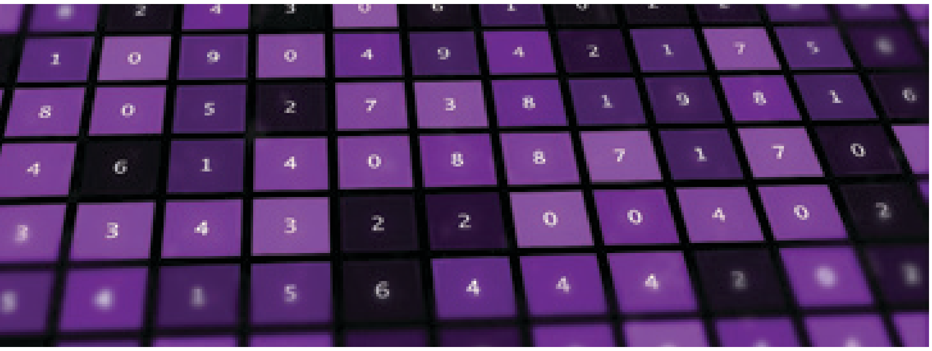
The following statement sounds like it could have come from today's news: "54% (of [chief executive officers] CEOs) are funneling money toward growth initiatives, including emerging technologies in mobile devices, social media, and data analytics."[1] However, it is actually from a 2011 survey conducted by PricewaterhouseCoopers. Fast-forward eight years, and PricewaterhouseCoopers' 2019 survey found that "49% of IA [internal audit] functions do not use RPA [robotic process automation], but 45% plan to within 2 years."[2] Investment in next-generation technologies such as data analytics and RPA has been a priority for almost a decade, but within the IA function, the implementation of these technologies is self-reported at only 50 percent. In the same decade, many of IA's IT partners have successfully implemented digital transformation (or risked irrelevancy). Project risk has not gone away, but it may not be a coincidence that IT's acceleration in digital innovations coincided with its acceleration in Agile project management.

Before examining the application of Agile for IA teams, it is important to note a few of the key project success factors the Agile methodology was developed to maximize. COBIT 2019's Build, Acquire and Implement (BAI) BAI11 Managed Projects identifies three alignment goals (AGs) goals for the project management process:

1. AG03 Realized benefits from information and technology (I&T)-enabled investments and services portfolio
2. AG06 Agility to turn business requirements into operational solutions
3. AG09 Delivering programs on time, on budget and meeting requirements and quality standards

The Project Management Institute (PMI) has identified seven key performance factors that can be associated with the four goals listed previously and used to evaluate how effectively the Agile model meets COBIT® process goals. For example, goal 1 is tied to PMI's performance factor that states, "focus on business value, not technical detail." Goal 2 relates to PMI's guidance to "provide the project team members the tools and techniques they need to produce consistently successful projects." Goal 3 is tied to PMI's performance factor that states, "include the customer at the beginning of the project and continually involve the customer as things change."[3]

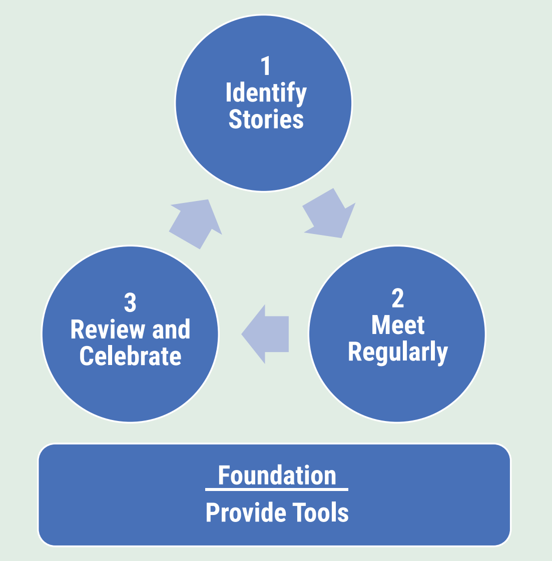
Agile addresses both the primary goals of COBIT 2019's BAI11 and PMI's performance factors. In accordance with the primary focus on business value, Agile starts by identifying desirable business features, which are presented as stories. These stories do not include the specific software modules that will be implemented; technical how-to decisions are made after a story has been understood and documented. After identifying the desirable business value, regular meetings are held to ensure that requirements are understood, to provide feedback and to generate ideas that can feed the next set of stories. Although this sounds simple, and although communication is generally easy to do, maintaining it consistently throughout



Chris Sanders, CISA, COBIT 5 Foundation Certified
Is senior manager of identity and access management (IAM) controls assurance and review for Charles Schwab in Denver, Colorado (USA). He has nine years of IT audit and security experience and has led the creation of multiple data analytics programs for IT audit and control monitoring groups.

the life of a project requires either proper discipline or a methodology such as Agile that makes it second nature. Audit teams have probably already examined Agile or have considered using it as a tool, but Agile also offers a disciplined approach to incorporating data analytics or RPA into audits (**figure 1**).

Figure 1—The Agile Model



The first step in the Agile model for next-generation audit development is to identify stories. This is where big ideas are turned into actionable deliverables and where overall projects are prioritized and carved into stories.[4] Planning to automate the user termination control review via RPA is a great idea, but proposing this project to an audit team and asking for an update in a couple of months is the opposite of Agile. Agile is not an approach that consists of handing out a new tool and asking the team to run with it; it requires discipline to realize benefits. Identifying time-bound stories keeps the project team from going into the "back room" for months and emerging with an unexpected result (good or bad). Rather than asking for the overall project to be executed and devising a week-by-week plan for the next three to 12 months (otherwise known as the waterfall approach), a team leader or project manager serving as the scrum master divides the project into stories that can be completed in short sprints of approximately two weeks. For example, the team may decide to automate the extraction of user lists for three applications in the first sprint (**figure 2**), fully knowing that this is only the first of several steps in the overall termination testing process. These bite-size stories can yield results in a relatively short period. If any of them fail, the project team knows within the sprint period (known as "failing fast") and can quickly pivot. This is a huge benefit of Agile (failures are still counted as results). Week after week, the team keeps learning and pivoting by focusing on specific outcomes.

> "IDENTIFYING TIME-BOUND STORIES KEEPS THE PROJECT TEAM FROM GOING INTO THE "BACK ROOM" FOR MONTHS AND EMERGING WITH AN UNEXPECTED RESULT (GOOD OR BAD)."

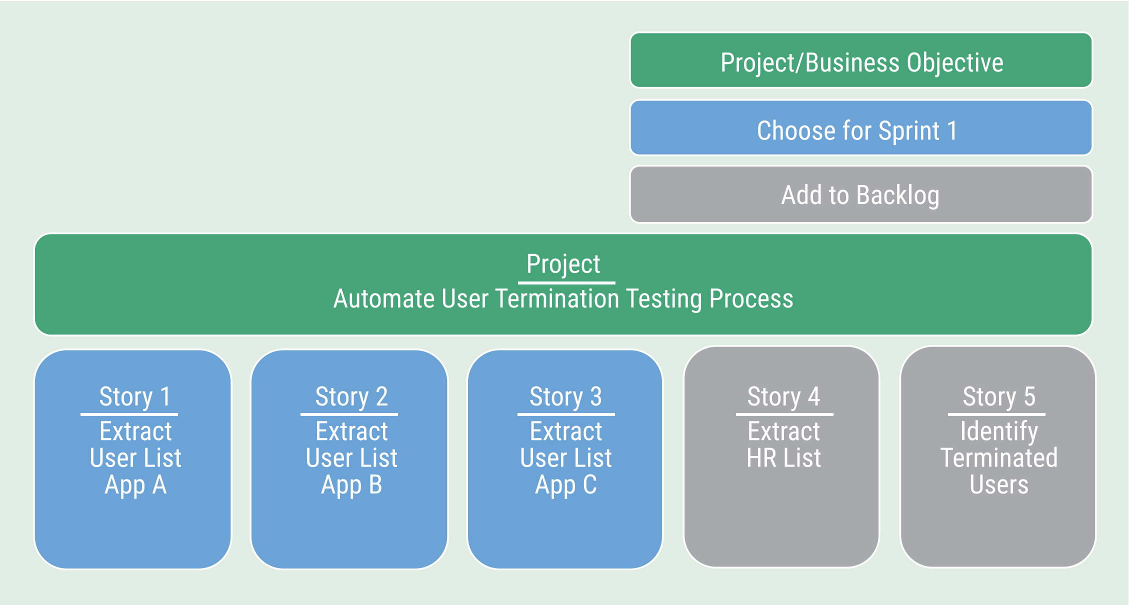
After dividing the project into stories and selecting the stories to target in the first sprint, the Agile approach moves to step 2: Meet regularly. At this point, the new scrum master is tasked with organizing daily "stand-ups" to evaluate the progress from the previous day, quickly identifying and resolving any roadblocks with the development team. The term "stand-up" is important; attendees at these meetings actually stand, providing the incentive to keep the meeting short and to the point. (Of course, adjustments should be made to accommodate team members with different physical needs.) This is not a meeting for everyone on the team; it is a meeting where the project development team can focus on the assigned work and avoid digressions from the product owner that are better handled during sprint planning and the gathering of story requirements. This is also not the time to do a project deep dive. The meetings allow the scrum master to identify whether team members are being pulled in other directions or key stakeholders are not cooperating—directly related to the team's ability to address the goal of delivering benefits on time and on budget. IA professionals have been waiting almost a decade for better success in delivering digital capabilities, so they are depending on scrum masters to hold them accountable for prioritizing this project. Success does not happen by accident.

At the closure of every sprint, it is important to execute step 3—review and celebrate—sometimes called a retrospective. This meeting should be facilitated by the scrum master and attended by the development team, product owner and other

Enjoying this article?

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

Figure 2—Sample Stories



stakeholders. During the meeting, the team reviews the completed stories and shares lessons learned along the way. This is an opportunity to identify any key insights that can be applied to future stories. For example, perhaps the team delivering automation for five applications identified a tool near the end of story development that might be more efficient than the one originally selected. By recognizing this after the completion of only five applications, rather than working on the whole suite of applications, the team can adapt and proactively pivot before automating other applications in future stories. Another feature of this approach is being able to ask questions early. Do team members understand how an application was built, and will the team be able to use it after a key developer leaves? This review gives stakeholders the opportunity to ask key questions that might spark better approaches in subsequent sprints and provides shared ownership of the outcome. The "celebrate" part of this step gives leadership the opportunity to recognize the contributions of the development and testing teams and encourage future progress before they repeat the cycle for the next sprint. Digital transformation requires a clear and demonstrated commitment from leadership, as lasting change has a material impact on people, process and technology.

Although the foundation layer of the model—to provide tools—is not specific to Agile, it was identified by PMI as a key project performance factor. The accounting team would not be asked to give up its enterprise resource planning (ERP) and book journal entries in Excel. Similarly, the IT team should use an Agile software development program to prioritize and collaborate, not Excel project trackers; IT professionals should use a data analytics program for analyzing data sets, not Vlookups. Beyond the basic audit documentation infrastructure, the team needs analytic tools to identify and develop stories. A US$2,000 software license sounds like a lot, but it is minuscule compared to the time saved when audit teams utilize the right prioritization, delivery framework and tools. However, simply funding the team may not be enough. The leader may need to support the team through the bureaucracy of the

> "ALTHOUGH THE FOUNDATION LAYER OF THE MODEL—TO PROVIDE TOOLS—IS NOT SPECIFIC TO AGILE, IT WAS IDENTIFIED BY PMI AS A KEY PROJECT PERFORMANCE FACTOR."

enterprise's purchasing department. The good news is that the team's IT organization may already have these tools or a signed contract to procure them. This may be the best starting point to identify tools that can be acquired quickly.

Conclusion

Even after applying all the elements of the Agile model, there is no guarantee of a successful digital audit transformation project. However, executing according to Agile with discipline will result in more transparent week-to-week progress and faster identification of problems. It cannot be overstated that applying digital transformation is not a one-and-done project. Systems and their respective databases within the enterprise are constantly changing, and teams must be able to react quickly to these changes. The value of Agile is not limited to completing long-awaited RPA and data analytics projects; Agile is an operating procedure with the reactiveness to keep up with the rest of the enterprise and allow IA to lead by example.

Author's Note

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

> “EXECUTING ACCORDING TO AGILE WITH DISCIPLINE WILL RESULT IN MORE TRANSPARENT WEEK-TO-WEEK PROGRESS AND FASTER IDENTIFICATION OF PROBLEMS.”

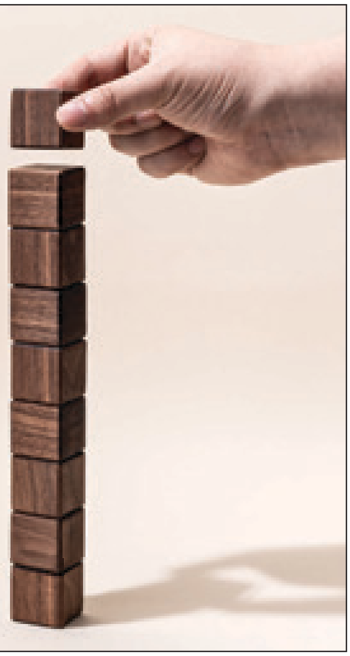
Endnotes

[1] PricewaterhouseCoopers, *2011 State of the Internal Audit Profession Study*, USA, 2011, *www.utsystem.edu/sites/default/files/offices/system-audit/state-of-internal-audit-profession-study-2011.pdf*

[2] PricewaterhouseCoopers, *2019 State of the Internal Audit Profession Study*, USA, 2019, *https://www.pwc.com/us/en/services/risk-assurance/library/assets/pwc-2019-state-of-the-internal-audit.pdf*

[3] Discenza, R.; J. B. Forman; “Seven Causes of Project Failure,” Project Management Institute (PMI), 2007, *https://www.pmi.org/learning/library/seven-causes-project-failure-initiate-recovery-7195*

[4] Sanders, C.; “Launching a Value-Based Analytics and RPA Program,” *ISACA® Journal*, vol. 6, 2018, *https://www.isaca.org/archives*



Emerging Technologies Do Not Call for Emerging Cybersecurity

The world is undergoing constant transformation, and IT is the powerhouse of this process. Data are produced in high volumes every day, and the pace is increasing in areas such as social media, for example, which has evolved from text to images and from images to videos and soon will move from videos to augmented reality (AR) and virtual reality (VR).

Today's emerging technologies shape the way people live and work as cloud computing, the Internet of Things (IoT), blockchain, robotic process automation (RPA), machine learning (ML) and artificial intelligence (AI) solutions sprout up in the marketplace.[1] New attack formats such as Ransomware as a Service (RaaS) are also following the technology evolution.

Emerging technologies are changing the business landscape and, therefore, cybersecurity needs to be reexamined.

Demetrio Carrión, CISA, CRISC, CISM, CISSP, PMP
Is the Latin America south cybersecurity leader at EY Brazil. He is a seasoned cyberprofessional with more than 20 years of experience, 15 of them working at EY. Carrión has received two ISACA® awards for achieving the highest grade on the 2007 Certified Information Security Manager® (CISM®) exam and the second highest grade on the 2006 Certified Information Systems Auditor® (CISA®) exam in the South/Central America region.

When it comes to cybersecurity and privacy, there are two groups with which to be concerned:

- **Cyberalchemists**—Those who believe new technologies are the key to turning an insecure world into a secure one just by the fact that they exist[2]
- **Cyberrevolutionaries**—Those who believe cybersecurity must be rebuilt from the ground up and changed in the same way emerging technologies change the world

There is a need for a third group of cybersecurity and privacy professionals who recognize that the IT landscape is ever evolving, yet the fundamentals remain the same. A threat is a threat, a vulnerability is a vulnerability, data are data, and cybersecurity professionals are still protecting the confidentiality, integrity and availability of data and privacy of all people.

On Cyberalchemists

People do not always have good memories. As a matter of fact, they sometimes create memories to support their beliefs and arguments or fill a gap in their recollection of a fact.[3] This supports the ideas of cyberalchemists because they do not create a bridge between the past and the future.

Cyberalchemists see technology as a miracle, and they do not focus on the fact that today's technology is yesterday's emerging technology. Because they forget to make this connection, they turn a blind eye to cyber and privacy incidents and breaches that affect emerging technologies such as the cloud, IoT, blockchain, AI, wearables and implantables.

There is an abundance of examples of cyberincidents targeting emerging technologies such as instances of information inadvertently leaked from cloud storage,[4] double extortion, finance spear phishing, IoT abuse and implantables manipulation.

Despite all the good intentions in creating new products, vulnerabilities exist, and there will always be actors willing to exploit them.

Most of the time, cybersecurity and privacy are not built by design but by default, leading to software and hardware with dozens to thousands and even millions of vulnerabilities. Even if a vendor considers cyber and privacy by design in its engineering processes, experience backs a view that bugs will be present. However, in most cases, fewer vulnerabilities will be present when compared to an engineering process without a cyber-by-design approach. But vulnerabilities will be there to be exploited.

If someone designs and develops a vulnerability-free software, people will find ways to run the software on faulty platforms, people will configure the software with insecure options and software may connect with other applications in ways not anticipated during its design phase.

People are not machines and cannot be built with a cyber-by-design approach in mind (at least not yet). People choose weak passwords; make poor judgments regarding risk;[5] are not able to act on every single alarm, incident or threat;[6] and tend to value performance over security and features over privacy.

On Cyberrevolutionaries

If past cybersecurity and privacy initiatives did not make us safer, why would they be able to build a safer future? Cyberrevolutionaries speculate that old solutions are not suited to cope with the emergence of the bright, new world. Their core beliefs are:

- Threats are constantly changing and spreading across industries.
- The amount of information is insurmountable.
- AI is spreading at a fast pace.
- The cloud is not under anyone's control.

In summary, the new world is practically detached from yesterday's world.

It is important to recognize the cyberrevolutionaries' narrative is valid, is based on facts and presents the world as it is. Nonetheless, they do not present a compelling reason as to why privacy and cyberfundamentals should be thrown away and new ones built.

> A FRAMEWORK ALONE WILL NOT CREATE A CYBER-READY ENTERPRISE OR PRODUCT.

When looking at the big picture, there are still the same challenges: unpatched systems, weak passwords, unsecure configurations and software, privacy and cybersecurity bolted on instead of built in, and a myriad of well-known controls vastly documented in OWASP Top 10[7] and the 20 CIS Controls and Resources.[8]

The More Things Change, the More They Remain the Same

It is important to avoid the extremes. The fundamentals are good, and technologies are not bulletproof.

Cybersecurity professionals should rely on the rock-solid cybersecurity/privacy frameworks and bodies of knowledge and standards to support them when deciding to evaluate, implement or audit emerging technologies.

The US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), International Organization for Standardization (ISO) ISO 27000 standards, (ISC)^2 Body of Knowledge and ISACA® auditing guidelines have been around for quite a while, and cybersecurity professionals still fail to fully implement these concepts and controls.

Why should practitioners rely on them? They are trustworthy sources in that:

- They stand the test of time. Their fundamentals are valid today and will be in the future.
- They are acknowledged by professionals, organizations and institutions.
- They are thorough and avoid blind spots.
- They are risk based.
- They are integrators providing a common taxonomy.

Enjoying this article?

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

However, a framework alone will not create a cyber-ready enterprise or product. It is paramount to keep things simple and base the design, integration, execution and auditing on the confidentiality, integrity, availability and privacy (CIAP) and people, processes and technologies (PPT) models.

Every time a complex problem arises, cybersecurity professionals should refer to CIAP and PPT. CIAP goes directly to the core questions: What is it that is being protected? How does this solution support achieving CIAP?

For example, complying with a privacy law such as the EU General Data Protection Regulation (GDPR) or the Brazilian Lei Geral de Proteção de Dados (LGDP) can be very complex, and it is easy to get caught up in discussions that focus on choosing technology A over B based on someone's ranked list rather than solving the issue.

Practitioners must focus more on the risk at hand instead of software features. Any solution should be a proportioned response to the risk an organization is entitled to manage and not an end in itself.

Many people used to think that GDPR/LGPD translated into cryptography and data anonymization. This is far from true. It is important to not lose sight of the challenge or issue that is really being faced: getting back to the fundamentals.

> “EMERGING TECHNOLOGIES DEFY THE STATUS QUO AND THERE IS NOT AN EXTENSIVE BODY OF KNOWLEDGE ON HOW TO ADDRESS THEM.”

Avoiding Common Errors

Emerging technologies defy the status quo and there is not an extensive body of knowledge on how to address them. There are not a lot of success cases to back implementation, execution and auditing approaches, and there is sometimes a shortage of skilled professionals to help with this process as the technologies themselves are new and new ways of using them are being created on the fly.

There are several common pitfalls to avoid, though this list is not exhaustive:

- **Security and privacy must not be taken for granted.** On the contrary, because a technology is new, it must be tested and scrutinized.
- **Smooth and secure integrations must not be taken for granted.** Emerging technologies may have been built to seamlessly integrate with legacy protocols and systems, but that is not always the case. Legacy systems may need to be patched, and inline solutions may need to be created to integrate emerging technologies with old ones.
- **Cyber and privacy diligence and awareness must not be taken for granted.** Even if new technology is created to avoid past vulnerabilities, someone could still choose a poor password, fall victim to a social engineering attack or forget to revoke an access. Even after years and years, it is still customary to complete an audit and find weak passwords, IoT devices without secure passwords and protocols, applications with default passwords, and other much-discussed lack of controls.
- **Testing and auditing must not be taken for granted.** Many cybersecurity professionals may rely on a big cloud provider running continuous testing and auditing on their services and products, for example. However, it is important to take into consideration that software fails, robots break and technology might operate differently in less than ideal situations. In this example, the big cloud provider's internal procedures are just one of the protection layers. Cybersecurity and privacy practitioners should add other testing and auditing layers customized to their organizations' needs and operations.

Conclusion

Emerging technologies should be leveraged for the enterprise's benefit, and the audit plans, framework and body of knowledge established and designed by the cyber and privacy community should be used for the good of society.

Dealing with emerging technologies is challenging because of their novelty, but there are shortcuts to ease the work, such as:

- Leveraging cybersecurity and privacy frameworks, standards and bodies of knowledge
- Keeping it simple by basing solutions on fundamentals (CIAP and PPT)
- Not taking cybersecurity and privacy for granted in emerging technologies

Endnotes

[1] Schwab, K.; *The Fourth Industrial Revolution*, Crown Business, USA, 2017

[2] Alchemists, among other things, attempted to transform mercury into gold. The substance capable of transmuting one metal into a noble metal was called the "philosophers' stone."

[3] Loftus, E.; "Creating False Memories," *Scientific American*, vol. 277, iss. 3, 1997, p. 70–75, *https://staff.washington.edu/eloftus/Articles/sciam.htm*

[4] Morris, B.; "More Keys Than a Piano: Finding Secrets in Publicly Exposed EBS Volumes," DEF CON 27, Las Vegas, Nevada, USA, 8–11 August 2019, *https://www.defcon.org/html/defcon-27/dc-27-speakers.html#Morris*

[5] Schneier, B.; "Perceived Risk vs. Actual Risk," Schneier on Security, 3 November 2006, *https://www.schneier.com/blog/archives/2006/11/perceived_risk_2.html*

[6] Carlson, D.; "Maximize Your Security Operations Center Efficiency With Incident Response Orchestration," *Security Intelligence*, 9 January 2019, *https://securityintelligence.com/maximize-your-security-operations-center-efficiency-with-incident-response-orchestration/*

[7] Open Web Application Security Project (OWASP), OWASP Top 10, *https://owasp.org/www-project-top-ten/*

[8] Center for Internet Security (CIS), The 20 CIS Controls and Resources, *https://www.cisecurity.org/controls/cis-controls-list/*

CASE STUDY

How FAIR Risk Quantification Enables Information Security Decisions at Swisscom

Swisscom is Switzerland's leading telecom provider. Due to strategic, operational and regulatory requirements, Swisscom Security Function (known internally as Group Security) has implemented quantitative risk analysis using Factor Analysis of Information Risk (FAIR). Over time, Swisscom's FAIR implementation has enabled Group Security to objectively assess, measure and aggregate security risk. Along the way, Swisscom's Laura Voicu, a senior security architect, has led the Swisscom security risk initiative.

Introduction

Information risk is the reason businesses have security programs, and a risk management process can be a core security program enabler. With an effective risk program, business risk owners are well-informed about risk areas and take accountability for them. They are able to integrate risk considerations into managing value-producing business processes and strategies. They can express their risk tolerance (i.e., appetite) to technical and operational teams and, at a high level, direct the risk treatment strategies those teams take.

Most organizations now operate as digital businesses with a high reliance on IT. They can benefit by shifting the corporate culture from one that focuses on meeting IT compliance obligations to one that targets overall risk reduction. Visibility into the overall security of the organization plays an important role in establishing this new dialog. Security leaders can prioritize their security initiatives based on the top risk areas that an organization faces.

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.

Laura Voicu, Ph.D.
Is an experienced and passionate enterprise architect with more than 10 years of experience in telecommunication and other industries. She is a leader in enterprise and data architecture, cybersecurity and quantitative risk analysis. Her latest passion is data science and driving innovation with a focus on big data and machine learning. Voicu frequently presents at conferences and volunteers as an ISACA SheLeadsTech Ambassador.

Swisscom uses quantifiable risk management enabled through Open FAIR to:

- Communicate security risk to the business
- Ascertain business risk appetites and improve business owner accountability for risk
- Prioritize risk mitigation resources based on business impact
- Calculate the return on investment (ROI) of security initiatives
- Meet new and more stringent regulatory requirements

Company Background

Swisscom is the leading telecom provider in Switzerland and one of its foremost IT companies, headquartered in Ittigen, near the capital city of Bern. In 2019, 19,300 employees generated sales of CHF 11,453 (USD $12,490) million. It is 51 percent confederation-owned and is considered one of Switzerland's most sustainable and innovative companies. Swisscom offers mobile telecommunications, fixed network, Internet, digital TV solutions and IT services for business and residential customers. Swisscom's Group Security, which is a centrally managed function at Swisscom, provides policies and standards for all lines of business, while allowing each business to operate independently.

> “WHATEVER ITS MANY BENEFITS, DIGITIZATION IN THE VIRTUAL WORLD ALSO HAS A DARKER SIDE AND ORGANIZATIONS ARE FACING NEW KINDS OF RISK.”

Digitization, changing customer requirements, predatory competition in the saturated core market and new providers with disruptive business models put the business under pressure. The long-term corporate strategy aims to compensate for the decline in revenue and profit, thus maintaining the financial strength to invest heavily in new technologies. Whatever its many benefits, digitization in the virtual world also has a darker side and organizations are facing new kinds of risk. Therefore, Swisscom defined security as one of its strategic capabilities, and having a risk-based decision-making capability is a critical success factor.

Qualitative Risk Analysis Pain Points

Prior to 2019, Swisscom managed and assessed information risk using qualitative analysis methods. The process was well-suited to quick decisions and easy to communicate with a visually appealing heat map. However, the Swisscom security team identified several fundamental flaws, including bias, ambiguity in meaning (e.g., What does "red” or “high" really mean?) and a probability that the person doing the measurement had not taken the time to clearly define what it is he or she just measured.

For reference, **figure 1** illustrates a sample 5x5 heat map plotting nine risk areas (R1 to R9) on a graph where the vertical access plots the probability of a risk materializing and the horizontal access plots the hypothetical impact.

Risk Terminology

- **Risk (per FAIR)**—The probable frequency and probable magnitude of future loss
- **Open FAIR**—Factor Analysis of Risk (as standardized by The Open Group)
- **Information risk**—Risk of business losses due to IT operational or cybersecurity events
- **Qualitative risk analysis**—The practice of rating risk on ordinal scales, such as 1 equals low risk, 2 equals medium risk or 3 equals high risk
- **Quantitative risk analysis**—The practice of assigning quantitative values, such as number of times per year for likelihood or frequency, and mapping impact to monetary values
- **Enterprise risk management**—The methods and processes used by organizations to manage the business risk universe (e.g., financial, operational, market) as well as to seize opportunities related to the achievement of their objectives

Enjoying this article?

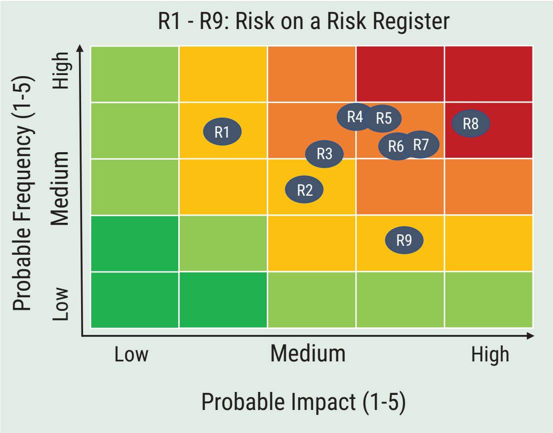
- Read *Risk IT Practitioner Guide, 2nd Edition. www.isaca.org/risk-it-pg2*
- Learn more about, discuss and collaborate on risk and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Inconsistent Risk Estimates

Qualitative risk estimates tended to be calculated in an inconsistent manner and were often found to be unhelpful. Because analysts did not use a rigorous risk quantification model such as FAIR to rate risk, they relied on the mental models or years of habit.

Early staff experiments with quantifying security risk also failed; per a senior security officer at Swisscom, the reasons for this were, "Too little transparency and too many assumptions. In short: a constant discussion about the evaluation method and not about the risk itself."

Figure 1—Qualitative Risk Estimates Graphed as a Heat Map



Too Many "Mediums"

Odd things happened: Virtually all risk areas were rated "medium." A high rating is a strong statement and draws unwanted attention to the risk from business management, who might then demand some strong justification for the rating. A low rating would look foolish if something bad actually happened. Rating risk "medium" equals the safe way out.

Inability to Prioritize Risk Issues

Although utilizing qualitative methods may provide some prioritization capability (a risk rated red is some degree worse than one rated yellow), Swisscom had no way of economically evaluating the difference between a red and yellow, between one red or two yellows, or even between two yellows such as R1 and R9 as shown in **figure 1**. In short, Swisscom had poor visibility into the security risk landscape, thus potentially misprioritizing critical issues. Over time, Swisscom staff came to share the FAIR practitioner community objections articulated in the article "Thirteen Reasons Why Heat Maps Must Die."[1]

Demand for More Accurate Risk Assessments After a Breach

In 2018, Swisscom went public to announce a large data breach. Swisscom took immediate action to tighten the internal security measures to prevent such an incident from happening again. Further precautions were introduced in the course of the year.

Following the data breach, Swisscom IT and security executives sought to improve the risk assessment process. Staff had made early attempts to quantify security risk using single numerical values, or single-point estimates of risk by assigning values for discrete scenarios to see what the outcome might be in each. This technique provided little visibility into the uncertainty and variability surrounding the risk estimate.

Establishing a Quantitative Risk Analysis Program

Swisscom's Group Security team learned about FAIR in 2018 and became convinced that its model was superior to in-house risk quantification approaches that the team had attempted to use in the past. FAIR allows security professionals to present estimates of risk (or loss exposure) that show decision-makers a range of probable outcomes. Using ranges brings a higher degree of accuracy to estimates with enough precision to be useful.

> " FAIR ALLOWS SECURITY PROFESSIONALS TO PRESENT ESTIMATES OF RISK (OR LOSS EXPOSURE) THAT SHOW DECISION-MAKERS A RANGE OF PROBABLE OUTCOMES. "

The decision was made to use FAIR in 2018 and Senior Security Architect Laura Voicu was assigned to lead a core team of a few part-time FAIR practitioners. The risk project's initial phase was to define risk scenarios in a consistent manner throughout Swisscom. As result of this work effort, the team produced a formal definition and consistent structure for normalizing risk register entries into FAIR-compliant nomenclature, shown in **figure 2**.

The FAIR team performed multiple analyses and continued to deepen its experience with the quantitative approach. As a best practice, the team interviewed or held workshops with subject matter experts (SMEs) on controls, incidents, impacts and other areas representing variables in the FAIR analysis.

Starting in early 2019, a small group of stakeholders within the security organization conducted a proof of concept (POC) to perform assessments of the customer portal data breach risk, risk associated with different cloud workload migration strategies, outage of systems or networks due to ransomware and, recently, remote working use cases to continue operating amid the COVID-19 disruption.

In parallel, Group Security defined roles, analysis processes and risk management processes. The team defined the following roles:

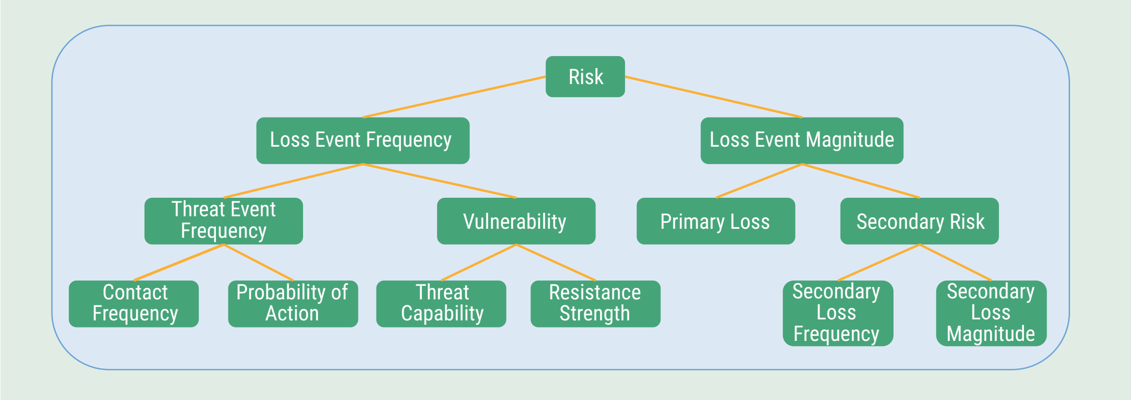
- **Risk reporters**—Security professionals who help identify and report security risk. Risk reporters work interdepartmentally to identify, assess and reduce security risk factors by recommending specific measures that can improve the overall security posture. They also have the overall responsibility to oversee the coordinated activities to direct and control risk.
- **Risk owners**—Business owners and operations managers who manage the security risk scenarios that exist within their business areas. They are responsible for implementing corrective actions to address process and control deficiencies, and for maintaining effective controls on a day-to-day basis. They assume ownership, responsibility and accountability for directly controlling and mitigating risk.

> “THE RISK ANALYSIS PROCESSES NORMALIZE RISK SCENARIOS INTO THE FAIR MODEL, PRIORITIZE THEM AND ASSESS THE ACTUAL FINANCIAL LOSS EXPOSURE ASSOCIATED WITH EACH RISK SCENARIO.”

The team also established the following processes:

- **Identification**—Uncover the risk factors (or potential loss events) and define them in a detailed, structured format. Assign ownership to the areas of risk.
- **Assessment**—Assess the probable frequency of risk occurrence, and the probable impacts. This helps prioritize risk. It also enables comparison of risk relative to each other and against the organization’s risk appetite.
- **Response**—Define an approach for treating each assessed risk factor. Some may require no actions and only need to be monitored. Other risk factors considered unacceptable require an action plan to avoid, reduce or transfer them.

Figure 2—Open FAIR Risk Ontology



- **Monitoring and reporting**—Reporting is a core part of driving decision-making in effective risk management. It enables transparent communication to the appropriate levels (according to Swisscom's internal rules of procedure and accountability) of the net or residual risk.

Thus, the risk analysis processes normalize risk scenarios into the FAIR model, prioritize them and assess the actual financial loss exposure associated with each risk scenario. In parallel to the strategic risk analysis of the top risk areas, the FAIR team can also provide objective analysis to support tactical day-to-day risk or spending decisions. These analyses can help assess the significance of individual audit findings and efficacy of given controls, and can also justify investments and resource allocations based on cost-benefit.

The FAIR team is constantly improving and simplifying the process of conducting quantitative risk assessments using the FAIR methodology. In a workshop-based approach, the team tries to understand the people, processes and technologies that pose a risk to the business.

Ongoing Work Items

As of early 2020, Swisscom's core FAIR team consists of three part-time staff members. This team is part of a virtual community of practitioners concerned with security risk management in the company.

The team continues to drive the following work items:

- Risk scenario analysis
- Risk scenario reporting
- Risk portfolio analysis and reporting
- Internal training
- Improving the tool chain
- Improving risk assessment processes

Risk Scenario Analysis

The FAIR team performs the deep analysis of risk scenarios using an open-source tool adapted for Swisscom's use. Based on the analysis, it provides quantitative estimates for discussion with risk, IT and business analysts (**figure 3**).

Figure 3's loss exceedance curve depicts a common visualization of FAIR risk analysis output. The Y axis, Probability of Loss or Greater, shows the percentage of Monte Carlo simulations that resulted in a loss exposure greater than the financial loss amount on the X axis. Each Monte Carlo simulation is like a combination of random coin tosses of all the risk components of the FAIR risk ontology shown in **figure 2**. During the analysis, the FAIR team generates calibrated estimates for the range of values for each risk component. A calibrated estimate is an SME's best estimate of the minimum, maximum and most likely probability of the risk factor. Each estimated risk factor in the ontology is fed into the Monte Carlo simulation by the FAIR tool.

> “THE FAIR TEAM PERFORMS THE DEEP ANALYSIS OF RISK SCENARIOS USING AN OPEN-SOURCE TOOL ADAPTED FOR SWISSCOM'S USE.”

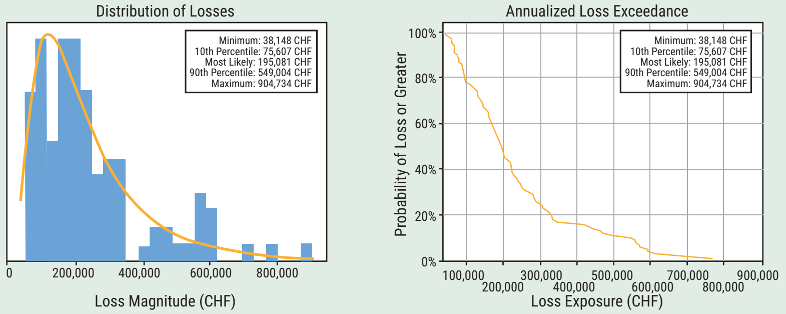
Although the SMEs tend to provide fact-based, objective information for use in estimates to the best of their abilities, challenges can arise when presenting initial completed analyses to stakeholders.

“Risk owners tend to want to push the numbers down, but security leaders try to keep them up,” Voicu explained.

Often, however, the stakeholders can meet in the middle for a consensus and come together on risk treatment proposals with a strong return on security investment (ROSI) measured by the difference between the inherent risk analysis and the residual risk analysis.

In the case of the customer portal data breach scenario, the FAIR team and the business stakeholders agreed on adding two-factor authentication (2FA) for portal users. This solution had a low cost because Swisscom already possessed the 2FA capability and needed only to change the default policy configuration to require 2FA. **Figure 5** shows a diagram of the current (or inherent) vs. residual risk analysis amounts using

Figure 3—Results of a FAIR Analysis



Annualized View

Per-Event View

Per-Event Primary Losses			
	Min	ML	Max
Loss Events/year	0	0.3	1
Loss Magnitude	18,048	50,200	104,734
Vulnerability			**81.76%**

Per-Event Secondary Losses			
	Min	ML	Max
Loss Events/year	0	0.07	1
Loss Magnitude	20,100	144,881	800,000
Total Single Loss Event	**38,148**	**195,081**	**904,734**

fictional numbers aligned with the assessment shown in **figure 4**. The current risk depicts the amount of risk estimated to exist without adding new controls to the current state. The residual risk shows the amount of risk estimated to exist after the hypothetical addition of the new 2FA control.

Risk Scenario Reporting

Once the analysts reach a consensus on estimates during working meetings, the FAIR team provides management reports using one-page summaries with quantitatively scaled, red-yellow-green diagrams based on the risk thresholds (i.e., risk appetite) of the risk owner (**figure 4**). The Swisscom FAIR team has found that often management trusts the teams' analysis and does not want to see the FAIR details. However, the numerical analysis drill-down is available if management wishes to understand or question the risk ratings and recommendations.

Risk Portfolio Analysis and Reporting

Strategic risk analyses are typically driven by boards and C-level executives with the intent of understanding, communicating and managing security risk holistically and from a business perspective. This enables executives to define their risk appetite and boards to approve it. The organization can also right-size security budgets, prioritize risk mitigation initiatives and accept certain levels of risk. Strategic risk analyses conducted by the FAIR team can be used to measure risk trending over time. The FAIR team began providing a strategic risk analysis report on a quarterly basis to the board of directors in early 2020. **Figure 6** provides an example.

Internal Training

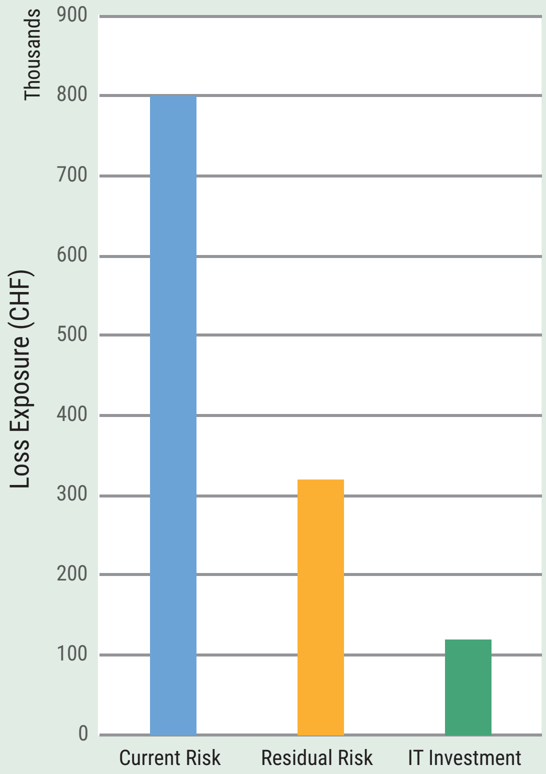
The team began by socializing FAIR concepts among the cybersecurity functions and other internal groups to establish a broader FAIR adoption. The team provided workshops and training for additional security staff as well as stakeholders and aims to further extend training offerings.

Improving the Tool Chain

Swisscom has assessed several FAIR risk quantification tools:

- **Basic risk analysis**—Pen and paper, qualitative method using *Measuring and Managing Information Risk: A FAIR Approach*[2]
- **FAIR-U**—Free, basic version of RiskLens. For noncommercial use only. Registration required.
- **RiskLens**—Commercial, fee-based FAIR application
- **Evaluator**—Free open-source application, OpenFAIR implementation built and run on R + Shiny

Figure 4—Risk Treatment Evaluation



CHF 480,000 Average Risk Reduction
CHF 120,000 IT Investment

Figure 5—One-Page Summary Risk Report

RISK-00000—Data Breach Customer Data on Swisscom Customer Portal

Risk Scenario Description:
Data loss/data breach of sensitive customer data (e.g., customer data records, billing information) due to weak authentication (username and password). Potential violation of legal and regulatory requirements according to DSG and FMG as well as contractual infringement (compliance).

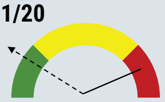
Risk Owner: Customer Portal Product Owner
Security Responsible: Security Officer Residential Customers

Status Measures: On track

- ◑ Monitoring access control
- ◑ Regulating access rate (throttling)
- ◑ Verification of external employees (Identity management)

○ Not started ◑ In Progress ● Implemented

Target: Q1/20



Value at risk

Financial	🔴	🔴	🔴	🔴
Regulatory	🔴	🔴	🔴	⚪
Reputation	🔴	⚪	⚪	⚪

Business unit at risk

Primary	**Residential customers**
Secondary	n/a

Assets at risk

Confidentiality	🔴
Integrity	⚪
Availability	⚪
Safety	⚪

Ease of exploitability

Insider	🔴	🔴	🔴	⚪
External attacks	🔴	⚪	⚪	⚪

Risk mitigation strategy

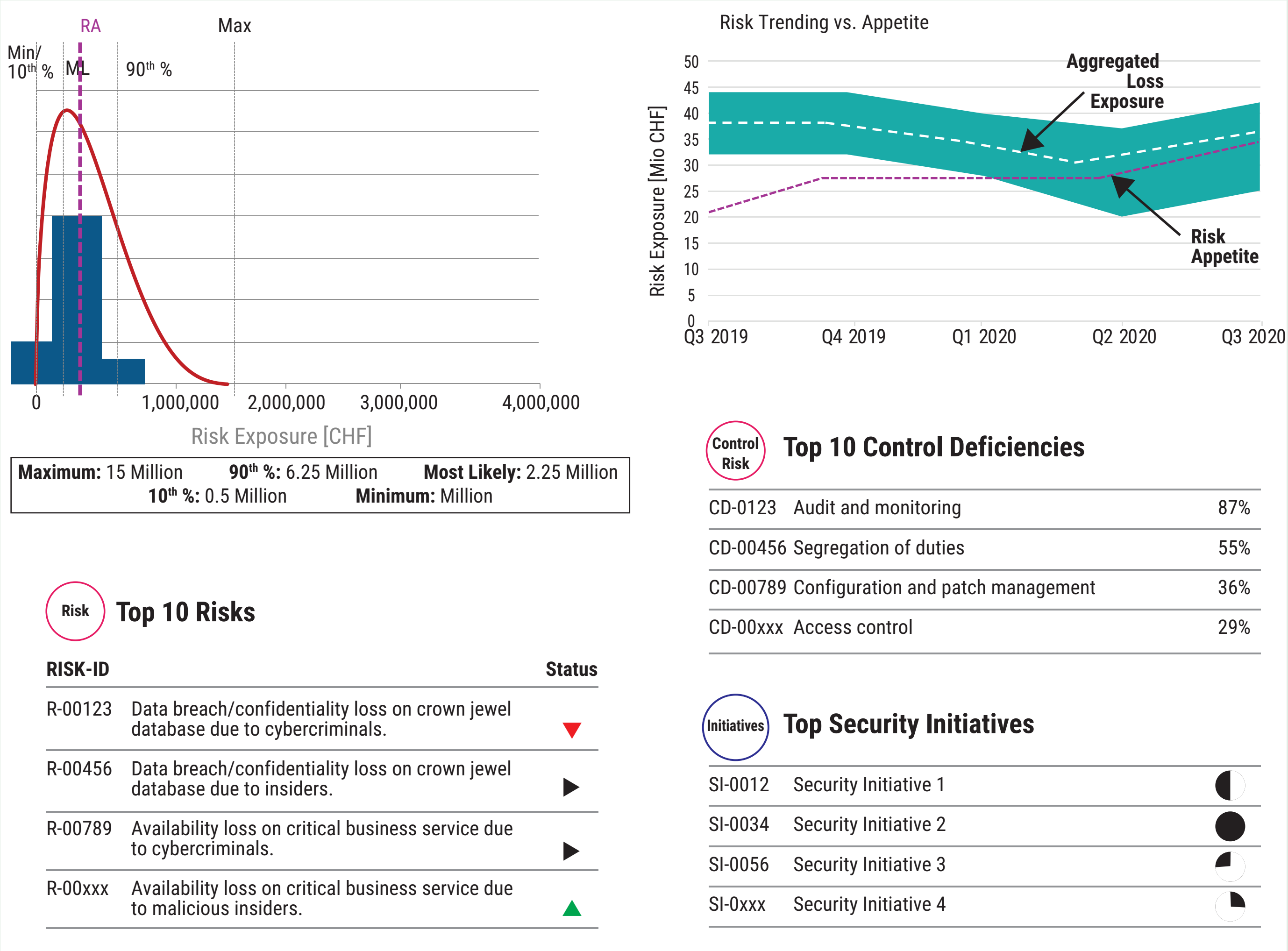
Avoid	⚪	Reduce	🔴
Accept	⚪	Transfer	⚪

- **PyFair**—FAIR implementation built on Python
- **FAIR Tool**—Free open-source application built on R + Shiny
- **OpenFAIR Risk Analysis Tool**—OpenGroup's Excel-based application. Registration required.
- **RiskQuant**—Open-source application built in Python

In the end, Swisscom has opted for developing the tool in-house by adapting the RiskQuant analysis module. Swisscom is improving the tool chain by enhancing the analysis module with reporting capabilities and multiscenario aggregated analyses capabilities. The in-house tool is designed to support the entire security risk management life cycle—from risk identification and scoping to risk analysis and prioritization to the evaluation of risk mitigation options to risk reporting. The team is progressively adding additional modules to the in-house tool, such as:

- **Decision support**—Enabling decisions on the best risk mitigation options based on their effectiveness in reducing financial loss exposure. The tool already provides the capability for conducting comparative and cost-benefit analyses to assess what changes in security strategy or what risk mitigation options provide the best ROI.
- **Security data warehouse**—Swisscom's existing security data warehouse defines, stores and manages critical assets in a central location. Risk tools can leverage this information in risk

Figure 6—Risk Portfolio Reporting



Maximum: 15 Million **90th %:** 6.25 Million **Most Likely:** 2.25 Million
10th %: 0.5 Million **Minimum:** Million

Top 10 Risks

RISK-ID		Status
R-00123	Data breach/confidentiality loss on crown jewel database due to cybercriminals.	▼
R-00456	Data breach/confidentiality loss on crown jewel database due to insiders.	▶
R-00789	Availability loss on critical business service due to cybercriminals.	▶
R-00xxx	Availability loss on critical business service due to malicious insiders.	▲

Top 10 Control Deficiencies

CD-0123	Audit and monitoring	87%
CD-00456	Segregation of duties	55%
CD-00789	Configuration and patch management	36%
CD-00xxx	Access control	29%

Top Security Initiatives

SI-0012	Security Initiative 1	◐
SI-0034	Security Initiative 2	●
SI-0056	Security Initiative 3	◔
SI-0xxx	Security Initiative 4	◔

> “WHAT STARTED AS A SHORT-TERM OPPORTUNITY TO NORMALIZE AND PRIORITIZE RISK TURNED INTO A LONG-TERM JOURNEY TO MANAGE A PORTFOLIO OF SECURITY INVESTMENTS.”

scenarios related to assets. Stakeholders can also view the risk areas and issues associated with their assets and understand the risk posture on a continuous basis.

- **Risk portfolio**—The module aims to provide a deeper understanding of enterprise risk as well as aggregate or portfolio views of risk across business units. This module will also allow Swisscom to set key metrics to measure and manage cyberrisk, such as risk appetite, and conduct enterprise-level what-if analyses.

Improving Risk Assessment Processes

To enhance Swisscom’s ability to identify risk scenarios deserving full FAIR analyses, the FAIR team is creating a triage questionnaire that will enable IT and security staff to perform a quick assessment of issues before submitting them as risk areas for analysis. The triage consists of 10 yes-or-no questions and requires less than 15 minutes to complete.

Lessons Learned

It is instructive to review lessons learned after establishing a risk program:

- **Bring the discussion to the business owners of the risk and the budget.** Prior to the FAIR program, the risk acceptance process was not formally aligned to Swisscom’s rules of procedures and accountability. These rules provide a process whereby executives are authorized to accept risk up to certain levels, and how to decide whether higher risk can be accepted. When the FAIR program was introduced, Swisscom began identifying the executives who will end up covering the losses if risk scenarios actually materialize. With very rare exceptions, those identified business executives should also be responsible for owning or accepting risk.
- **Focus on the assumptions, not the numbers**. As noted earlier, risk ratings or quantities can become politicized. Some parties may desire lower or higher results depending on their own agendas. The FAIR model can act as a neutral arbiter if stakeholders understand the assumptions. Although participants in the risk process will always have agendas, focusing on assumptions puts the discussion on a more logical footing.
- **Be flexible about reporting formats.** Once risk analysts learn FAIR, there can be a temptation to take a “purist” position and evangelize the methodology too ardently. However, not all stakeholders were interested in the complexity of simulations and ontology. The Swisscom FAIR team found that the one-page risk summary using a familiar “speedometer” diagram (**figure 4**) facilitated easier acceptance of quantitative analysis results from the business risk owners. It should be noted that quantitative risk values still underlie the one-page summary. Behind the scenes, quantitative risk appetites and risk estimates determine a risk’s status as red, yellow or green.
- **Maintain momentum.** When the FAIR journey started, the project scope was fluid. The FAIR team has found that the more the scope expanded, the more resources were required to provide increasing value. What started as a short-term opportunity to normalize and prioritize risk turned into a long-term journey to manage a portfolio of security investments.

Metrics

Swisscom is currently preparing to begin tracking formal risk metrics. **Figure 7** displays planned metrics and observations on the data collected or expected at this time.

Figure 7—Swisscom Proposed Metrics

Metric	Post-FAIR Implementation
Percent of risk below/above risk appetite	Approximately 5 percent of risk above risk appetite
Percent of critical assets with loss exposure above the risk appetite	Undisclosed number has been calculated
Percent of business units covered by the security risk management process	Approximately 80 percent
Percent of large solutions and agile release trains undergoing risk assessments	Approximately 60 percent of security projects that get worked on are now validated by quantitative risk assessments
Complies with regulatory requirements (Yes/No)	Yes
Dollar value of inherent risk exposure reduction due to risk program	Swisscom has reduced millions of dollars of loss exposure by its own measurements.
Cost savings (dollar value)	Saved on canceled projects or phased-out systems
Number of trained risk specialists	8
Number of trained stakeholders conversant with the methodology	Security 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 a couple of days to two weeks depending on the scenario's scope
Number of identified control gaps or vulnerabilities contributing to top risk	Undisclosed number has been calculated
Number of top gaps resolved during reporting period	Undisclosed number has been calculated

Benefits

Swisscom considers the benefits of the FAIR process to be that the company can:

- Objectively assess information risk, which enhances the ability to approve large security initiatives
- Measure aggregated information risk exposure
- Break out risk exposure for business units, risk categories and top assets or crown jewels

Next Steps

The team is optimistic as of 2020 about the ability of the FAIR program to enable data-driven decision-making. The team is improving its risk reporting portfolio to produce reports such as the ones shown in **figure 6** both at an enterprise level and at the business unit level. The team plans to conduct ROI analyses to assess the effectiveness of security spending. It is also currently in discussions with operational risk management and enterprise risk management (ERM) functions on the possibility of expanding the use of FAIR, especially in the domain of operational availability risk.

Endnotes

1 Salah, O.; "Thirteen Reasons Why Heat Maps Must Die," FAIR Institute Blog, 28 November 2018, *https://www.fairinstitute.org/blog/13-reasons-why-heat-maps-must-die*

2 Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, United Kingdom, 2014, p. 205–214

The Role of Governance in Digital Reporting

In today's environment, decision-making has become more challenging than ever, and the ability to adapt is vital. The availability of real-time digital reports allows management to form strategies and adjust them to meet changing conditions. The foundation of such decisions, however, is the quality of the information produced and published in such reports. It is imperative that reports convey information that can drive the enterprise's objectives and actions in the right direction.

Compiling a report can be a daunting task, requiring the consideration of many factors before a final report is designed, developed and published. Compared with conventional manual reports, which are generally tied to a specific purpose such as the reporting of inventory, sales or fixed assets for a certain period, digital reporting allows the integration of multiple variables into a kind of digital dashboard, providing stakeholders with a comprehensive view of what is going on in the enterprise (**figure 1**).

Rajul Kambli, CISA, CMA
Is a business insight manager with Schlumberger and has more than 17 years of experience in global accounting, planning, budgeting project management, and financial and systems audit. Currently, he is managing a digital reporting initiative. Prior to this, he had been part of the global transformation team, conducting review and gap analysis, optimization, process improvements, and readiness assessment to deploy SAP. He has also served as finance controller for various verticals—driving compliance, liquidity generation and advising on effective cost management to business partners.

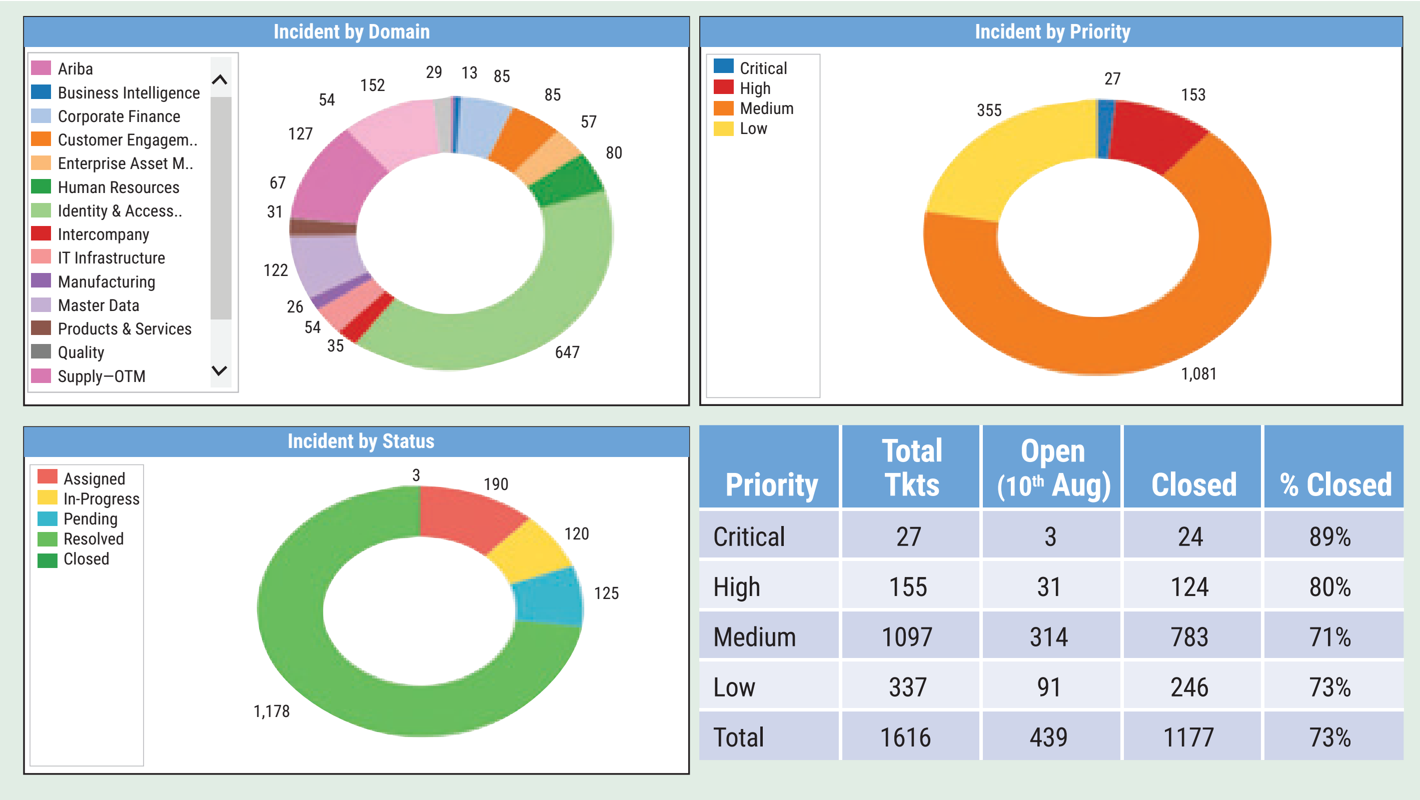
The obvious benefit of this type of digital dashboard is flexibility. In this example, it provides the overall number of incidents in each domain and divides them into critical-, high-, medium- and low-priority categories. This enables stakeholders to understand the magnitude of the problems identified and to allocate appropriate resources to address them. Similar dashboards can be conceived to track division profitability and inventory levels of aging fixed assets, which can address liquidity status.

One of the biggest advantages over manual reports is that digital reports can be linked to an auto-refresh function (**figure 2**). Such auto-refreshes can be performed in real time, for example, every hour or every day, depending on needs.

There are various factors that go into the development of a digital dashboard. These factors require the involvement and expertise of key personnel across the enterprise, in addition to the development team, which is typical of any management project. This complex development process can best be addressed by a robust governance process to ensure consistency and clarity for everyone involved.

Broadly, governance refers to the initiative to create and enforce a set of rules and policies related to a particular aspect of the enterprise. In an environment where reporting is manual, additional controls are required, primarily to limit access to data, manage how data are maintained and ensure that any changes to existing reports are approved by the appropriate authorities. In a digital reporting framework, these controls are built in, based on preapproved rules, and they can be monitored through a review of logs at predetermined intervals.

Figure 1—Digital Dashboard for Incident Tracking and Monitoring



Priority	Total Tkts	Open (10th Aug)	Closed	% Closed
Critical	27	3	24	89%
High	155	31	124	80%
Medium	1097	314	783	71%
Low	337	91	246	73%
Total	1616	439	1177	73%

Figure 2—Comparison of Manual and Digital Reporting

Manual Reporting	Digital Reporting
Manual efforts are required to access the source of the data.	Digital reporting allows for direct connection to the source of the data.
Manual efforts could result in potential errors. Validation is required to ensure integrity.	Direct connection to the data source ensures the accuracy and integrity of data, offering greater reliability.
Manual reports are subject to time lag (e.g., awaiting a bank statement to check the balance), and manual input is subject to human error.	Online refresh function provides real-time information for decision-making.
Access to paper reports is problematic for people on the move.	Access to reports through laptops, smartphones and tablets makes decision-making simpler and faster.

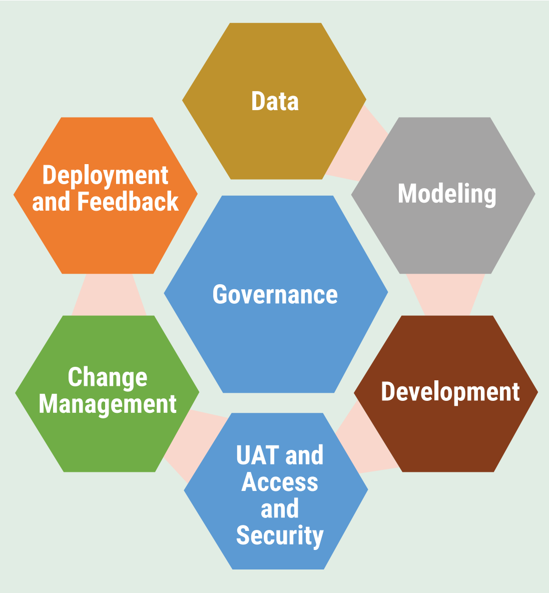
Governance clarifies each of the factors involved in developing a digital report (**figure 3**) and it ensures that all the vital steps are followed. It is also helpful to provide timelines for each step as part of project management.

In addition to governance, stakeholders play an important role in reporting. Stakeholders are groups of individuals representing different functions in an enterprise; they can include people consuming the report to make informed decisions; people affected by the decisions made; and people involved in the process of development, design, training and change management. Relevant stakeholders depend on the nature of the report being developed. For example, a report on vendor statistics would be relevant to stakeholders in the supply chain, procurement and finance.

Data

Data are any raw, unorganized facts that need to be processed. Data are the basis of any report, whether digital or nondigital. However, one of the biggest challenges is determining which data are necessary.

Figure 3—Factors Integral to the Development of a Digital Dashboard Report



Data Variables

Data availability is not necessarily a challenge, but collecting the right data can be. Ascertaining which data variables need to be included in a report can entail discussions across multiple groups.

Figure 4 provides an example of the amount of data available from a single purchase order—more than 90 field variables. When compiling a report to analyze open purchase orders, not all these data would be relevant.

Data Sources

Enterprises typically generate data in one form or another throughout the organization. For instance, data relating to vendors might exist in both the supply chain procurement system and the finance system. To create a meaningful report, both types of data would have to be integrated. For example, the number of purchase orders placed with vendors would be available through the procurement

Figure 4—Raw Data From a Purchase Order

Fields	Fields	Fields	Fields	Fields	Fields	Fields
PO Number	Company Code	Sales Order Number	Cart Number: Created By	Stat. Del. Date	G/L Account	Latest PO Approval Date
PO Line Item	Item Category	Sales Document Item	Cart Number: Created By (Text)	Plant	GL Account Description - Short Text	Confirmation Delivery Date
PO Document Date	Item Category Description	Valuation Class	Shopping Cart—Buyer Name	Plant Name	SLB Vendor Category	Effective GR Qty
PO Created by Name	Material	Valuation Class Description	Purchase Requisition Number	Storage Location	Main Vendor ID	Effective GR Amount in Local Currency
PO Document Type	Material Short Text	Acct Assignment Cat.	Requisition Item	Incoterm Line	Main Vendor Name	Open GR Amount
PO Document Type Description	Vendor Material No.	Acct Assignment Cat. Description	Requisition: Created on Date	Incoterm Line Location	OA Vendor ID	Local Currency (GR)
Incoterm_Header	Net Price Per Price Unit	Cost Center	Requisition: Created By	SRM Shopping Cart Number	OA Vendor Name	Effective GR Amount in Document Currency
Incoterm Header Location	PO Requested Quantity	Profit Center	Requisition: Created By (Text)	SRM Shopping Cart Item	PI Vendor ID	Document Currency (GR)
PO Header Currency	Order Unit	WBS	Requisition: Creation Indicator	Sum of SRM Shopping Cart Number: Created on Date	PI Vendor Name	Quantity Still to Be Delivered
PO Requested Delivery Date	Net Order Value	P&L Account	Requisition: Creation Indicator (Text)	PO Release Status	PO Release Indicator	“Delivery Completed” Indicator
Effective Invoice Amount in Document Currency	SCCode	GeoMarket	Category	First PO Approval Date	Requires Approval	Effective Invoice Qty
Document Currency (IR)	Commodity	Sub-GeoMarket	Sub Category	Family	Country of Ordering Plant (Destination Country)	Effective Invoice Amount in Local Currency
Material Group	Old_STCode	Sub-Product Line	Area	Region	Group	Open IR Amount
					Product Line	Local Currency (IR)

system, but the value of invoices paid would come from the finance system. A report based solely on either procurement or financial data would provide decision makers with an incomplete analysis.

Data Modeling

When data are processed, organized, structured or presented in a given context to make them useful, the result is called information. Data modeling refers to this process of structuring data to provide the necessary information for a digital report. **Figure 5** provides a good example of data. However, it conveys no meaningful information that could be used for analysis and decision-making.

When the same data are processed (**figure 6**), various types of information are conveyed:

- Total sales by month
- Comparison of sales by month (e.g., March sales were half of those in January and February)
- Sales by client, by month, by revenue and by product

Such reports allow an analysis of trends and can help decision makers take the necessary action. For example:

- The drop in sales in March can be attributed to United Hospitality.
- Toys continue to be the most popular product.

Data mining (techniques that find patterns in large data sets), data modeling and connecting source data to published data require a standardized approach and constitute an integral part of the governance process.

Presentation

Presenting reports in tabular form is the most common presentation approach, but with many advanced tools, a combination of visuals and data is

Figure 5—Vendor Data

Customer	Description of Items Sold	Amount ($,000)	City	Country	Date
Mack & Sons	Toys	80	Houston	United States	8-Feb-20
Lincoln Brothers	Toys	26	Los Angeles	United States	16-Feb-20
United Hospitality	Toys	25	Chicago	United States	18-Feb-20
Mack & Sons	Toys	45	Houston	United States	12-Feb-20
Lincoln Brothers	Paper	10	Los Angeles	United States	19-Mar-20
Westlock Inc.	Paper	35	Seattle	United States	3-Jan-20
Westlock Inc.	Toys	30	Seattle	United States	9-Mar-20
Mack & Sons	Frames	54	Houston	United States	14-Mar-20
Mack & Sons	Paper	28	Houston	United States	5-Mar-20
Lincoln Brothers	Cards	40	Los Angeles	United States	14-Jan-20
United Hospitality	Frames	50	Chicago	United States	11-Feb-20
Lincoln Brothers	Toys	40	Los Angeles	United States	17-Jan-20
Westlock Inc.	Frames	6	Seattle	United States	29-Jan-20
Mack & Sons	Paper	40	Houston	United States	5-Jan-20
United Hospitality	Paper	100	Chicago	United States	22-Jan-20

Figure 6—Vendor Information

Client Name	Jan	Feb	Mar	Total
Lincoln Brothers	80	26	10	116
Mack & Sons	40	125	82	247
United Hospitality	100	75	0	175
Westlock Inc.	41	0	30	71
Total	**261**	**226**	**122**	**609**

Item Name/Type	Jan	Feb	Mar	Total
Toys	40	176	30	246
Paper	175	0	38	213
Frames	6	50	54	110
Cards	40	0	0	40
Total	**261**	**226**	**122**	**609**

possible. However, designing this type of report often requires many iterations and can be time-intensive. **Figure 7** presents a snapshot of a brainstorming workshop to design and develop a single report to meet various stakeholder requirements.

Figure 8 provides an example of a digital report that blends visuals and data.

Development

Once the preliminary requirements related to data, visuals and parameters have been finalized, development of the report is the next step. The developers who configure the report are not expected to be functional experts in the field to which the report relates; therefore, expected results need to be clearly defined. An agile framework to monitor report development at predefined milestones is recommended so that any necessary corrective action can be taken and delays can be minimized.

User Acceptance Tests (UAT) and Access and Security

One of the earliest opportunities to test the report and gain firsthand feedback is through user acceptance tests (UATs). A successful UAT includes the following elements:

- Appropriate number of testers who are representative of actual users
- Correlation of testers' profiles with the complexity and sensitivity of the data and the magnitude of the report within the enterprise
- Specific time period for testing to take place
- Use of constructive feedback to add to or amend the report before it is distributed to users

Data and information are central to any enterprise. When a report is created, who will have access to it and how that access will be controlled are important considerations. There may be both internal and external requirements, such as statutory provisions or mandatory fiscal filings. In addition, laws such as the EU General Data Protection Regulation (GDPR) require that data confidentiality be maintained, and an enterprise that fails to do so could face serious financial and reputational damage.

One way to control access to reports and information is to link access to job codes and job areas through identity access management. This is considered the best practice to ensure that access is limited to those with a need to know.

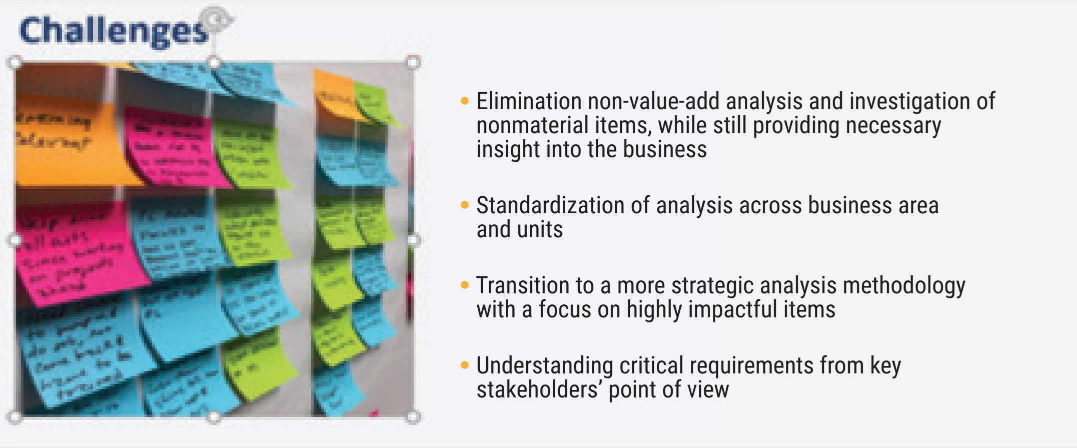
Also, a review of access logs at regular intervals, such as monthly, quarterly or semiannually, depending on the sensitivity of the information, is a common practice to ensure compliance.

Change Management

One of the most difficult challenges can be resistance to change. The magnitude of resistance depends on many factors, and in the case of digital reports, the reasons might include the following:

- Reluctance of current users to use digital reports
- Preference for printed reports rather than digital reports

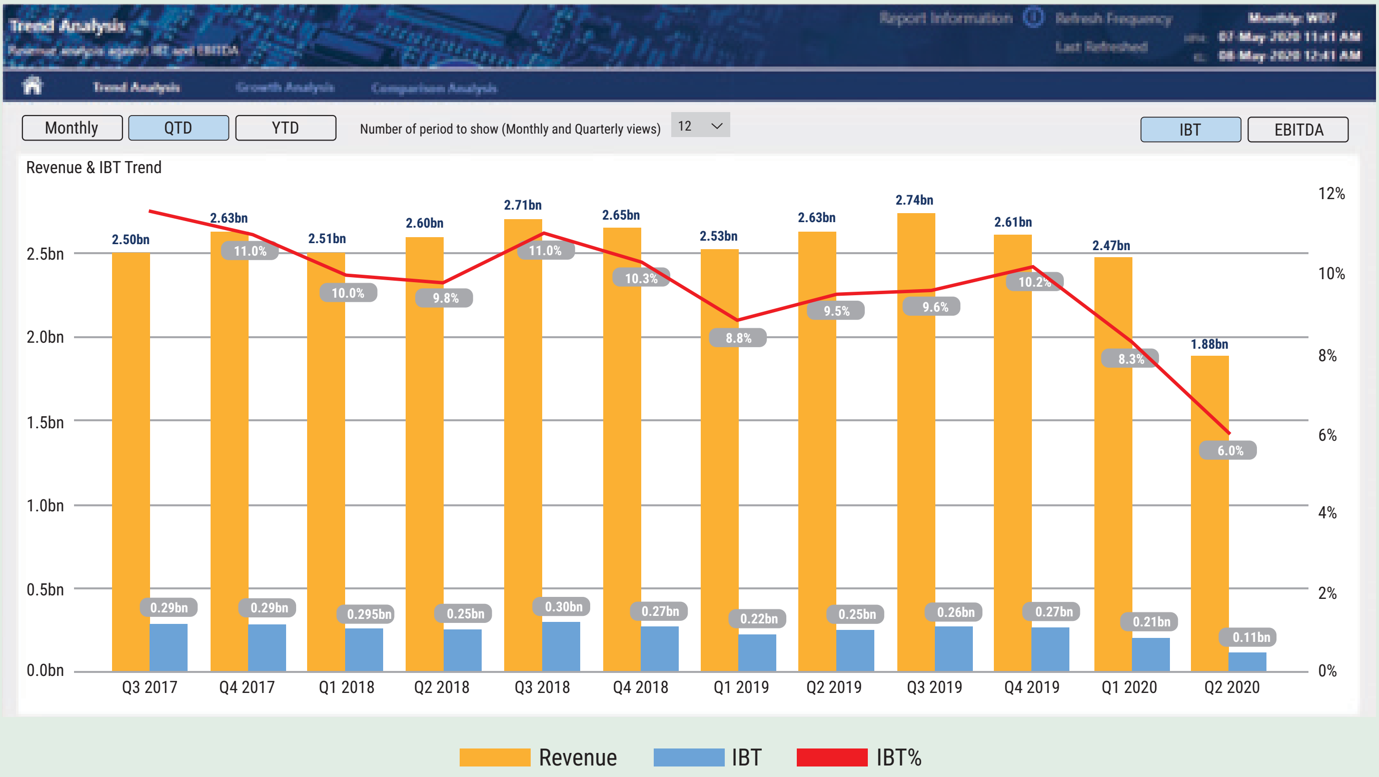
Figure 7—Brainstorming Workshop



Challenges

- Elimination non-value-add analysis and investigation of nonmaterial items, while still providing necessary insight into the business
- Standardization of analysis across business area and units
- Transition to a more strategic analysis methodology with a focus on highly impactful items
- Understanding critical requirements from key stakeholders' point of view

Figure 8—Report on Revenue and Income Before Tax (IBT)



Number of period to show (Monthly and Quarterly views): 12

Considering that the digital reporting system affects individuals across the enterprise, it is vital that all staff members buy in to the new system. Change management workshops may be useful, depending on the nature and complexity of reports. Multiple sessions may be required not only to gain acceptance, but also to ensure that people are comfortable accessing and interpreting reports in digital form.

Deployment and Feedback

Critical elements in the deployment of a digital report include:

- User access list
- Due diligence related to connectivity and configurations
- Regression testing and stress tests on load and performance issues

Once these technical aspects have been handled, it is important to consider the usage frequency and the number of users accessing the report compared with the original user list. This can provide the acceptance ratio and the value added throughout the enterprise.

Finally, formal user feedback, in the form of surveys, should be used to determine how the digital report could be enhanced to add more value.

Conclusion

Certainly, the information contained in digital reports and manual reports should be the same. However, considering the dynamic nature of real-time information, the use of a digital dashboard with multiple key drivers, data integrity through connectivity to source and efficiency through automation can all lead to benefits for an enterprise.

Only a well-defined and robust governance model can aid in the transformation of raw data into information, stimulating action from stakeholders. An effective governance process identifies various factors in the development cycle, defines the process, and determines the roles and responsibilities of various people. Enterprises with flexible governance processes will be able to adapt not only to a changing external environment, but also to new technological developments.

Q We are a service organization providing IT-based services to customers. Because of containment efforts and stay-at-home orders, most of our personnel are working from home, and only essential support staff who reside near the office are managing support from the office location. The internal audit department is proposing a remote IS audit. How can this be performed? What challenges might we face, and how can we overcome them?

A The COVID-19 pandemic has created a unique situation. To complicate matters, we are experiencing a global lockdown for the first time since continuity planning processes have matured. Despite not being prepared, many organizations have adopted work-from-home (WFH) strategies and developed policies for employees accessing an organization's information resources remotely in a fairly short period of time. Though employees managing essential services such as security, power, network, food and fuel can travel to work locations, many prefer to work remotely given the risk traveling to and working in an office presents.

Given that many organizations had not considered lockdowns as a possibility, the need to look at internal audit functions during this scenario was not anticipated. It is quite possible that audit firms have not thought that WFH might be required for auditors. Since the lockdown, many audit firms have developed strategies, approaches, policies and procedures for remote audit.

The American Institute of Certified Public Accountants (AICPA) has developed and shared best practices for conducting remote audits while complying with the Accounting Standard Board standards.[1] Audit companies such as the British Standards Institution (BSI)[2] and DNV GL[3] have developed a remote audit approach and started conducting remote audits. The International Organization for Standardization (ISO) Auditing Practices Group (APG) published guidelines for conducting remote audits in April 2020.[4]

Thanks to fast-moving advances in technology, conducting remote audits is becoming more popular among organizations. Enterprises already have high-tech strategies that allow audit teams to receive and share data, conduct interviews, and make observations for organizations all over the world without needing to commute to the audit site. Certification bodies will certainly have to adapt to this new situation. In fact, the last version of ISO 19011:2018 *Guidelines for auditing management systems*[5] includes new specifications for transitioning to conducting remote audits.

> “THANKS TO FAST-MOVING ADVANCES IN TECHNOLOGY, CONDUCTING REMOTE AUDITS IS BECOMING MORE POPULAR AMONG ORGANIZATIONS.”

A remote audit is performed the same as an onsite audit, except that the auditor depends on electronic devices to conduct the audit and obtain audit evidence without visiting the auditee in person. An auditee can share evidence and data files through electronic media such as email, Google Drive and more. Auditors can also use other advanced technologies to conduct walk-throughs and interviews. The technologies an auditor may consider using are:

- Smartphones, tablets and other handheld devices
- Laptops and desktop computers
- Video cameras
- Wearables, if required
- Drones for remote viewing or access to closed-circuit television (CCTV) recordings
- Data analytics access and reports
- Internet connections at remote locations or the homes of the auditors
- Remote conferencing facilities

Internal audit departments need to adapt the recommendation of AICPA and certification bodies to develop approaches, policies and procedures for conducting remote audits. This calls for a new way

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

of working and it requires the organization to receive support from management. Executives should take the lead and effectively communicate the new norm of remote internal audit throughout the organization. Remote auditing requires buy-in from various stakeholders and employees to ensure that it is given the importance it deserves and does not become diluted.

In addition to the restrictions created by the current pandemic, there are other situations where remote audits may be considered, either now or in the future, including:

- Availability of relevant stakeholders such as process owners, asset owners, risk owners and data owners for providing information for audits
- Restrictions on accessing production data remotely including those due to security policies
- Situations that limit or prohibit complete and accurate information for review of controls-related processes required for testing for audits
- Availability of technology required for conducting remote audit

There are pros and cons to conducting remote audits. Auditors should consider both before deciding to conduct remote audits. It may be noted, however, that during this current pandemic, conducting remote audits is a better option than deferring audits.

Conducting remote audits can improve productivity by eliminating inconveniences and saving time and money required for travel and logistics. Most important, the management of the auditee organization may also reduce costs and save money because onsite audits are timebound and must be completed in a pre-defined time period, which may not be required for remote audits.

There are some important questions identified by the APG to be considered in cases of remote audits:[6]

- When conducting virtual walk-throughs, either with the help of a remote video camera operated by the auditee or stored CCTV camera images, there can be questions such as:
  - Are these real-time images or video records?
  - Is this the entire control environment or just what is chosen by the auditee?

- Will the Internet connection required for interviews, meeting and other data gathering be stable and have adequate bandwidth?
- Can we audit the processes and sites as realistically as can be done in person?
- Can we get a good overview of the facilities, equipment, operations and controls?
- Can we access all required and relevant information?

When in doubt, a site visit may be considered for a shorter duration to confirm the answers to the questions once in an audit cycle, but it is not necessary for every audit.

There can be other challenges associated with remote audits, such as:

- Remote audits may not be approved or accepted by some regulators or certification and accreditation bodies.
- All auditee locations may not support sophisticated technology, which can lead to availability issues, malfunctions or other anomalies with technology.
- There may be a lack of management and process owner involvement.

- Auditors may be uncomfortable with technology, as some auditors feel they can trust the audit only if they have physical access to audit evidence. This can be true particularly in cases of physical walk-throughs.
- Auditors must have adequate training and experience in the use of technology.

To carry out remote audits, these steps should be considered:

1. Understand the audit scope and auditee area.
2. Determine the tools and setup required to conduct the audit.
3. Prepare an audit plan.
4. Set up audit meetings using virtual meeting tools. Discuss the plan and schedule during the first meeting, and explain the document sharing and evidence collection method. Ensure and provide assurance of the security of the information collected from the auditee.
5. Use CCTV footage or mobile cameras for physical walk-throughs. If this is not possible, defer the physical security audit until a site visit can be conducted.
6. Consider auditee resources, work schedules and plan breaks.
7. Review the documents and analyze evidence.
8. Discuss the draft audit report on a call or in a virtual meeting.
9. Declare the limitations of the remote audit, if any, in the report.

Remote audits will continue even after the current pandemic is over. These will not replace onsite audits, but the frequency of onsite audits may be reduced. Managers from auditee organizations are finding remote audits very attractive due to minimized interruptions, flexibility of schedules, and reductions in logistic efforts and costs.

Endnotes

[1] Murphy, M. L.; "AICPA Best Practices for Conducting Remote Audits in Uncertain Times," *Compliance Week*, 6 April 2020, *https://www.complianceweek.com/accounting-and-auditing/aicpa-best-practices-for-conducting-remote-audits-in-uncertain-times/28710.article*

[2] British Standards Institution, *Remote Audits*, United Kingdom, 2020, *https://www.bsigroup.com/globalassets/localfiles/en-th/our-service/assessment-and-cert/remote-audit/bsi-remote-audit-flyer-final.pdf*

[3] DNV GL, Remote Auditing—Getting the Most Out of Every Interaction, Norway, 2020, *https://www.dnvgl.com/assurance/remoteauditing/index.html*

[4] International Organization for Standardization (ISO) and International Accreditation Forum (IAF) *ISO 9001, Auditing Practices Group Guidance on: Remote Audits*, Switzerland, 2020, *https://committee.iso.org/files/live/sites/tc176/files/documents/ISO%209001%20Auditing%20Practices%20Group%20docs/Auditing%20General/APG-Remote_Audits.pdf*

[5] International Organization for Standardization (ISO), *ISO 19011:2028(en,) Guidelines for Auditing Management Systems*, Switzerland, 2018, *https://www.iso.org/obp/ui/#iso:std:iso:19011:ed-3:v1:en*

[6] *Op cit* ISO, IAF

CROSSWORD PUZZLE

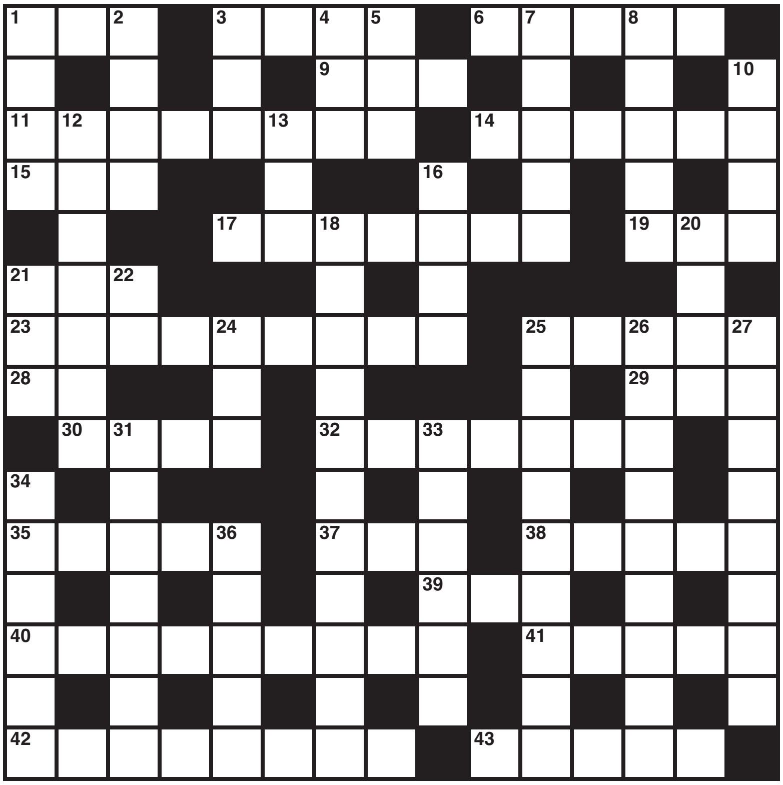
By Myles Mellor
www.themecrosswords.com

ACROSS

1 Popular acronym since the pandemic, relating to work location
3 Popular video communications company
6 Software company's security fix
9. Exclude
11 ____ analyzer
14 Security lapse
15 Frightened noise
17 Performance standards
19 Take, after taxes
21 Excitement
23 Yardstick
25 Electronic memory device
28 Hosp. hot spot
29 Something to check
30 Email, e.g.
32 Methodologies
35 Incident
37 Not forthcoming
38 Security breaches
39 Business name abbr.
40 Movement to and integration into another system
41 Fuel tanker
42 Assuming as an axiom
43 Gut feeling

DOWN

1 Erase
2 Catch
3 Animal sanctuary
4 Sale clause, abbr.
5 ___ware
7 Special qualities
8 Word with block or supply
10 It is best live
12 Card ____ (plural)
13 Signal
16 The R in KRIs in COBIT®



18 Instance of buying or selling
20 Continental currency
21 16th US president
22. __ track
24 Concealed
25 It is used as a payload to exploit a software vulnerability
26 Hurdles
27 Disclosure of secrets
31 Materializes
33 Illegal activity of gathering classified information
34 Join forces (with)- 2 words
36 Characteristic

Answers on page 58

CPE QUIZ
#192

Take the quiz online.

https://bit.ly/31JNryO

Based on Volume 3, 2020—Human Element of Risk
Value—1 Hour of CISA/CRISC/CISM/CGEIT Continuing Professional Education (CPE) Credit

TRUE/FALSE

FREUND ARTICLE

1. In Aristotle's communication model, the sender is the individual who ultimately determines whether communication has taken place.
2. A risk scenario should specify who is doing something bad, the methods being employed to do it and the deed's ultimate impact on the organization. It should also be forward-looking and relatively perpetual.
3. The use of sampling in risk assessment calls for choosing samples from the "bottom" risk category level—samples that inform the top- and intermediate-level categories—then selecting the associated cyberscenarios and technology stacks.

PEARCE ARTICLE

4. Programming, design and data are basic human endeavors/outcomes that produce digital transformation technologies. They are also the same human activities that put those technologies at risk.
5. Three capabilities that can lead to a reduction in human error are detectability, traceability and resilience.
6. Digital transformation technologies are often introduced into each other, such as artificial intelligence (AI) in drones. This cascade effect of potential human error makes risk management more complex.

KOHAN ARTICLE

7. Data breaches can be extremely costly and they often arise from within the enterprise, rather than outside. Therefore, it is surprising that only 78 percent of enterprises monitor their employees' digital behavior.
8. To gather needed information about employees' activities while also protecting their privacy, enterprises must define the purpose of any monitoring undertaken, align processes with the purpose and regularly prioritize intentionality.
9. When choosing technology, it is important for the enterprise to consider vendor support and service level agreements, especially if the enterprise lacks in-house resources.

BLUM AND WEINBAUM ARTICLE

10. The enterprise in the article set up a timeline for establishing enterprise risk management (ERM) based on four 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; and a shifting risk appetite within the enterprise.
11. The team used a Scoping Triangle—built on assets, threats and effects—to create a generic risk matrix for business processes.
12. Among the lessons learned from the ERM project was that just-in-time training, or refresher training at critical points in the transformation process, was unnecessary and, in fact, was considered a waste of time by some stakeholders.

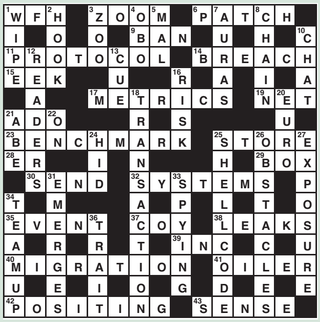
RAMASUBRAMANIAM AND SINGH ARTICLE

13. Risk intelligence can enhance an existing third-party risk management program. It is readily available and can help establish continuous monitoring.
14. Assessment of business-essential third parties should be conducted onsite annually and should cover baseline controls and focused control domains.
15. For the client enterprise, third-party risk management stops at the third parties themselves. The third parties are responsible for managing risk introduced by any fourth (or fifth or nth) parties and subcontractors.

TEODORO ARTICLE

16. While a security risk assessment can provide the basis to identify, protect against, detect, respond to and recover from security threats, it is not suitable for prioritizing areas of investment.
17. In determining which technology security features will help maintain continuous operations, enterprises must understand the likelihood and potential impact of a security risk, the types of cybersecurity attack vectors that can deliver malware, and their own risk tolerance.
18. Tokenization is a technique to replace an original value with a token value and store the data and the tokens centrally so data can be tokenized and de-tokenized.

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



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

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.

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 Editors

Andie Bernard
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

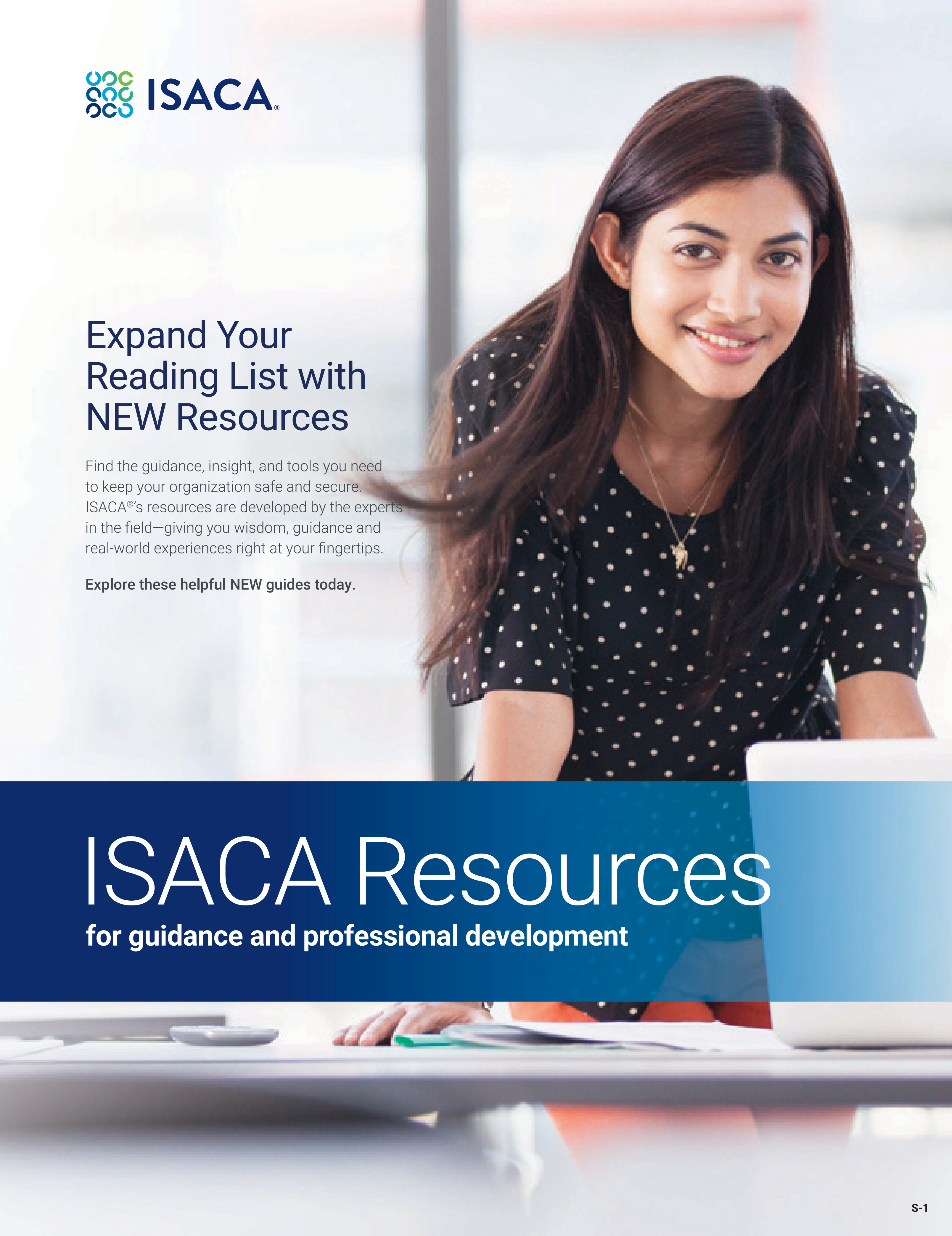
news@isaca.org

ISACA

Expand Your Reading List with NEW Resources

Find the guidance, insight, and tools 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.

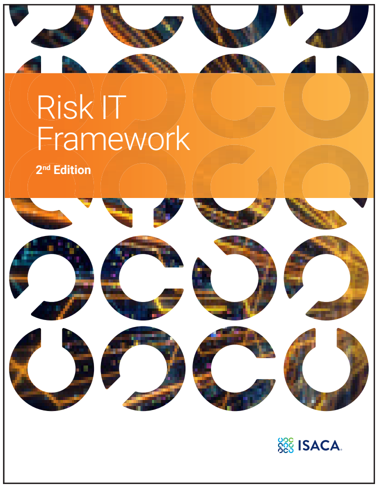
Explore these helpful NEW guides today.



ISACA Resources

for guidance and professional development

FEATURED RESOUCES



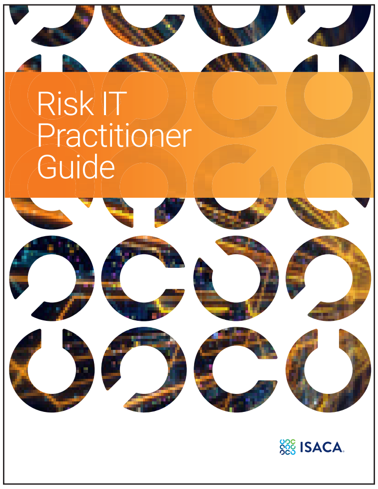
Risk IT Framework, 2nd Edition

Print Product Code: RITF2 | Member Price: $60 | Nonmember Price: $75
Web Download Product Code: WRITF2 | Member Price: Free | Nonmember Price: $75

The *Risk IT Framework* is designed to assist in developing, implementing or enhancing the practice of risk management by:

- Connecting the business context with the specific I&T assets
- Shifting the focus to activities over which the enterprise has significant control, such as actively directing and managing risk, while minimizing the focus on the conditions over which an enterprise has little control (threat actors)
- Increasing the focus on using a common risk language that correctly labels the items that have to be managed well to create value

The *Risk IT Framework* will enable enterprises to understand and manage all significant IT risk types, building upon the existing risk related components within the current ISACA frameworks.



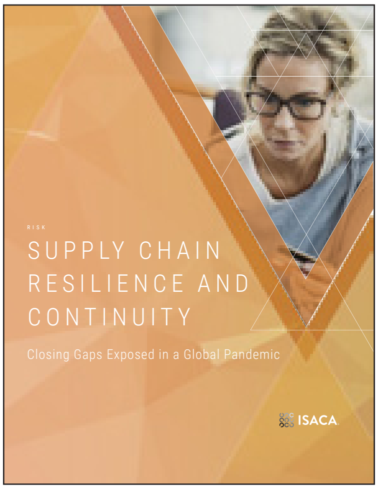
Risk IT Practitioner Guide, 2nd Edition

Print Product Code: RITPG2 | Member Price: $75 | Nonmember Price: $100
Web Download Product Code: WRITF2 | Member Price: Free | Nonmember Price: $75

The *Risk IT Practitioners Guide* is designed to assist in developing, implementing or enhancing the practice of risk management by:

- Connecting the business context with the specific I&T assets
- Shifting the focus to activities over which the enterprise has significant control, such as actively directing and managing risk, while minimizing the focus on the conditions over which an enterprise has little control (threat actors)
- Increasing the focus on using a common risk language that correctly labels the items that have to be managed well to create value

The *Risk IT Practitioner Guide* provides practical guidance for risk professionals. The guide includes a large variety of "how-tos" for people so that they can implement risk techniques into their daily jobs.



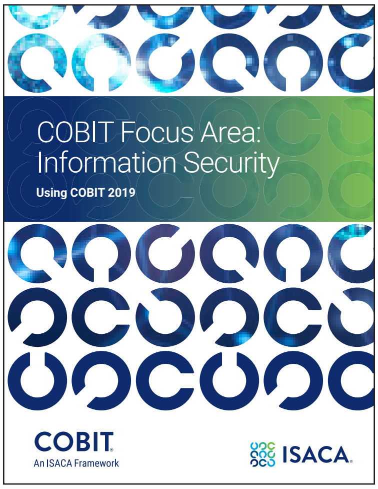
Supply Chain Resilience and Continuity: Closing Gaps Exposed in a Global Pandemic White Paper

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

With each major disaster we confront—including the current pandemic—business continuity management must continue to evolve. Learn how in our new white paper: *Supply Chain Resilience and Continuity: Closing Gaps Exposed in a Global Pandemic.* Supply chain management is facing major challenges worldwide due in part to area lockdowns and the lack of resources caused by the current pandemic. With the highlighting of these critical limitations, many enterprises are making building resiliency a priority. Explore approaches to make your enterprise supply chain more resilient during major interruptions.

This ISACA® white paper is for IT risk practitioners and other information technology and business professionals that deal with supply chains and business continuity.

Order online at www.isaca.org/resources



COBIT Focus Area: Information Security Using COBIT 2019

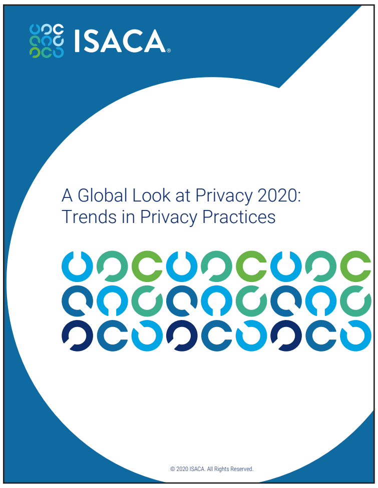
Web Download Product Code: WCB19IS | Member Price: $50 | Nonmember Price: $90
Print Product Code: CB19IS | Member Price: $60 | Nonmember Price: $100

COBIT Focus Area: Information Security provides guidance related to information security and how to apply COBIT to specific information security topics/practices within an enterprise. The publication is based on the COBIT core guidance for governance and management objectives, and enhances the core guidance by highlighting security-specific practices and activities as well as providing information security-specific metrics.

In COBIT 2019, a focus area describes a certain governance topic, domain or issue that can be addressed by a collection of governance and management objectives and their components. This publication describes information security and details additional metrics and activities that should be considered when implementing or assessing COBIT in the context of information security.

Key publication details include:

- Provides a contemporary view on information security governance and management
- Clarifies roles of governance and management and shows how they relate to each other in the context of information security
- Provides a clear end-to-end view into distinction within the enterprise and during all process steps between information security governance and information security management practices
- Provides a comprehensive and holistic guidance on information security – not only to processes but to all components in an enterprise, including organization structure, skills, policies, etc.
- Additional information security-specific activities, metrics and information flows.


ISACA
A Global Look at Privacy 2020:
Trends in Privacy Practices
© 2020 ISACA. All Rights Reserved.

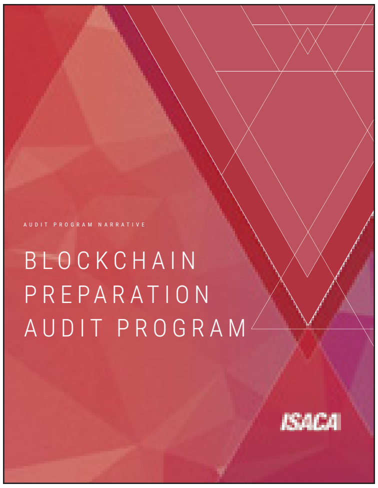
A Global Look at Privacy 2020: ISACA Research Report White Paper

White Paper Product Code: WHPGLP20 | Member/Non-member: FREE

Despite challenges in identifying and understanding their privacy obligations, organizations see the importance of data protection and compliance. For a detailed insight into privacy accountability, confidence in enterprises' ability to secure sensitive data and privacy controls, download our new white paper: *A Global Look at Privacy 2020: Trends in Privacy Practices.*

Based on a survey conducted by ISACA® in Q4 2019, *A Global Look at Privacy 2020* collected information from respondents around the world about the privacy practices in their enterprises. This report provides answers to a wide range of questions, from who is accountable for privacy in each respondent's organization to the amount of interaction the privacy function has with other areas of the organization to how many privacy professionals are employed to meet an organization's needs.

Explore these responses and identify differences in privacy program effectiveness.



Blockchain Preparation Audit Program

Zip File Product Code: WAPBAP | Member Price: Free | Nonmember Price: $49

As blockchain is still an emerging technology, there is not yet a published uniform auditing standard. However, this program is intended to help organizations identify and develop key policies, procedures and controls to mitigate risk and streamline processes.

Audit Subject: Blockchain Technology Audit Preparation Program

Blockchain is the underlying distributed network system that stemmed from the world's first decentralized cryptocurrency, bitcoin. It has quickly become one of the most promising technological advancements in recent times. Blockchain has the potential to transform a variety of key industries that are ubiquitous to modern life: finance, healthcare, manufacturing, and real estate, to name a few.

Blockchain's prominent feature is its ability to eliminate the need to trust a central authority for approval, as it instead relies upon decentralized participants to reach consensus. Its benefits include: transparency, cost reduction, enhanced speed, and embedded security. However, with any new technology, there are often drawbacks that can result in issues for organizations. Blockchain is still not a mature technology, and caution must be used when deploying it at an enterprise level. As the risks are often misunderstood and overlooked for this emerging technology, ISACA has developed an audit preparation program to provide organizations with a framework to manage blockchain.

The blockchain technology audit preparation program worksheet is provided as a separate file.

Audit Objectives

- Provide management with an assessment of whether their blockchain technology control environment is adequately designed and operationally effective.
- Identify blockchain risks which could result in reputational and/or material financial impact.
- Provide management with a holistic perspective on blockchain technology that considers both technical and non-technical factors.

Audit Scope

The audit preparation program is built on the following six categories:

- Pre-Implementation
- Governance
- Development
- Security
- Transactions
- Consensus

The auditor performing the review will be required to determine the scope of organizational functions, systems, and assets that will be tested.

ONE IN TECH™

An ISACA Foundation

Join us in creating a **Healthy Digital World** that's safe, secure and accessible for ALL.

www.oneintech.org