ISACA

Journal

VOLUME 1, 2023

BUILDING DIGITAL TRUST

REALITY CHECK: THE USE OF BIG DATA AND PREDICTIVE DATA MODELS

TOWARD REBUILDING DATA TRUST

EXTENDING ZERO TRUST TO THE END USER ECOSYSTEM

ISACA.ORG

Contents

DEPARTMENTS

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 January and February.

Blockchain Smart Contracts, Part 3
SAMUEL SMITH AND ANDY GARCIA, PH.D., CPA

The Future of Cryptography: Performing Computations on Encrypted Data
DEVHARSH TRIVEDI

The True Cost of a Data Breach
NATALIE JORION, PH.D., AND JACK FREUND, PH.D., CISA, CRISC, CISM, CGEIT, CDPSE, NACD.DC

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505
Fax: +1.847.253.1755
Web: www.isaca.org

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 information technology, IT audit, risk, governance, privacy, security, assurance and emerging technology.

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.

/ISACANews

/ISACAOfficial

ISACAHQ

/isacanews/

Dear Readers

You have heard ISACA® members talk a great deal about digital trust this past year—and for good reason. Digital trust is the important commitment to ensure that customers, employees and shareholders feel secure when partnering with an organization or using an organization's product or service.

By treating security, privacy, assurance, governance and all other key components of digital trust less as afterthoughts and more as strategies organizations are better positioned to protect their customers, employees and shareholders.

As a chief information security officer (CISO), I approach digital trust primarily from a security perspective. Viewing it through that lens, digital trust is about more than fixing security bugs. It is about the tremendous opportunity to build security features that customers want and need. These security features allow more granular and transparent security controls and better authorization (i.e., multifactor authentication [MFA] options). It is my goal to use a risk-based approach driven by data and transparency to promote a security culture that is woven into products and services, and how business is conducted. Encouraging a security-focused culture and having security teams involved in product development reduces costs, helps avoid potential incidents, and creates features for privacy and security that customers and employees want.

It is also important to drive security innovation that allows organizations not only to respond to current threats and issues, but also to best position themselves to address the ever-evolving risk landscape. Organizations must stay ahead of the curve, especially as they migrate to fully cloud-based products.

As you think about your role, how do you advance digital trust? How does the work you do help your organization fulfill its commitment to its customers and stakeholders? As you read this issue of the *ISACA® Journal*, I hope you find additional clarity and guidance relative to your vitally important role as a digital trust professional.

As a long-time member, I am excited to see ISACA commit to digital trust to help organizations and individuals build and benefit from a safer and more secure digital world. It is an honor to be a member of ISACA's new Digital Trust Advisory Council, and to be a part of advancing ISACA's vision.

I hope the articles you are about to read inspire you to get more involved in advocating for stronger digital trust.

Best regards,

Rinki Sethi

RINKI SETHI | CISA

Is vice president and chief information security officer at BILL, where she leads the global IT functions, advances efforts to protect BILL's information and technology assets, and provides advice on the company's continued innovations in the security space. Sethi serves on the board of ForgeRock, a public company in the identity and access management space, and is a member of the ISACA Digital Trust Advisory Council.

Advertising Information Security

So, I am watching a sporting event on television and a former employer of mine runs an advertisement that says its devices will solve my cybersecurity problems. Later in the match, another former employer tells the world that its consultants can produce privacy for my business. A full page advertisement in my Sunday newspaper tells me that this organization's software can give me peace of mind that my data are safe.

What is going on here?!? Everywhere I look, it seems that someone is trying to sell me information security.

Information Security for the Mass Market

I have been a specialist in information security long enough to remember the times when we few, we happy few in InfoSec had to fight for any recognition at all. The struggle for budget, personnel, tools and seniority had to be fought endlessly, as did the battle against the bad guys trying to break into our employers' systems and data. So, for me at least, seeing information security sold to the general public leaves me in shock.

STEVEN J. ROSS | CISA, CDPSE, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. He has been writing one of the Journal's most popular columns since 1998. Ross was inducted into the ISACA® Hall of Fame in 2022. He can be reached at stross@riskmastersintl.com.

I am concerned that people at large will come to believe that information security can be achieved simply by buying it.

I understand that advertising is a reflection of reality, not reality itself. I have long been told that if I only buy the right products, I will be healthier, wealthier, wiser and sexier. None have worked so far. I actually have greater confidence that some of the security products and services that I see advertised will work as promised. But I am concerned that people at large will come to believe that information security can be achieved simply by buying it. Yes, tools are important, but the security program that chooses and uses those tools is paramount.

There is something wondrous about advertising information security products to mass markets. It implies that the number of actual buyers of these products is great enough that it pays manufacturers and service companies to reach out to them through the general media. ISACA® take note: Our members are a large cohort of valued potential customers.

It is also pleasing that my friends and family who have long asked me, "What is it that you do exactly?" now are treated to an explanation that neither trivializes nor aggrandizes information security. These ads tell them what I and every other information security professional I know has been saying for years: Information security is good for business.

It Pays Not to Advertise

But there is something missing. I do not see advertisements for the banks, insurers, manufacturers, educational institutions, governments or any other industry that buys security products stressing their own security. If we make the case, as I often have, that information security creates a competitive advantage, why are these organizations not claiming it? Are they just shy? Are their information security practices not thorough enough? Have they not spent enough on people and products?

I believe that many organizations are spending appropriately large amounts of money on information security.[1] (On the other hand, I do not believe any of the reported global outlays, which, with a brief search of the Internet, vary from US$23 billion[2] to US$40.8 billion[3] to US$140.12,[4] which is quite a spread.) So why am I not seeing ads that say, “Do business with us! Your data are secure with us!”?

I believe the reason is that they are afraid their entire marketing strategy can be upset in an afternoon by a successful cyberattack. A demonstrated lack of security could instantly become a competitive disadvantage. I realize how unfair this is. Not naming names, but I know of many top-flight organizations with excellent information security functions that have been victimized by cyberattacks and frauds. If the best are not safe, what can lesser institutions say or do?

This has long been a dilemma for those information security professionals who have tried over the years to demonstrate the effectiveness of their programs. The burden of proof rests with the criminals and terrorists. The best team in the league occasionally loses a game; they do not get relegated to the second division for that loss. But a single cyberattack can undermine the credibility of an entire information security program. No wonder marketing executives conclude that it pays not to advertise the strength of their information security.

Promoting Information Security

I propose that it is the responsibility of organizations’ information security functions to capitalize on what they are doing to enhance the business’ public image. They should aid their marketing departments in developing ad campaigns featuring what is being done to protect customers’ information. In a bygone era, banks built large and imposing branches to imply their solidity; they called themselves trust companies. Insurance companies named themselves after mountains and large rocks. Manufacturers were proud to print pictures of giant factories on their labels. All of this was to say, “We are here to stay. We look after you and your assets. You can trust us.”

Organizations and their information security functions can capitalize on this security literacy by explicitly demonstrating what they are doing to prevent theft or misuse of customers’ information.

Perhaps it is time to rebrand information security and privacy as more than fancy technology and super sleuths. Customers and prospects can be told that the information security department is their friend looking out for their data. The chief information security officer (CISO) might be styled as the customer information protection executive (CIPE). Of course, the function will continue to protect all information as well as that of customers, but the public image would be altered.

Then an advertising campaign might be launched featuring the CISO/CIPE and the security staff. There would not be, must not be, any guarantees of secure information. Rather, the ads might explain what the individuals are doing to protect customers’ interests. Note that the individuals would be featured, not the organization. The point is that there are people—not a faceless, impersonal institution—looking after you.

In large measure, because cyberattacks have been so well publicized, the general population is increasingly well-educated about issues such as cybersecurity, privacy and access control. Those TV spots during ballgames for security vendors have not hurt either. Organizations and their information security functions can capitalize on this security literacy by explicitly demonstrating what they are doing to prevent theft or misuse of customers’ information.

I urge organizations to change the imagery of security and the way they use information security as a marketing tactic. Enough of locks, armaments and bulldogs as our symbols. Organizations should stress what they are doing to allow authorized customers, and only them, to access their information, rather than placing the focus on keeping the wrongdoers out. The avatar for information security should be the school crossing guard, not the burly cop.

LOOKING FOR MORE?

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

Ultimately, advertising for information security should convey that security is beneficial for the customer, more than a way of preventing bad things from happening.

Endnotes

1. For example, the chief executive officer (CEO) of one of the world's largest banks said in an interview that his organization spends more than US$1 *billion* every year on cybersecurity. Bursztysnsky, J.; "Bank of America Spends Over $1 billion per Year on Cybersecurity, CEO Brian Moynihan Says," CNBC, 21 June 2021, *https://www.cnbc.com/2021/06/14/bank-of-america-spends-over-1-billion-per-year-on-cybersecurity.html*
2. Smith, R.; "Global Cybersecurity Spend to Hit $23bn in 2022 – Report," *Insurance Business America*, 3 June 2022, *https://www.insurancebusinessmag.com/us/news/cyber/global-cybersecurity-spend-to-hit-23bn-in-2022-report-408361.aspx*
3. Sava, J. A.; "Spending on Cybersecurity Worldwide From 2017 to 2021 (COVID-19 Adjusted)," Statista, 16 February 2022, *https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/*
4. Research and Markets, *Global Cyber Security Market, By Type, By Solution, By Industry Vertical, By Services, and By Region—Forecast and Analysis 2022–2028*, Ireland, 2022, *https://www.researchandmarkets.com/reports/5597513/global-cyber-security-market-by-type*

Building Digital Trust Through Advocacy

In late 2022, the ISACA® New England (USA) Chapter president received an invite for Hill Day—an opportunity to join in a day of advocacy with other US chapters on Capitol Hill in Washington DC, USA. The topic was digital trust and the objective was for chapter participants to meet with their respective US congressional representatives to build the ISACA relationship, offer expertise as IS audit/risk professionals, and promote education support for information systems risk and audit-related programs.

To be honest, I did not realize the degree of engagement ISACA had in terms of advocating for our profession. After years of working at a local level for environmental causes, I know how powerful it is when people get involved. Here was an opportunity to make a difference in my own profession related to a topic that truly impacts everyone because technology plays a role in even the most basic activities of daily life and the most complex enterprise strategies. Hill Day not only offered an opportunity for advocacy, but also carried the promise of building relationships with state representatives as an ISACA-credentialed expert on the topics of risk, cybersecurity, privacy and resilience.

After accepting the invitation, I looked up digital trust to make sure I was not interpreting the concept based on my experience alone. The ISACA definition provides a holistic approach to technology and is significant for ISACA-certified professionals. Digital trust encompasses the disciplines ISACA promotes where we as professionals make a difference in our organizations, in learning institutions where we contribute thought leadership and the local community where our subject matter expertise provides meaningful information. It is encouraging to know that digital trust is not confined to cybersecurity or privacy but instead encompasses the key elements that are hallmarks of the ISACA disciplines, including:

- Quality
- Security and privacy
- Transparency and honesty
- Availability
- Ethics and integrity
- Resilience

For IS risk and audit professionals, digital trust is about the relationships that can be built by promoting a multidiscipline approach to risk assessments, controls testing and audit. The concept resonates with business objectives because it builds operational understanding and fosters client relationships through an ever-stronger enterprise reputation in an increasingly technological world. Most important, it puts technology center stage as an enabler instead of behind the computer room door, relegated to the roles of managing support systems and maintaining applications. This change in thinking means IS risk and audit professionals can and should take an integrated approach to the work, with full participation as business partners.

Capitol Hill and Digital Trust

The business advantages of a digital trust framework are many, but technology still feels foreign to many business operations teams, or it feels scary to organizations that dread attacks from cyber bad guys who seem undefeatable. Digital trust replaces fear and a sense of being chained to technology with educational awareness. It engages business professionals and students in a powerful way to start a paradigm shift that will add value to what they do. That is where Hill Day and the US Congress enter the picture.

It is exciting that ISACA has a government relations team advocating for ISACA members all over the world. As an accrediting institution, the value of ISACA's certifications

CINDY BAXTER | CISA, ITIL FOUNDATION

Is director at What's the Risk, LLC. Her practice focuses on integrated risk control and process assessments for cybersecurity, privacy and business continuity/disaster recovery. She views risk management and control assessment as a chance to learn the nuts and bolts of a business and help her clients worry less, because gaps have been uncovered and a stronger operating model can be built. Baxter draws upon her experience in banking, insurance, healthcare and technology after holding compliance and management roles at State Street Corporation, American International Group (AIG), Johnson & Johnson and AT&T. When she is not doing risk and audit work, she enjoys volunteering on climate and environmental issues that impact her community.

grows even stronger when government representatives are aware and understand that there is a population of ISACA-certified professionals present in their constituent bases. The start of Hill Day included an "Advocacy 101" overview by ISACA's chief executive officer (CEO) and government affairs leadership team. Expectations were set for whom chapter members would meet, how to lead conversations and how to constructively follow up. Focusing on what the congressional representatives could do to support ISACA's proposal for digital trust was critical, and to drive that point, retiring US Representative from the State of New York John Katko, a ranking member on the US House Committee on Homeland Security, addressed ISACA participants regarding the importance of cybersecurity awareness, the activities of the US Cybersecurity and Infrastructure Security Agency, (CISA), and the challenge of building a collaborative mindshare founded on trust and knowledge. How does one establish that mindshare, especially in a US election year, in the fourth quarter when the 117th US Congress is winding down, on a subject that is not quite headline news? Key points for getting attention include:

- The topic of discussion must matter to constituents in the US representatives' and senators' home states. As constituents from each representative's home areas, ISACA chapter participants were the perfect messengers to highlight the relevance of digital trust.
- The meeting can be effectively held with staffers instead of bigwigs. Staffers understand the details on behalf of the representatives and senators and are the behind-the-scenes workforce ready and able to bring attention to the cause.
- The topic needs to have an "ask," namely a specific area in which the representative can help. An offer to support the representative is also good to help keep follow-up communication active after the initial meeting.

The Hill Day ask was to support technical education and the US National Defense Authorization Act (NDAA) for fiscal year 2023, when an annual review of funding and target areas for the NDAA is on the voting agenda. The annual bill authorizes US Department of Defense (DoD) spending levels and sets overarching military policy to equip, supply and train US troops and provide for military families.[1] Both the US House of Representatives (House) and the US Senate propose annual funding recommendations and then arrive at a compromise upon which the US Congress agrees for the following year's funding levels in specific categories, including technology and cybersecurity. The 2023 House version of the funding proposal includes specific areas of interest to ISACA, namely funding for technical education and funding support for veterans. Growing skills through formal programs in hopes of increasing the talent pool of qualified professionals would institutionalize consistent learning for the profession and assist in standard and repeatable digital trust attributes.

Digital trust replaces fear and a sense of being chained to technology with educational awareness.

Meeting With Congressional Representatives

It is easy to think of US senators and US House representatives as driven by special interests or swept up in dealing with global calamities based on the soundbites in the media. Those big interest events always seem to overshadow life in the communities that each US Congressmember represents. Hill Day was a good reminder that whether priorities are global in nature, such as the economy and climate, or specifically local to a representative's district, work must aim to improve life in each representative's home region. The meetings held with staffers and US Congress members focused on what digital trust means for local businesses, how it can improve consumer experiences in a complex technical world, and how education and awareness can accelerate positive change through technology, from receiving care at the doctor's office to scanning purchases in a checkout line. The ISACA New England (USA) Chapter (my local chapter) did not meet with the elected officials on Hill Day; instead, chapter members met with the representatives' technology staffers whose backgrounds on technology and cybersecurity enabled the conversations. Our ISACA Global sponsors had set expectations that we might not be meeting with US senators and representatives directly, so the chapter team was prepared with more detailed questions and requests for support on technical education, which the topic-focused staffers were able to address. Each meeting included targeted leave-behind materials that opened the door for future discussions and invitations for the representatives to attend local ISACA chapter meetings.

The benefit for chapter members to build relationships with specific staffers whose roles are in technology promised to make follow-ups meaningful and on target with local needs. Meeting with technically fluent staffers also provided a direct relationship for chapter members to become involved as subject matter experts and to support legislation that helps the profession. Even better than getting legislation passed into law, the relationships initiated on Hill Day allow ISACA members to work with their legislative teams to operationalize existing regulatory frameworks and to take advantage of government support that extends beyond the walls of each person's enterprise environment.

The People Network Matters

The kickoff of networking with US congressional staffers and elected officials is a significant area of opportunity that ISACA introduced on Hill Day. The chance to meet with other chapters from around the United States was a very important advantage for attendees. It allowed members to look outside their local and enterprise environments to see other viewpoints on digital trust and other key areas that are important to ISACA members. In the emerging post-pandemic world, it was a good reminder of the value ISACA professionals bring to each other, whether it is from coast to coast in the United States—as was the case on Hill Day—or from around the world, through sharing common themes and concerns. In a fast-paced world with careers that never stand still, it is comforting to fraternize with like-minded individuals and share experiences and consider future partnerships.

What You Can Do

Even though the pace of work, home and play does not seem to slow down, we are part of a larger community of IS professionals with common understandings and similar goals. Digital trust brings our work center stage in the enterprise and community landscapes, and that can be a differentiator for us. We can make it global, or we can focus on our own backyards. Regardless, there are some points to consider:

> Growing skills through formal programs in hopes of increasing the talent pool of qualified professionals would institutionalize consistent learning for the profession and assist in standard and repeatable digital trust attributes.

- It is important to vote for candidates who resonate with your priorities. Legislative support and government funding stem from representation that advocates for digital trust (and other causes that are important to voters) because representatives know that is what constituents want.
- Consider how you use your ISACA membership. Might more involvement in your local chapter open networking opportunities for you? Could you benefit from a Hill Day experience that gets you in touch with your local government officials? The local chapter volunteers make a dramatic difference in ISACA's reputation and recognition to benefit all of us.
- Leverage the ISACA experience with your priorities for work and volunteering. Are there themes among the different areas in which you are involved? Can ISACA contribute to what is important to you either through a meaningful network, a meaningful event, or support of a cause that matters to what you do? If so, the possibilities are as close as an email to your local chapter or an inquiry made to ISACA's Engage page.

Who knew so much was possible and that there is so much opportunity for involvement, advocacy and change? It is all a great opportunity to get involved.

Editor's Note

To learn more about and become involved in ISACA's global government relations initiatives, please go to *https://www.isaca.org/why-isaca/about-us/advocacy*.

Endnotes

[1] United States Committee on Armed Services, "Reed and Inhofe File Fiscal Year 2023 National Defense Authorization Act," USA, 18 July 2022, *https://www.armed-services.senate.gov*

LOOKING FOR MORE?

- Visit the ISACA Advocacy Page. *www.isaca.org/why-isaca/about-us/advocacy*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

THE BLEEDING EDGE

Infrastructure as Code: Digital Trust Enabler?

On the surface, digital trust is a simple enough concept to grasp: It speaks to confidence in the digital ecosystem all around us and in the systems, applications, technologies, data and processes that support our online and other digital interactions. For example, it reflects our belief in the resilience of systems, integrity of information and data, privacy and confidentiality of information about ourselves and our loved ones, and the security of applications and data. But when we really stop to think about digital trust, we realize that, while subtle, there is nuance to unpack—for example, the connection between familiarity and trust.

In the analog world, one key underpinning of trust is experience—meaning trust is often impacted by how much experience we have with a thing. As an example, most people trust cars more than planes, even though the overwhelming quantitative evidence supports air travel as safer. Why is this? One reason is that cars are more familiar. This is actually a well-documented cognitive bias. The familiarity principle, or the mere exposure effect,[1] is an inherent bias in people to perceive familiar things as "better" (i.e., safer, more comfortable, more desirable). We ascribe a perception of risk to the novel just because it is novel.

ED MOYLE | CISSP

Is currently director of Software and Systems Security for Drake Software. In his 20 years in information security, Moyle has held numerous positions including director of Thought Leadership and Research for ISACA®, Application Security Principal for Adaptive Biotechnologies, senior security strategist with Savvis, senior manager with CTG, and vice president and information security officer for Merrill Lynch Investment Managers. Moyle is co-author of *Cryptographic Libraries for Developers* and *Practical Cybersecurity Architecture*, and a frequent contributor to the information security industry as an author, public speaker, and analyst.

In practice, this means that our perceptions of risk associated with new technology might be out of line with the actual objective, empirical risk. Any new technology introduces new risk—no technology is completely risk free—but in some cases the risk factors introduced are offset by the mitigation of current risk such that the cumulative net effect is overall reduction in risk to the organization depending on factors such as usage, what is being replaced, changes to business processes and more. Will this always be the case? Of course not. Some technologies might be new enough that the attack surface is still emerging; or there might be nascent design flaws that have yet to be fully exposed (consider the early days of Wired Equivalent Privacy [WEP)] as a proof point for this.) But the overall point is that, in some cases, even though it might not feel that way to us because of the familiarity principle, empirical analysis supports risk reduction if used strategically.

What this means then, is that we—as the enablers of digital trust in our organizations—should look for areas where we can squeeze the most risk reduction out of the technologies we deploy. In other words, in situations where there is new technology in the offing, it is incumbent upon the practitioner to both objectively analyze the risk and evaluate the technology for its potential in reducing risk and enabling trust. One example of this is Infrastructure as Code (IaC). When used strategically, IaC can actually help achieve digital trust outcomes. It is worthwhile to look at some circumstances in which this is true and consider how IaC can be harnessed to strengthen our trust posture.

What Is IaC?

IaC refers to technologies that allow the provisioning and configuration of workloads (usually in a cloud context) to be assigned through the use of human and machine readable artifacts. Technologies include Hashicorp's Terraform, AWS CloudFormation, Salt (i.e., SaltStack), Puppet, Ansible and others.

Through the use of IaC, developers and administrators can automate the provisioning and configuration management of cloud workloads and even on-premises nodes. Instead of manually provisioning, configuring and, ultimately, maintaining workloads (e.g., in virtual machines or containers), they instead author code that, when parsed by a supporting framework, automatically creates and configures the desired resource.

Why is this advantageous? In modern environments (particularly cloud), it automates provisioning and configuration, which is necessary for DevOps/DevSecOps toolchains to stage and field changes automatically. So, instead of there being a manual step required for an engineer to build out and configure test, staging, and production environments, the necessary process can be almost fully automated. It also helps eliminate configuration "drift," which allows individual production systems to develop unique "personalities" through the application of direct administrator actions. (Drawing on the famous adage, it helps foster a "cattle not pets" mindset.) This means less time is required to debug quirks on a given node thanks to a reliable baseline configuration. And, it helps to ensure that documentation exists, and that the documentation matches what is fielded.

So, what does IaC look like? As an example to illustrate IaC, an administrator or developer might author a declarative statement like the Terraform snippet below. Terraform is used in the examples here because it is one of the more popular approaches, but the concepts apply equally to other IaC technologies:

```
resource "google_compute_instance" "default" {
    name     = "example-vm"
    machine_type = "f1-micro"
    zone     = "us-central1-c"
    tags     = ["ssh"]
    metadata = {
     enable-oslogin = "TRUE"
    }
   ...
```

> IaC directly supports the ability of practitioners to conduct reviews and/or assessments of the resources and workloads described in IaC artifacts.

This simple example illustrates the definition of an Infrastructure-as-a-Service (IaaS) compute resource which, in this case, is a small workload deployed into Google Cloud Platform (GCP). It should be noted, however, that this is not a complete example. Several important details have been left out for the sake of brevity, including:

- The network interface
- The configuration of the resource
- The storage volume(s) it will use
- Some critical supporting elements such as informing Terraform of the provider to be used, which allows the framework to understand the context and, in turn, understand GCP resources

While it is simplified, the example is sufficient to illustrate what IaC is for those who are not already familiar with the concept.

IaC as a Pillar of Digital Trust

For those concerned with digital trust (i.e., our confidence in the technology components that enable our businesses and support the way we live), there are several very important benefits that a shift to IaC can bring about. These include:

- Transparency in review and assessment; source of objective truth
- Assistance creating documentary artifacts
- Compliance and audit support

It is helpful to unpack what is meant by each potential benefit and examine how IaC can help bolster trust. It is important to note, though, that this is not intended to be an exhaustive list of all possible benefits. Specific business contexts, circumstances, usage or other details unique to an enterprise can potentially facilitate dozens (or more) of additional benefits. The items listed here are likely to apply to most usage contexts.

Transparency in Review and Assessment

IaC directly supports the ability of practitioners to conduct reviews and/or assessments of the

LOOKING FOR MORE?

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

IaC can help bring trust to an environment rather than being seen as a new source of risk.

resources and workloads described in IaC artifacts. Consider the sample used herein for the GCP IaaS resource. One does not have to look closely to know exactly what kind of workload it is (f1-micro VM), where it is located (us-central1-c), what its name is and so on. Had the full definition been included, we would know what volume(s) are attached to it, what configuration state it is in (e.g., if it is bootstrapped through a shell script or similar), network details and so forth.

For auditors, security professionals, or other technologists, the value of this should be obvious. Instead of having to interview staff, read through stale/obsolete architecture documentation, or gather information empirically through testing (e.g., vulnerability scanning, penetration testing), we can go directly to the source. Many IaC technologies even keep a running state definition that can be queried to get information about the current state. For governance, risk and privacy practitioners, the ability to view (in many cases at a glance) policy adherence all the way down to the technical level can give them a tool set to which they otherwise would not have access.

Assistance Creating Documentary Artifacts

The second benefit is in the advantage that IaC provides in facilitating the creation of diagrams, documentation and other derived artifacts. Rather than manually creating diagrams (that are usually stale hours or days after they are finished), IaC enables automated creation of certain types of diagrams. Going back to the Terraform example, tools such as open source projects Blast Radius[2] or InfraMap[3] can be leveraged to "automagically" create diagrams based on the HCL (the language used by Terraform) or the state information maintained by Terraform. Similar projects exist for other IaC technologies as well.

From a security practitioner point of view, imagine how much more quickly tasks such as application threat modeling can be accomplished when we have support for the creation of dataflow diagrams. For audit professionals, consider how much easier it is to understand the workings and interconnections between system components when we have a reliable diagram to draw upon. And, for compliance and governance professionals, keep in mind that a current and well-maintained diagram is a line-item requirement in some regulations (e.g., the Payment Card Industry Data Security Standard [PCI DSS] 1.1.2 and 1.1.3) in addition to being implicit in others.

Compliance and Audit Support

Last, IaC can help directly advance regulatory compliance and help with (third-party) audit responses. In addition to the compliance benefits potentially engendered by the creation of automated diagrams, keep in mind that not only actual state information (e.g., Terraform running state—tfstate[4]—using the earlier examples) but also the IaC artifacts themselves can be used as evidence to support the existence of configuration management controls, segregation of duties (SoD) (since the actual effecting of change is done through the tool rather than by human engineers), and other controls.

From the auditor or compliance practitioner perspective, again, it should be obvious why this is valuable. Instead of having to search for evidence to prove the implementation, scope and effectiveness of particular controls, we can (assuming our usage enforces those controls) produce instead the IaC artifacts or query state, or otherwise utilize the IaC framework to provide evidence.

The short version of all this is that IaC can help bring trust to an environment rather than being seen as a new source of risk. Because of the way it works, it can be strategically employed to reduce risk in many cases. This is particularly true when practitioners participate early and work in lockstep with technical development and operational teams on planning how IaC is to be used. This lets stakeholders leverage the properties of IaC to help advance trust goals and risk reduction. In fact, those who see how IaC can help and become accustomed to the value it can provide might become active champions for it inside their organization, promoting it and advocating for it with colleagues to help spread its use.

Endnotes

1. Staff, "Why Do We Prefer Things That We Are Familiar With?" *The Decision Lab*, *https://thedecisionlab.com/biases/mere-exposure-effect*
2. GitHub, 28mm/Blast-Radius, *https://github.com/28mm/blast-radius*
3. Gitub, Cycloidio/Inframap, *https://github.com/cycloidio/inframap*
4. Terraform, State, *https://developer.hashicorp.com/terraform/language/state*

Defining, Establishing and Measuring Digital Trust

At the time of this writing, there is a huge news story about possible cheating in the world of international chess.[1] Claims of cheating in chess are not exactly new. So why is this particular story so prominent? There are several reasons. First, one of the parties in the scandal is the reigning world champion, and he is the one leveling the cheating charge. Second, the one being accused has been caught cheating before. It is the second reason that is of particular interest because it has to do with trust. This individual has broken trust before. He has damaged his own reputation, having been caught cheating. As a result, people are more accepting that he cheated this time around, even though no proof has been presented and no method has been suggested, other than one that would typically be found in less-than-reputable news magazines. If the accused were a chess grandmaster who had never been shown to have cheated, likely more people in the world of chess would have demanded tangible proof of the cheating claim.

Trust, from an organizational perspective, is crucial to success. However, the nature of trust is shifting. More and more, transactions happen digitally. In some cases, relationships between organizations may be solely digital, with no physical interaction required in this era of digital signatures and the like. If an organization should violate trust in some way, news of that violation can fly immediately to everyone connected digitally, meaning an organization can acquire a tarnished reputation incredibly quickly. Therefore, trust, and especially digital trust, is critical. Digital trust is simply trust in a digital context. But the root word in that phrase, "trust," represents a nebulous concept. What defines and comprises trust? What about digital trust? Are there ways to improve the digital trust in our organizations? Are there methods to measure the trustworthiness of other organizations?

Can Digital Trust Be Measured?

I do believe that trust, and especially digital trust, can be defined and measured. Back in 1998–1999, when I was a young officer in the US Air Force serving as a project manager on commercial IT contracts, one of the key questions that plagued us was, "How do we measure a vendor's reputation to deliver on a contract?" We were asking that question because we had recently faced a situation in which one of our vendors for a key contract stopped shipping orders due to the company's acquisition by a larger organization. We had another vendor that also stopped shipping orders not only on our contracts, but on some contracts for sister agencies. We decided then that it was a good idea to apply a

K. BRIAN KELLEY | CISA, CDPSE, CSPO, MCSE, SECURITY+

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

"measuring stick" based on vendor performance. Ideally, this would be across the entirety of the US Department of Defense. Even back then, we were starting to define the criteria by which vendors could be measured.

Recently, I was having a similar conversation with my organization's third-party vendor management personnel. They were evaluating artificial intelligence (AI) products designed to help with IT vendor risk management. There is simply too much information to process nowadays. As a result, AI is being touted more and more to fill the gap.[2] If AI is involved, that means we do have ways to model or measure a vendor's reputation.

Digital Trust Is Not Just About Cybersecurity

Naturally, an organization's cybersecurity posture is a factor in overall digital trust. We want to keep the bad actors out and/or minimize their impact. That is what cybersecurity is for, and it is important to the overall success of an organization. After all, if an organization's cybersecurity posture is viewed as weak, or worse, it will affect the bottom line. A good example is the impact on profits for Target in 2014 after its highly publicized breach.[3] Poor cybersecurity equals poor reputation equals poor digital trust.

By increasing digital trustworthiness in individual organizations, we can expect the overall digital ecosystem to improve as well.

However, if you think about where IT vendor management is going, cybersecurity is just one of several factors third-party management professionals must consider. After all, an organization might have one of the world's best cybersecurity practices, but if it is terrible at shipping quality products, most organizations will rate it as an unacceptable business partner and it will develop a poor reputation. In short, the organization's digital trust rating will be near the bottom even with an incredible cybersecurity posture.

A Digital Trust Ecosystem Framework

ISACA® has developed a framework for digital trust, called the Digital Trust Ecosystem Framework (DTEF). It is safe to say that ISACA believes digital trust is critical in today's modern digital environment.[4] The DTEF is a means of identifying what organizations should focus on with regard to digital trust. For instance, here is the DTEF sets forth a common working definition of digital trust :

> *Digital trust is the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, processes, information and technology to create and maintain a trustworthy digital world.*[5]

Crucial to the framework is its definition of ecosystem. In the DTEF, a digital trust ecosystem is made up of:

1. Relationships
2. Relationship mediums (i.e., how those relationships are conducted)
3. Activities (i.e., what an organization does digitally)
4. Stakeholders (i.e., customers, suppliers, peers)
5. An organization's ethics, reputation and privacy

Of course, there is much more detail within each of those five areas.

We Have to Implement Yet Another Framework?

In short, no. The DTEF is designed to encapsulate what goes into an organization's digital trust posture. Is the organization operating securely online? Is it handling data, especially sensitive and private data, in an ethical way? Is it collecting just the data it needs to operate, or is it capturing more than it should? Is the organization conducting its relationships with peers in a generally acceptable manner? Does the organization produce quality products? How does the organization treat its customers?

Like other frameworks, the DTEF is designed to function as scaffolding to help an organization meet certain expectations. In the case of the DTEF, the expectation and goal is a trustworthy digital ecosystem. The framework itself does not get an

LOOKING FOR MORE?

- Read *Digital Trust: A Modern Day Imperative. www.isaca.org/resources/white-papers/digital-trust-a-modern-day-imperative*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

organization there—the people, processes and core values of the organization do. Even if an organization does not formally adopt the DTEF, the organization can look at the DTEF as another tool to help better define and improve its digital trustworthiness. By increasing digital trustworthiness in individual organizations, we can expect the overall digital ecosystem to improve as well. That should be our overall goal, after all. I personally want a digital landscape where my transactions are safe and trustworthy. I want to interact with organizations that adhere to the same ideals. I would harbor a guess that most people feel likewise.

Where We Go From Here

Digital trust is crucial as we continue the shift to digital transactions, digital interactions and a heavier digital experience. There are a great many bad actors who seek to harm this digital ecosystem, but we need to think beyond them. We must look at how our own organizations stack up on the digital trust scale. We also have to consider what level of trust we can put in organizations we interact with digitally. This is about overall digital reputation, a paradigm shift from the industry focus on cybersecurity to counter bad actors. Cybersecurity is critical to overall reputation, but it is not the only factor.

Given that digital trust is an abstract concept, we do need to define it as clearly as possible. We also need some means of determining how trustworthy an organization is in the digital ecosystem. ISACA has a framework to help with that, but this is about more than a framework. The focus and overall goal is for a trustworthy digital world. Going forward, in this column we will focus on that goal as we delve into issues, events and components that affect digital trust and the digital ecosystem.

Endnotes

1 Kumar, A.; “Inside the Chess Cheating Scandal and the Fight for the Soul of the Game,” ESPN, 6 October 2022. *https://www.espn.com/espn/story/_/id/34736588/inside-chess-cheating-scandal-fight-soul-game*

2 Dambrot, J.; “Streamlining Third-Party Risk Management With AI,” KPMG, 2021, *https://advisory.kpmg.us/blog/2021/streamline-third-party-risk-ai.html*

3 Harris, E. A.; “Data Breach Hurts Profit at Target,” *The New York Times*, 26 February 2014, *https://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html*

4 ISACA®, “Empowering IT Professionals to Advance Digital Trust,” USA, 2022, *https://www.isaca.org/digital-trust*

5 ISACA, *Digital Trust Ecosystem Framework: Introduction and Approach*, USA, 2022, *https://www.isaca.org/digital-trust*

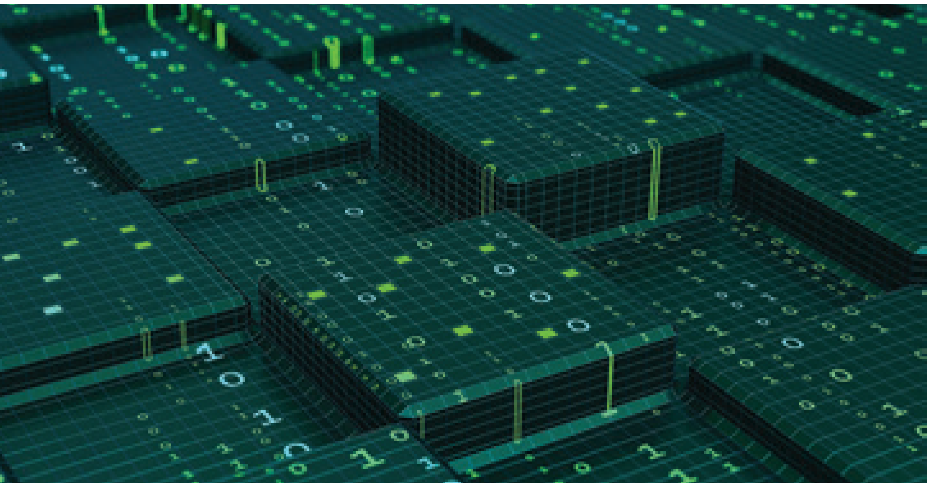
Reality Check: The Use of Big Data and Predictive Data Models

日本語版も入手可能
www.isaca.org/currentissue

Humans have long been enamored with the idea that if they can just feed enough data about the past into a machine—whatever that machine is—it can predict what will happen in the future. In a 1984 episode of the US animated television show *The Transformers*, the Autobots look for an elusive space bridge to their home planet, Cybertron. Their human friend, an archetypal whiz-kid named Chip Chase, informs them that:

> *[B]y feeding Teletraan 1* [the Autobots' supercomputer] *all the data we have about the space bridge's last appearance, I might get it to predict where the bridge will appear next.*[1]

It works. If only reality were as straightforward as cartoons.



KEVIN M. ALVERO | CISA, CDPSE, CFE

Is senior vice president of internal audit, compliance and governance at Nielsen Company. He leads the internal quality audit program and industry compliance initiatives, spanning the enterprise's global media products and services.

The idea of using vast amounts of data to anticipate what is going to happen is not new. However, the power, precision and affordability of predictive models are increasing based on the increasing volume and availability of data in general and the computing power of the cloud. More organizations are going to be faced with tough questions and issues related to the real-world use of such models—discussions that may previously have taken place on a more hypothetical level.

For many enterprises…investing in predictive data modeling is a worthwhile pursuit that can increase customer satisfaction, improve efficiency and even help save lives.

The notion that every organization is sitting on a veritable crystal ball in the form of untapped data is a fantasy. However, for many enterprises across a broad range of industries, investing in predictive data modeling is a worthwhile pursuit that can increase customer satisfaction, improve efficiency and even help save lives. But to realize this value, organizations must deal with some down-to-earth and sometimes messy realities.

Data Security and Integrity

Cybersecurity remains at or near the top of every organization's risk register. The threats to data security and integrity are increasing from within organizations (e.g., complexity of data governance, conflicting priorities, neglect) and from the outside (e.g., malicious acts, lack of control over third parties). At the same time, the stakes accompanying a data breach are growing in terms of potential financial and reputational damage and legal/regulatory liability.

According to a 2022 Protiviti report:

> *IT audit teams, as well as other departments (e.g., legal, compliance, IT), are scrambling to keep pace with new data privacy and data security rules as well as changing legal and regulatory compliance requirements that have growing implications for organizational data management and technology-related activities.*[2]

Particularly as it relates to sensitive data, the fundamental question is whether the value the organization is getting from these data is worth the risk of ownership. To answer that question, top leadership must have a clear and shared understanding of how predictive modeling is expected to support the organization's mission, strategy and core values. At the same time, the capacity for predictive modeling to impart value to the organization is directly related to the quality and integrity of the data that are input into the models. Therefore, a strong sense of purpose and a commitment to data security and integrity must be in place from the top down for organizations to avoid dabbling in, or lunging after, the prospective benefits of predictive data modeling in a manner that puts the organization at excessive risk.

Bias, Privacy and Other Ethical Concerns

Members of the general public have become increasingly concerned that the personal data organizations collect (with or without consent) will be used in ways that violate their right to privacy or their right to fair and equitable treatment. Anticipating people's thoughts and actions too well can be downright creepy, and it can negatively impact their perception of a brand and its level of trust. Voicing that concern has led to change, both in government and in the marketplace. A 2022 *Harvard Business Review* article notes that:

> *Until now, companies have been gathering as much data as possible … often without customers understanding what is happening. But with the shift towards customer control, data collected with meaningful consent will soon be the most valuable data of all, because that's the only data companies will be permitted to act upon.*[3]

Leadership must be able to determine if available data are relevant to the prediction they are trying to make, and if it is worth the risk and cost of acquiring, accessing, storing and including that data in the modeling.

In addition to the increased focus on privacy, there is a greater demand for transparency to ensure that organizations that utilize advanced data analytics are treating people fairly and equitably. In particular, this concern is relevant to a type of predictive data modeling called clustering, in which data (and the people that data represent) are placed into various groups based on their common attributes. In addition to targeted advertising:

> *…other use cases of this predictive modeling technique might include grouping loan applicants into 'smart buckets' based on loan attributes, identifying areas in a city with a high volume of crime, and benchmarking [Software-as-a-Service] SaaS customer data into groups to identify global patterns of use.*[4]

At one level, this seems intuitive and reasonable. If the purpose of advertising is to inform people about products and services they might want, then using information about those people to improve the odds of suggesting relevant products to them only makes sense. The same could be said about applying the known, historical likelihood of a destructive event occurring to the decision of how much a customer should have to pay for insurance against that event.

However, when organizations make determinations (even well-supported ones) about whether certain clusters of people can, should or would want to do certain things, they risk crossing the line between prudent risk management or beneficial tailoring of the customer experience and discrimination. The data economy, "was structured around a 'digital curtain' designed to obscure the industry's practices from lawmakers and the public … [but] that curtain has since been lifted."[5] Therefore, organizations must understand how their model-powered decision-making processes will tolerate this sunlight and, more important, consider proactively how their use of predictive data modeling aligns with their core values.

LOOKING FOR MORE?

- Read *Data Science Fundamentals Study Guide.* *www.isaca.org/credentialing/itca/data-science-fundamentals-certificate*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Data Relevance

Forecasting is another common use case for predictive modeling. Although organizations have traditionally used historical data to anticipate demand, the comprehensiveness and immediacy of information that can be included in the calculation necessitates a new level of scrutiny over the relevance of data. In the past, an enterprise had, perhaps, transaction volume, returns data, customer loyalty program data, foot traffic statistics and some demographic data, but now there exists the ability to incorporate a much wider variety of variables into the computation with real-time trending. The fundamental problem thus shifts from needing more data to determining where to draw the line. Leadership must be able to determine if available data are relevant to the prediction they are trying to make, and if it is worth the risk and cost of acquiring, accessing, storing and including that data in the modeling on the premise that doing so could make forecasts even incrementally more accurate.

Organizational leaders must seriously consider whether they have, or can acquire, the skilled workers needed to execute their strategies for predictive modeling.

Disruption

It is also important for business leaders to fully comprehend the ongoing commitment to monitoring that is required for the responsible and effective use of predictive models. Such models cannot simply be deployed and left to run at the risk of developing biases that could impair their decision-making and expose the business to risk.

Ensuring that changes in the marketplace or the broader world do not break data models necessitates vigilance, but it also requires that resilience be an upfront consideration in the early stages of planning the development and use of a predictive model. In short, the model must be built with the assumption that the environment in which it ultimately performs will change frequently postdeployment in ways that may not have been foreseen during development. These are key factors in the return on investment (ROI) equation that business leaders must understand before embarking on a predictive modeling initiative.

ROI

For organizations in certain industries, investment in advanced data modeling algorithms will almost certainly be worthwhile. However, the organization must still be able to quantify its ROI. The ability to better anticipate ROI can have numerous quantifiable benefits, including:

- Less waste resulting in lower costs
- Fewer inefficiencies and useless procedures
- Reduction in costly or dangerous delays
- Improved quality with fewer errors

For example, when it comes to emergency response or disaster preparedness, better predictive models can literally translate to lives saved. However, in other situations, the cost-value picture is less clear. For example, a taxi or ride-sharing service could benefit greatly from the ability to analyze vast amounts of consumer and marketplace data to predict—as accurately as possible—the timing of an event that will draw prospective customers and precisely how many. On the other hand, a brick-and-mortar storefront managing inventory levels can probably predict demand well enough simply by tracking historical sales data, meaning that investment in advanced predictive models is likely not worth the cost.

Moreover, customer demand for forward-thinking experiences that help them make better decisions and actions “doesn’t always suggest a predictive solution.”[6]

This speaks once again to the need for leadership to understand how increased accuracy and insight from predictive models can benefit the organization and, even better, to be able to quantify those benefits before investing in predictive technologies.

Organizational Skills and Expertise

It is expected that 97 million jobs involving artificial intelligence (AI) will be created between 2022 and 2025.[7] “AI has the potential to transform every industry…however, businesses are still struggling to find employees with the skills necessary to create, train and work alongside intelligent machines.”[8]

Although demand for skilled workers in the field reportedly has been quickly outstripping supply, the problem of organizational skills and expertise related to predictive modeling is not strictly a hiring problem. According to research by the Massachusetts Institute of Technology (MIT) (Cambridge, Massachusetts, USA) Center for Information Systems Research:

> *Creating successful artificial intelligence programs doesn't end with building the right AI system. These programs also need to be integrated into an organization, and stakeholders—particularly employees and customers—need to trust that the AI program is accurate and trustworthy.*[9]

This, the researchers conclude, is the case for building enterprisewide AI explainability.[10]

Organizational leaders must seriously consider whether they have, or can acquire, the skilled workers needed to execute their strategies for predictive modeling. They must also determine if they can raise the level of literacy within their organization to realize the full potential benefits of predictive modeling.

Conclusion

Anybody who has ever researched a potential investment opportunity has been somberly reminded that past performance is not indicative of future results. Nevertheless, for many organizations, gaining the power to anticipate the needs of individual customers ever more accurately and foresee shifts in the broader marketplace is worth tackling the unknowns and potential pitfalls associated with advanced predictive data models.

Research shows that:

> *Most large firms already suffer from a series of internal tensions over customer data…and up to 90 percent of current IT budgets are spent simply trying to manage internal complexities, with precious little money actually spent on data innovation that improves either productivity or the customer experience.*[11]

That type of dysfunction cannot be overcome by an algorithm, no matter how sophisticated. Rather, it requires commitment, a clear strategy and well-aligned goals to ensure that any predictive model is built on a solid foundation.

Endnotes

[1] *The Transformers*, Season 1, Episode 6, "Divide and Conquer," directed by John Walker, written by Donald F. Cohort, 20 October 1984, syndicated

[2] ISACA® and Protiviti, *IT Audit Perspectives on Today's Top Technology Risks*, USA, 2022, *www.isaca.org/it-audit-2022*

[3] Rahnama, H.; A. Pentland; "The New Rules of Data Privacy," *Harvard Business Review*, 25 February 2022, *https://hbr.org/2022/02/the-new-rules-of-data-privacy*

[4] Insightsoftware, "Top Five Predictive Analytics Models and Algorithms," 1 January 2022, *https://insightsoftware.com/blog/top-5-predictive-analytics-models-and-algorithms/*

[5] *Op cit* Rahnama and Pentland

[6] Blanchard, B., *et al*.; "Predictive Modeling and Influencing Customer Behavior," Microsoft, *https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/innovate/considerations/predict*

[7] Marr, B.; "What Are the Most In-Demand AI Skills?" *Forbes*, 13 June 2022, *https://www.forbes.com/sites/bernardmarr/2022/06/13/what-are-the-most-in-demand-ai-skills/?sh=4682e7b3249c*

[8] *Ibid*.

[9] Brown, S.; "Why Companies Need Artificial Intelligence Explainability," Massachusetts Institute of Technology (MIT), Swan School of Management, Cambridge, Massachusetts, USA, 21 September 2022, *https://mitsloan.mit.edu/ideas-made-to-matter/why-companies-need-artificial-intelligence-explainability*

[10] *Ibid*.

[11] *Op cit* Rahnama and Pentland

Toward Rebuilding Data Trust

日本語版も入手可能
www.isaca.org/currentissue

External auditors should be trusted members of the business community. They analyze structured data (e.g., log files, transaction records) and unstructured data (e.g., interview responses and reports) to draw conclusions about the veracity of an enterprise's systems and controls for cybersecurity, compliance and quality, and finance. Ultimately, they provide assurance—to the public, in some cases—that an enterprise is well managed.

However, some of the world's biggest audit firms are struggling with their most important obligation: to be a trusted source of independent information about the state of an enterprise. The Enron and WorldCom scandals have not been forgotten, and there has been a series of more recent high-profile events: One of the world's largest audit firms is being sued for US$830 million and has been charged with misconduct,[1, 2] and two other leading audit firms have been caught cheating.[3, 4]

As audits become more data-driven, audit firms can be exposed to risk if the client enterprise fails to adhere to good data management practices. A key question for the data-driven auditor is how to assess the reliability (e.g., accuracy, completeness) of the data captured by a client's system and the methods of data acquisition used by that system.[5] This question applies not only to auditors, but also to banks, insurers, securities traders, retailers, telecommunications organizations and even social media enterprises—all entities that people trust with their data.

The data trust domain is vast (**figure 1**), even as a subset of the immense digital trust domain. Poor data management in general, and poor data quality in particular, can have negative impacts on data trust and, thus, on digital trust. But there are steps enterprises can take to improve their overall levels of trust based on the data management discipline and the principles of trustworthiness.

The Poor State of Organizational Trust

The world is becoming less trusting partly because of failures related to poor data management. The Facebook-Cambridge Analytica scandal is a case in point, specifically from a privacy perspective.[6] Businesses are actually the most trusted organizational type—more trusted than nongovernmental organizations (NGOs), governments and media.[7] However, there is a global trust crisis in business, with two thirds of senior executives believing that trust between people and the enterprises and institutions they deal with is declining because of enterprise data misuse, corporate scandals and misrepresentations of the truth.[8]

This is not a recent phenomenon. Trust in the US government has been declining for 70 years.[9] Trust has simultaneously been declining in business enterprises, media and NGOs since 2017, with the average level of trust across dozens of countries in all four organizational categories combined being less than 50 percent.[10]

The Poor State of Data Trust

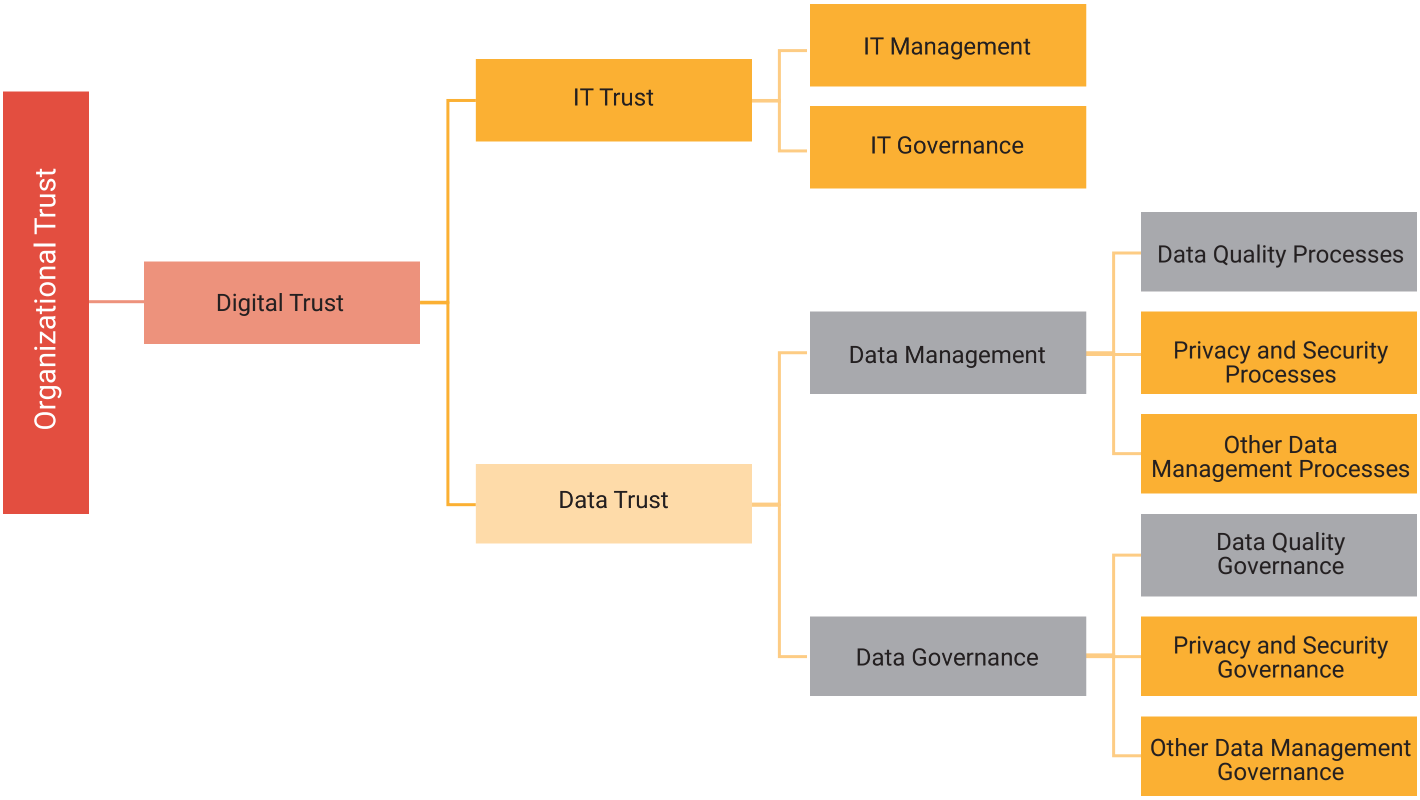
When discussing data trust in a digital trust context, a useful analogy is that data are like water and IT is like plumbing. Data trust is like trusting that the water is

GUY PEARCE | CGEIT, CDPSE

Has an academic background in computer science and commerce and has served in strategic leadership and governance capacities mainly in the services sector; IT governance; and enterprise governance capacities, mainly in financial services. He is a career-long digital innovator balancing the creation of two-way value—customer and organization—while ensuring the effective integration of emerging technology and its beneficial adoption. He has been active in digital transformation since 1999, focusing on the people and process integration of emerging technology into organizations to ensure effective adoption. Pearce was first exposed to artificial intelligence (AI) in 1989, and he has followed the evolution of the discipline from symbolic AI to statistical AI during the intervening decades. He was awarded the 2019 ISACA® Michael Cangemi Best Author award for contributions to IT governance, and he consults in sustainable IT architectures and the respectful, compliant use of data bounded by sound governance, digital transformation, data governance and IT governance.

FIGURE 1

Data Trust Domain



potable, and IT trust is like trusting that the plumbing functions properly. Just as water cannot flow or be stored without the right plumbing, data cannot flow or be stored without IT. Digital trust is about trusting the entire data and IT ecosystem.

Whereas "digital trust focuses on how trust manifests in a digital context,"[11] data trust is exclusively about the data context of the digital ecosystem, including, but not limited to, the data components of privacy and security. Data trust includes data management aspects such as data quality, metadata management, master and reference data management, content management (unstructured data) and data consumption mechanisms (e.g., reporting, analytics, artificial intelligence [AI]). Specifically, data trust means that data management activities produce verifiably healthy data.

More than three quarters of consumers say that sharing data with enterprises is a necessary evil.[12] Worse, 78 percent of consumers say their trust in an enterprise's ability to protect their data has stayed the same or declined over the past two years.[13] Worst of all is that 55 percent of enterprises believe that consumers' trust has increased over the same period.[14] There is clearly significant dissonance between enterprises and their customers when it comes to data trust.

The use of third-party personal data—when an enterprise buys personal data from another enterprise to augment its own data on individuals—has been identified as a major cause of declining trust.[15] It can lead to inaccurate representations of customers because of inaccurate data and the guesswork involved in merging data and possibly not following regulations. In addition, the purchase, processing and use of the integrated data are not transparent to the end user, and transparency is a requirement for building (or rebuilding) organizational trust.[16]

However, it is important to note that trusted enterprises do not need transparency.[17] Rather, distrusted enterprises need transparency to recover from distrust. The current president of the European Central Bank and former chair and managing director of the International Monetary Fund reinforced this sentiment by saying, "In my experience, the best tonic for depleted trust is heightened transparency."[18] In other words, transparency is needed where trust has been eroded, not where trust is intact. For example, the medical profession is considered a bastion of trust, so

one trusts a physician's opinion without demanding transparency about how that opinion was reached.

But data trust involves more than transparency; it also includes value delivery and acceptance of consequences—that is, the trust a person places in an enterprise's data practices.[19] Consequence acceptance is a major element of data governance through an enterprise's culture and its management structures, specifically insofar as they relate to accountability and responsibility.

There are many critical attributes for effective data management that are missing in enterprises that are struggling with data management initiatives.

Data trust requires healthy data, and healthy data are clean, appropriately accessible, understandable, up-to-date and traceable.[20] Each of these criteria is a subset of effective data management. In other words, well-managed data drive data trust; unhealthy data—that is, data with lower than desired levels of quality because of poor data management—cause low levels of data trust.

The Poor State of Data Management

In general, data management details the tasks and activities required for a healthy data environment, while data governance defines accountability and responsibility for those tasks and activities based on a defined policy and, generally, with respect to defined processes. Both elements are in response to a data strategy aligned with an enterprise's overall strategy.

The Capability Maturity Model Institute (CMMI) found that ineffective data management negatively impacted 100 percent of the technology failures it surveyed, and technology initiatives experienced a 50 percent failure rate.[21] An academic study of the factors causing the failure of AI projects found that earlier studies cited data management issues as a significant factor.[22]

Although these findings are indicative of failure on the process side of data management, failure is also happening from a people and governance perspective. For example, the 2010 promise of big data being key to competition remains unfulfilled because enterprise leaders still have not recognized that data are important to everyone, not just a few data-oriented managers.[23] A decade later, the tide may finally be turning, with a renewed focus on self-service business intelligence and data democratization—making data accessible to all, "irrespective of their technical know-how"[24] and giving them appropriate permissions—increasingly enabled by metadata-driven data fabric platforms and the domain-led data products of data mesh architectures.

The overall result of these failures is that 90 percent of data governance projects fail to perform well.[25]

There are many critical attributes for effective data management that are missing in enterprises that are struggling with data management initiatives, including:[26, 27, 28]

- Senior executive sponsorship
- Clear objectives linked to measurable organizational value; half of all enterprises do not assess, monitor or measure their data governance initiatives[29]
- Integrated data strategy with a shared language and consistent expectations shared by all relevant stakeholders
- Focus and commitment; that is, attention to the meaningful rather than the menial
- Manageable scope driven by prioritization
- Defined operational accountabilities and responsibilities and shared responsibility for operational success

LOOKING FOR MORE?

- Read *Defending Data Smartly. www.isaca.org/defending-data-smartly*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

- Data governance and data management expertise
- Recognition that data management is an ongoing operational responsibility, not just a project
- Balanced rather than overt focus on tools and technology
- Focus on communication, transformation and change management from the start

Many of these attributes are related to data governance. For example, the UK government's coronavirus data were flawed and misleading, negatively impacting public understanding and government decision-making.[30] One of the problems was termed a technical glitch that led to thousands of positive results being omitted from the calculation of national coronavirus cases. The glitch was said to be "a data file exceeding its maximum file transfer size."[31] There were other issues as well, such as inflated figures that necessitated recalculation.

Given this assessment, it seems that some of the data governance questions not asked or answered may include:

- Who was responsible for validating the file transfer?
- Was there a process in place for that person to follow with respect to file identification and data transport validation? If so, was the process approved?
- Was the process for calculation validated by the identified stakeholders?
- Were there clear and agreed-on definitions for variables such as dates (e.g., day of report vs. day of death) and when data were to be captured, including accommodation for weekends? If so, were the definitions approved?
- How were data inputs and data outcomes approved? Attestation or certification? (Presenting data without supporting information means that interpretation is left to the observer.)

Even if data management (the process) is sound, failures in data governance (accountability and validation) can mean that all data-reliant efforts come to naught. Data management and data governance need to function in tandem for data to be sustainably fit for purpose.

Even if data management (the process) is sound, failures in data governance (accountability and validation) can mean that all data-reliant efforts come to naught.

The Poor State of Data Quality

Given the poor state of data trust and data management, it should be no surprise that data are unhealthy. Poor data quality cost the US economy US$3 trillion in 2016, a cost driven by decision makers, managers, knowledge workers and data scientists having to accommodate unhealthy data in their everyday work.[32] The accommodation of unhealthy data by these individuals includes understanding, correcting and preparing the data to make them usable for their intended purpose.

Assuming that the causes of dirty data (a subset of unhealthy data) are similar in all large developed economies, the cost of dirty data for all countries in 2016 can be estimated as:

$$\text{Estimated Cost of Dirty Data}_{\text{In 2016}} = \frac{\text{Country}_{\text{GDP}_{\text{In 2016}}}}{\text{US}_{\text{GDP}_{\text{In 2016}}}} * \text{US\$3 trillion}$$

The gross domestic product (GDP) of the United States (the total economic value produced) in 2016 was US$18.7 trillion.[33] Using this equation, the cost of dirty data for other major economies can be estimated (column B in **figure 2**). Large economies such as Brazil and China were excluded from this analysis because comparable data were not available from the sources used and because of their developing economic status.[34]

Next, it is possible to determine the impact of poor data quality on employees—that is, the extra work they must perform to clean and prepare data for use. Based on the number of economically active people in each country (column C in **figure 2**), the average cost of dirty data per employee can be calculated (column D in **figure 2**). Note that because the data for **figure 2** were collected in different years, this introduces a timing error into the estimate. Based on the average wage per employee (column E in **figure 2**),

FIGURE 2

Time Spent Cleaning Dirty Data per Employee in Selected Large Economies

Country	A	B (from the equation)	C	D = B/C	E	F = D/E
	GDP (in US$ Trillions, 2016)[a]	Calculated Annual Cost of Dirty Data in US$ Billions (2016)	Number of Employees in Millions (2021–22)[b]	Calculated Cost of Dirty Data per Employee per Year in US$ Thousands	Average Wage per Employee in US$ Thousands (2020)[c]	Calculated Average Percent of Time Fixing Data per Employee
United States	$18.7[d]	3,000[e]	158.1	19.0	69.4	27 percent
Japan	$4.9	786	67.2	11.7	38.5	30 percent
Germany	$3.5	561	45.4	12.4	53.7	23 percent
United Kingdom	$2.6	417	32.7	12.8	47.1	27 percent
France	$2.5	401	29.0	13.8	45.6	30 percent
Italy	$1.8	289	23.0	12.6	37.8	33 percent
Canada	$1.5	241	19.6	12.3	55.3	22 percent

Sources: a) World Bank, "GDP Current US$," *https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?order=wbapi_data_value_2010+wbapi_data_value+wbapi_data_value-last&sort=desc*; b) SME Finance Forum, "MSME Economic Indicators," *https://smefinanceforum.org/data-sites/msme-country-indicators*; c) OECD Stat, "Average Annual Wages," *https://stats.oecd.org/Index.aspx?DataSetCode=AV_AN_WAGE*; d) Countryeconomy.com, "United States (USA) GDP—Gross Domestic Product," 2016, *https://countryeconomy.com/gdp/usa?year=2016*; e) Redman, T. C.; "Bad Data Costs the U.S. $3 Trillion Per Year," *Harvard Business Review*, 22 September 2016, *https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year*

the average percentage of time each employee spends on data quality issues can be calculated (column F in **figure 2**). Some jobs involve more work with data than others, but the average provides an estimate of the extent of the problem at the per-person level.

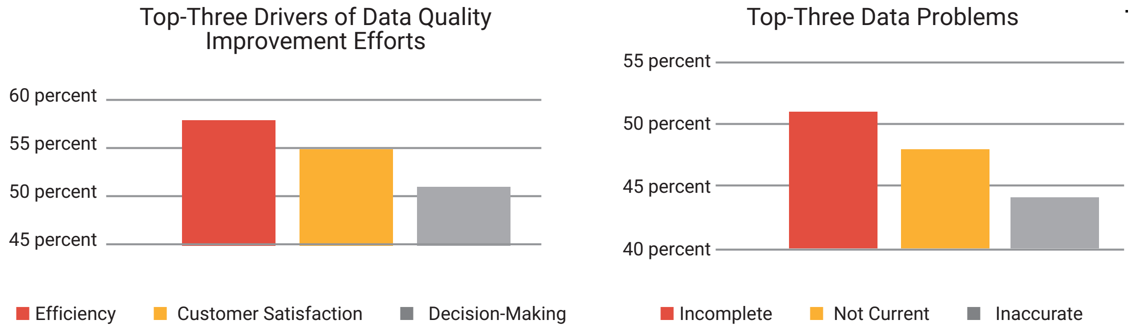
This means that between one quarter and one third of the average employee's time is spent accommodating the vagaries of dirty organizational data—that is, up to one third of every day, week, month and year that could be better spent adding value to the enterprise's customers. The cost of dirty data is approximately 15- to 25-percent of revenue for most enterprises.[35] Reputational risk is often cited as a risk of dirty data,[36] and dirty data have damaged the reputations of 21 percent of enterprises.[37]

What initiatives are driving data quality improvement efforts, and what major problems are they attempting to solve? Fifty-eight percent of enterprises cite greater efficiency as a primary reason to improve data quality; 55 percent cite enhanced customer satisfaction; and 51 percent cite informed decision-making (**figure 3**).[38] Furthermore, enterprises struggle with data that are incomplete (51 percent), out of date (48 percent) or inaccurate (44 percent).[39]

The fact that the cost of poor data management can be quantified (in a top-down manner using enterprise-specific data, as shown in **figure 2**, but potentially in a bottom-up manner as well) means that making a business case for improving data quality is a good place to start. This should involve quantifying the benefits of addressing the issues.

FIGURE 3

Top-Three Data Problems and Reasons to Improve Data Quality



Restoring Data Trust: Where to Start

Poor data quality can compromise organizational economics, operations and customer trust. It can also be a powerful trust builder with the potential to increase trust in business by 3 percent and trust in government by 6.1 percent.[40] There is also a strong argument that better quality data can help close the income divide.[41]

Forty-two percent of respondents to one survey said that organizations are not doing enough to ensure trustworthy information.[42] By addressing data quality, a major part of that trust problem can be resolved.

There are several steps an enterprise can take to rebuild data trust:[43]

- Clean and validate data (data quality).
- Add operational metadata (data management).
- Secure private and sensitive data.
- Ensure data traceability (i.e., lineage and provenance; another aspect of data management).
- Ensure visibility and control of data management processes (transparency).

Increasing data trustworthiness depends on data that are:[44]

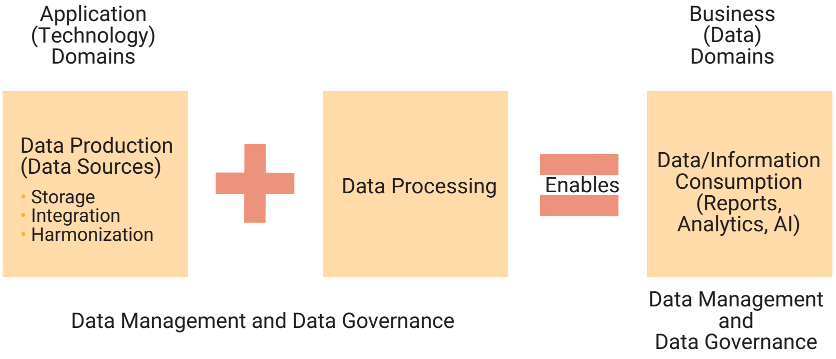
- **Transparent**—Verifiably clean and compliant
- **Thorough**—Providing a complete picture of the relevant domain
- **Trending**—A measurement of data consumption
- **Telling**—Verified and tested

Quality, transparency, traceability and verifiability are recommended points of focus for rebuilding data trust by means of a revised data management program. Thoroughness is an interesting consideration because it entails the best single view of the customer. Measuring data consumption is one of the greatest indicators of success. If nobody is using the platform, the reason is probably a lack of trust.

Many different stakeholders have roles to play in effective data governance, including those involved in data consumption (business) and data production (IT), because fit-for-purpose data are not just an IT function (**figure 4**). Indeed, data owner and data steward are both recognized data management roles. In addition, data consumers' participation in managing the problem fosters greater engagement and buy-in, which promotes trust and legitimacy.[45]

FIGURE 4

Data Production (Sources) vs. Data Consumption (Users)


Application (Technology) Domains
Business (Data) Domains
Data Production (Data Sources)
Storage
Integration
Harmonization
Data Processing
Enables
Data/Information Consumption (Reports, Analytics, AI)
Data Management and Data Governance
Data Management and Data Governance

In analytics, data trust is defined by four trust pillars: data quality, effectiveness of the analytics, integrity of data use (akin to data consumption) and resilience, which is concerned with long-term sustainability, optimization, governance and security.[46] In particular:

> *[R]esilience is key to winning customer trust. It only takes one service outage or one data leak for consumers to quickly move to (what they perceive to be) a more secure competitor.*[47]

Quality, transparency, traceability and verifiability are recommended points of focus for rebuilding data trust by means of a revised data management program.

Data resilience—which involves well-governed data management—is the cornerstone of digital resilience.[48] Data are in constant flux, which means that active risk management by means of appropriate controls is part of a full-fledged approach to data resilience.[49] Data and analytics are constantly evolving and, over time, there can be shifts in the way they are used, their impact and the risk they create.[50] These shifts can impact the data resilience of the enterprise. If they are not monitored, there can be serious negative repercussions.

Privacy and security are just two dimensions of data management; they should not be considered in isolation from the many other elements inherent in the management of data.

In terms of the interoperability of data resilience, it is important that enterprises ensure that their data operations are visible, which is part of trust building. Visibility facilitates identification of the interdependencies and interrelated risk factors across the entire data ecosystem.[51]

In terms of the robustness of data resilience, only 52 percent of 165 data and analytics decision makers surveyed indicated that data could be changed only by those authorized to do so.[52] The others indicated that anyone could change data. It is no wonder that data trust is in such a poor state.

From Third-Party Data to First-Party and Zero-Party Data

One of the challenges in building data trust is breaking the reliance on third-party data supply chains and ecosystems.[53] To limit liability, rebuild customer trust and create more accurate personalization, enterprises need to move away from the use of third-party data.[54] First-party data are the data an enterprise collects on individuals during the usual course of doing business, and zero-party data are data that customers willingly submit, such as by answering surveys.[55]

Growing regulatory pressure may reduce the market for third-party data and reverse the trend of negative experiences individuals have had over the years as a consequence of their use.

Data Trusts and Personal Data Stores

Lack of user, customer or citizen control over personal data in organizational hands fuels distrust.[56] Lack of control (e.g., data on Facebook, Google) leads to the wider problem of decreasing trust in government, institutions and other enterprises.[57] Data trusts and personal data stores (PDSs) are two of the most popular alternative data management models that support enhanced controls, with PDSs supporting enhanced user control.

Based on legal trusts, data trusts are structures that provide independent stewardship of data for an agreed-on purpose.[58] This is not a new concept, and much has been written about the subject. However, a public survey in the United Kingdom indicated that personal control, regulatory oversight and opt-out options were all preferable to data trusts.[59]

The preference for personal control brings PDSs to the forefront of the data management conversation. PDSs store an individual's data, and third parties have access only when the individual provides it. Blockchain-based personal identity products support PDSs. In one survey, PDSs were deemed preferable to six other data management models, with current data management methods scoring the lowest.[60]

Conclusion

Trust in businesses, governments, media and institutions has been declining for years, and trust in their abilities to manage and appropriately use customer data is following that downward trend. Furthermore, there is significant evidence that traditional data management is failing. A major part of this evidence is the poor state of data quality. Combined, these factors have negatively affected data trust, digital trust and overall organizational trust.

Data governance and data management are linked, yet privacy and security are considered mainly from a data management perspective. Missing is an active discussion about their governance, not only with respect to compliance, but also considering metrics such as trust, which are driven by defined responsibilities and accountabilities. Furthermore, privacy and security are just two dimensions of data management; they should not be considered in isolation from the many other elements inherent in the management of data.

To address issues of data trust, digital trust and, ultimately, enhanced organizational trust, the first step is to focus on a subset of data management—specifically, data quality and metadata—in addition to privacy and security. Other important aspects are certification, attestation and increased visibility of the various data management processes. One measure of success would be increased data consumption.

In the information age, good organizational trust depends on good digital trust, and good digital trust depends on enhanced trust not only in the enterprise's IT, but also in its data. From a data perspective, data trust is forged by paying attention to privacy and security, data quality and metadata, and by exhibiting the ability to certify data and information as being fit for purpose.

Endnotes

1. Kinder, T.; "KPMG Sued for $830mn Over 'Appalling' Chinese Audit," *Financial Times*, 5 September 2022, *https://www.ft.com/content/07af027a-a1ed-4847-bcfc-263ce9b48a03*
2. O'Dwyer, M.; "KPMG Hit With Half of UK Accounting Fines as Penalties Reach New Record," *Financial Times*, 28 July 2022, *https://www.ft.com/content/73e48574-673a-4725-9b78-ba940a8060f5*
3. US Securities and Exchange Commission, "Ernst & Young to Pay $100 Million Penalty for Employees Cheating on CPA Ethics Exams and Misleading Investigation," 28 June 2022, *https://www.sec.gov/news/press-release/2022-114*
4. Ellis, C.; "PwC Canada Fined Over One Million CDN by US, Canadian Regulators," *Canadian Accountant*, 1 March 2022, *www.canadian-accountant.com/content/profession/pwc-canada-fined-by-us-canadian-regulators*
5. Chartered Professional Accountants (CPA) Canada and American Institute of Certified Public Accountants (AICPA), *The Data-Driven Audit: How Automation and AI Are Changing the Audit and the Role of the Auditor*, Canada, 2020, *https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/the-data-driven-audit.pdf*
6. Wong, J.C.; "The Cambridge Analytica Scandal Changed the World—But It Didn't Change Facebook," *The Guardian*, 18 March 2019, *https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook*
7. Edelman, *Edelman Trust Barometer 2022*, USA, 2022, *https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20Global%20Report_Final.pdf*
8. Michels, D.; "The Trust Crisis in Business," Forbes, 17 June 2019, *https://www.forbes.com/sites/davidmichels/2019/06/17/the-trust-crisis-in-business/?sh=5418ceef44a6*
9. Vavreck, L.; "The Long Decline of Trust in Government, and Why That Can Be Patriotic," *The New York Times*, 3 July 2015, *https://www.nytimes.com/2015/07/04/upshot/the-long-decline-of-trust-in-government-and-why-that-can-be-patriotic.html*
10. Harrington, M.; "Survey: People's Trust Has Declined in Business, Media, Government, and NGOs," *Harvard Business Review*, 16 January 2017, *https://hbr.org/2017/01/survey-peoples-trust-has-declined-in-business-media-government-and-ngos*
11. ISACA®, *Digital Trust: A Modern-Day Imperative*, USA, 2022, *www.isaca.org/digital-trust-modern-day-imperative*
12. PricewaterhouseCoopers (PwC), "In Data We Trust: Living Up to the Credo of the 21st Century," *https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/defining-data-trust-strategy.html*
13. *Ibid.*
14. *Ibid.*
15. Bianchi, T.; "First-Party Data Key to Rebuilding Trust in Online Platforms," *AI Magazine*, 23 July 2022, *https://aimagazine.com/data-and-analytics/first-party-data-key-to-rebuilding-trust-in-online-platforms*
16. Morey, T.; T. Forbath; A. Schoop; "Customer Data: Designing for Transparency and Trust," *Harvard Business Review*, May 2015, *https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust*
17. Harrington, S.; "You Can't Build Trust Through Transparency," The People Space, 14 November 2018, *https://www.thepeoplespace.com/ideas/articles/you-cant-build-trust-through-transparency*
18. Lagarde, C.; "There's a Reason for the Lack of Trust in Government and Business: Corruption," *The Guardian*, 4 May 2018, *https://www.theguardian.com/commentisfree/2018/may/04/lack-trust-government-business-corruption-christine-lagarde-imf*
19. Kinch, N.; "Data Trust, by Design: Principles, Patterns and Best Practices (Part 1)," *Medium*, 22 February 2018, *https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-best-practices-part-1-defffaac014b*
20. Talend, "What Is Data Trust?" *https://www.talend.com/resources/what-is-data-trust/*
21. Mohrmann, R.; "Most Technology Projects Fail. What Is Your Data Management Plan?" Datafloq, 23 February 2018, *https://datafloq.com/read/technology-projects-fail-data-management-plan/*
22. Westenberger, J.; K. Schuler; D. Schlegel; "Failure of AI Projects: Understanding the Critical Factors," *Procedia Computer Science*, vol. 196, 2022, p. 69–76, *https://www.sciencedirect.com/science/article/pii/S1877050921022134/pdf?md5=2846ce14f794d777a06b39fdcb82781d&pid=1-s2.0-S1877050921022134-main.pdf*
23. Bean, R.; "The 'Failure' of Big Data," *Forbes*, 20 October 2020, *https://www.forbes.com/sites/randybean/2020/10/20/the-failure-of-big-data*
24. Choudhury, A.; "What Is Data Democratization? Definition and Principles," *Amplitude Blog*, 27 January 2022, *https://amplitude.com/*

blog/data-democratization#:~:text=Data%20democratization%20is%20the%20ongoing,customer%20experiences%20powered%20by%20data

[25] Zentao, "Reasons for Data Governance Project Failure," 13 July 2022, *https://www.zentao.pm/blog/reasons-for-data-governance-project-failure-1268.html*

[26] *Ibid*.

[27] Schmidbauer, S.; "Five Reasons Your Data Governance Initiative Could Fail," Stibo Systems, 24 January 2022, *https://www.stibosystems.com/blog/five-reasons-your-data-governance-initiative-could-fail*

[28] Bradshaw, A.; "Why Your Data Governance Strategy Is Failing," Alation, 5 October 2021, *https://www.alation.com/blog/data-governance-strategy-failing/*

[29] *Ibid*.

[30] Mathieson, S. A.; "UK Government Coronavirus Data Flawed and Misleading," *ComputerWeekly*, 6 October 2020, *https://www.computerweekly.com/feature/UK-government-coronavirus-data-flawed-and-misleading*

[31] *Ibid*.

[32] Redman, T. C.; "Bad Data Costs the U.S. $3 Trillion Per Year," *Harvard Business Review*, 22 September 2016, *https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year*

[33] Countryeconomy, "United States (USA) GDP—Gross Domestic Product," 2016, *https://countryeconomy.com/gdp/usa?year=2016*

[34] Worlddata, "Developing Countries," *https://www.worlddata.info/developing-countries.php*

[35] Grensquared, "Top 5 Data and Analytics Challenges and How to Conquer Them," 28 March 2022, *https://www.gensquared.com/5-challenges-business-and-it-leaders-face-when-launching-data-analytics-projects/*

[36] Pearce, G.; "Quantifying the Impact of Data Projects," The Data Administration Newsletter (TDAN), 5 July 2017, *https://tdan.com/quantifying-the-impact-of-data-projects/21760*

[37] RingLead, "The Cost of Dirty Data," *https://www.ringlead.com/blog/the-cost-of-dirty-data*

[38] Brooke, C.; "What Is Poor Data Quality Costing You?" Business 2 Community, 9 May 2016, *https://www.business2community.com/marketing/poor-data-quality-costing-01539520*

[39] *Ibid*.

[40] *Op cit* Edelman

[41] *Ibid*.

[42] *Ibid*.

[43] Bluemetrix, "Five Ways to Build Trust in Data, While Improving Access to Data," *https://www.bluemetrix.com/post/5-ways-to-build-trust-in-data-while-improving-access-to-data*

[44] Talend, "Five Principles for Increasing the Trustworthiness of Your Company's Data," *Harvard Business Review*, 30 July 2020, *https://hbr.org/sponsored/2020/07/5-principles-for-increasing-the-trustworthiness-of-your-companys-data*

[45] Barzelay, A.; M. Veerappan; M. Lucey; "Promoting Trust in Data Through Multistakeholder Data Governance," World Bank Blogs, 13 December 2021, *https://blogs.worldbank.org/opendata/promoting-trust-data-through-multistakeholder-data-governance*

[46] KPMG, "Building Trust in Analytics," Netherlands, 2016, *https://assets.kpmg/content/dam/kpmg/xx/pdf/2016/10/building-trust-in-analytics.pdf*

[47] *Ibid*.

[48] Pearce, G.; "Data Resilience Is the Cornerstone of Digital Resilience," ISACA Now, 27 July 2022, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/data-resilience-is-the-cornerstone-of-digital-resilience*

[49] Pearce, G.; "Real-World Data Resilience Demands an Integrated Approach to AI, Data Governance and the Cloud," *ISACA® Journal*, vol. 3, 2022, *https://www.isaca.org/archives*

[50] *Op cit* KPMG

[51] *Ibid*.

[52] *Ibid*.

[53] PricewaterhouseCoopers (PwC), "Data Trust," *https://www.pwc.com/ca/en/services/consulting/cybersecurity-privacy/data-trust.html*

[54] *Op cit* Bianchi

[55] *Ibid*.

[56] Nesta, "The New Ecosystem of Trust," *https://media.nesta.org.uk/documents/nesta.org.uk-The_new_ecosystem_of_trust_-_printable.pdf*

[57] *Ibid*.

[58] Hartman, T.; H. Kennedy; R. Steedman; R. Jones; "Public Perceptions of Good Data Management: Findings From a UK-Based Survey," *Big Data and Society*, January–June 2020, *https://journals.sagepub.com/doi/pdf/10.1177/2053951720935616*

[59] *Ibid*.

[60] *Ibid*.

How to Digitally Verify Human Identity

The Case of Voting

Disponibile anche in italiano
www.isaca.org/currentissue

How important is individual identity in human beings, really? There are several possible answers, ranging from irrelevant to fundamental, but it depends on the context. In prehistory, there was likely no personal identity at all—only a dichotomic group identity. Subjects belonged to a utilitarian group that could comprise friends or enemies, males or females, or strong or weak, and so on. However, today personal identity is indispensable to the coexistence of people in society. All individuals have their own registered histories and identities to help them foster relationships with others or access services.

Technological evolution and new social habits have exacerbated the need to identify a person with increasing precision. In many countries, a license is required to drive a car, a passport is required to visit another country, a social security number (or equivalent) is required for a medical examination and an identity card (or equivalent) is necessary to exercise the right to vote. On the other hand, this excess of information used for identification is contrasted with the need to respect the fundamental rights and freedoms of people's privacy and, in particular, their right to protect their personal data. The difficulty lies in determining the right balance between the effectiveness of identification and people's privacy rights.

Defining Human Identity

Human identity is the set of characteristics that make an individual in society unique (when referring to a single individual, not the human species as whole). In a social context, it is a method of identifying a person compared to others. In computer terms, it is an object that has a unique code, internally to a defined space, associated with various attributes and methods of treatment. Defining identity in an abstract way is easy. But in practice, there are several different ways to choose or treat individual characteristics to identify subjects, which is more difficult. Sometimes, in addition to the information strictly necessary for the recognition of identity, further classes of information are requested, such as the address, gender, age or a photo of the person. In addition, these data over time may need to be changed, perhaps because personal characteristics have changed, or because the service has been terminated or for any other need of the interested party.

LUIGI SBRIZ | CISM, CRISC, CDPSE, ISO/IEC 27001:2013 LA, ITIL V4, NIST CSF, UNI 11697:2017 DPO

Is a lead auditor and senior consultant on risk management, cybersecurity and privacy issues. He has been the risk monitoring manager at a multinational automotive company for more than seven years. Previously he was head of information and communication operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia) and was the worldwide information security officer for more than seven years. He developed an original methodology for internal risk monitoring, merging operational risk analysis with consequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and an integrated system involving risk monitoring, maturity model and internal audit. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn at *https://www.linkedin.com/in/luigisbriz* or at *http://sbriz.tel*.

The identification method used must satisfactorily identify (i.e., authentication) a subject to consequently recognize the person's right (i.e., authorization) to complete certain actions or prohibit them. Sometimes it is not necessary to correctly identify an individual who requires a service; it is sometimes sufficient to obtain an adequate guarantee of a legitimate use of the identification method assigned for access. That is, if the credentials presented are considered authentic or the device is recognized, then the operation is authorized. For example, if the cash withdrawal from an automated teller machine (ATM) is performed by someone other than the holder of the bank account, but the person is in possession of the correct account credentials, the operation is considered lawful because the identification is made based on the physical device and password. The account holder is aware of the consequences of a lost device or disclosed password and assumes accountability for the diligent custody.

The construction of a realistic identity to be used on the Internet cannot be limited itself to a mere technological solution; it must include an abstract representation of the personal behaviors and distinctive characteristics of the individual. Furthermore, the characteristics to consider may have evolved with technology and may require periodic adjustments if they change over time. The primary reason for ensuring that an identity is constantly up to date is to counteract its falsification or misuse. Such a threat may appear in the form of a deep fake, which alters the human form in a graphic representation of the real world, making it difficult to verify the authenticity of the presented identity.

There is no single solution for managing identity recognition on a network. The proposed method will distinguish between two types of identity registration based on different complexities and characteristics.

1. Registration of a complete, secure, certified identity, to be of reference for other identities. To guarantee these properties, the certification of an authority is required, and, therefore, it will not be possible to resort to an entirely online procedure. Physical recognition is necessary to give value to the registration itself and activate the consequent certified online identity.
2. An identity that is easily used for daily activities and its application must be stress-free, fast and secure. It is used exclusively online and certified by the first type of identity.

Before explaining the network identity management scheme, it is helpful to analyze the different identity registrations used in daily life to understand how many different situations and solutions have been adopted for the same purpose: to recognize the identity of a person.

LOOKING FOR MORE?

- Read *Identity and Access Management Audit Program.* *www.isaca.org/iam-audit-program*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Contexts in Which Identity Is Required

In everyday situations in which it is necessary to demonstrate one's own identity, identification is mainly managed with physical documents issued by government bodies or electronic credentials issued by organizations' systems that authenticate the validity of the credentials. Some of the most common examples are illustrated in **figure 1**.

There are countless other situations in which a user profile is created and authentication credentials are issued, although each circumstance may have different requirements for identification. It is also worth noting that not all requests for personal data are regulated on a need-to-know basis. The principle of need to know is a basic concept of information security, and it requires that only necessary information is processed; collecting unnecessary information can compromise privacy.

Registrations and Personal Profiles

One concern related to the high number of identity recordings that occur on a daily basis is the repeated provision of personal data to service providers. This can become habitual to the average user and lead the user to pay less attention to the circumstances surrounding data collection. Recording personal data at a higher frequency exposes data to risk, and it also often means that there is not a clear explanation of why the data need to be provided and how they are being used. In addition, in the case of termination of a service that required personal data, data are not always promptly deleted according to the planned (contractual and legal) terms, exposing them to risk of unauthorized or illegal use (e.g., identity theft).

The countermeasure to the problem of the number of registrations and the amount of personal data entered is the use of a trustee who has custody of the personal data and has the right to operate in a controlled ecosystem made of technologies, protocols and operators of proven trust.[1, 2] The only guarantee of the real and complete identity of a person is the government entity that manages the legal identity and provides physical identity cards. This does not mean that there must be a single physical database containing all classes of personal data, such as personal, health, judicial, school and employment, only there is a single access control system for government databases.

In practice, it is like having access to a virtual database of legal data, managed by a trusted state custodian (i.e., government agency) that has the authority to regulate the registration operations of

FIGURE 1

Types of Identity in Daily Life

Document or Process	Identity	Characteristics
Passport	Digital but static (renewed after a number of years)	It can be reduced to an object composed of two parts: the information related to the subject's public identity and that which can be accessed by another country. Public data are partially visible (e.g., personal information, photo), while the biometric data of the person and integrity of the physical document are accessible via digital signature.[a]
Identity card	Digital but static (renewed after a number of years)	It is a reference document depicting a person's identity, but it is made for manual use, and although it has data in a digital format (e.g., magnetic strip, reading chip, holographic), it is not structured to be used with current technologies and the evolution thereof.
Driving license	Digital but static (renewed after a number of years)	It is formed by two types of information, one of identity and the other of specific driving qualification data. The latter data are the objective of the document but only in combination with the correct identity.
Social security number (SSN)	Static, electronically readable	It is a unique code associated with an individual for tracking activities conducted by public administration or government entities. It has no identity authentication goals; it only points to a person's data. It is sometimes required on websites to reduce user duplication.
Bank credentials	Digital, dynamic, strong authentication	Now more prevalent for digital banks, these vary in relation to the evolution of security technologies but do not directly authenticate the person. Rather, they are self-referencing; they verify that the credentials themselves are really those assigned. Separately, each bank or payment circuit retains the identifying data of the person and the risk profile.
Fidelity card	Static, electronically readable	Although nominal, it does not aim to recognize a person, but rather to direct the viewer to the buyer's purchasing data. The need is to identify the purchase profile that could also be associated with a group of people, such as a family.
Smartphone	Subscriber identity module (SIM) card and device ID	The SIM card is an integrated circuit that stores the phone number (i.e., international mobile identity), even before that of the person. There is no guarantee of the identity of the user, but the authentication of the device is guaranteed by valid international regulation, similarly to the eSIM,[b] a programmable SIM card that is embedded directly into the device.
Voting procedure	Physical recognition	Generally, authentication by an identity document is required before a person may access the voting booth. This is the most secure process, but requires voters to physically access the polling station.
	Postal voting	The postal vote is based on the principle of the double envelope, an external one for the sender identification, and an internal anonymous envelope to preserve the confidentiality of the vote. The check is on the consistency of shipping data and the integrity of the envelopes used. The counting process is slow and does not provide sufficient guarantees on the free expression of the vote.
	Remote electronic voting	Remote electronic voting (via the Internet) uses the same concept as postal voting. The physical envelopes are replaced by encapsulated digital messages. The external one is digitally signed by the voter and the internal one is anonymous. It is an effective technological response to the slowness of the physical counting of votes, however, the free expression of the vote is not verified and there is the risk of computer fraud.[c, d]

Sources: a) International Civil Aviation Organization (ICAO), "Public Key Directory: Secure Cryptographic Authentication of Chip-Based Traveler Information," *https://www.icao.int/Security/FAL/PKD/Pages/default.aspx*; b) GSMA, "eSIM," *https://www.gsma.com/esim/*; c) American Association for the Advancement of Science (AAAS), "Internet or Online Voting Remains Insecure," USA, 10 March 2021, *https://www.aaas.org/epi-center/internet-online-voting*; d) e-Estonia, "i-Voting—The Future of Elections?" 6 March 2019, *https://e-estonia.com/i-voting-the-future-of-elections/*

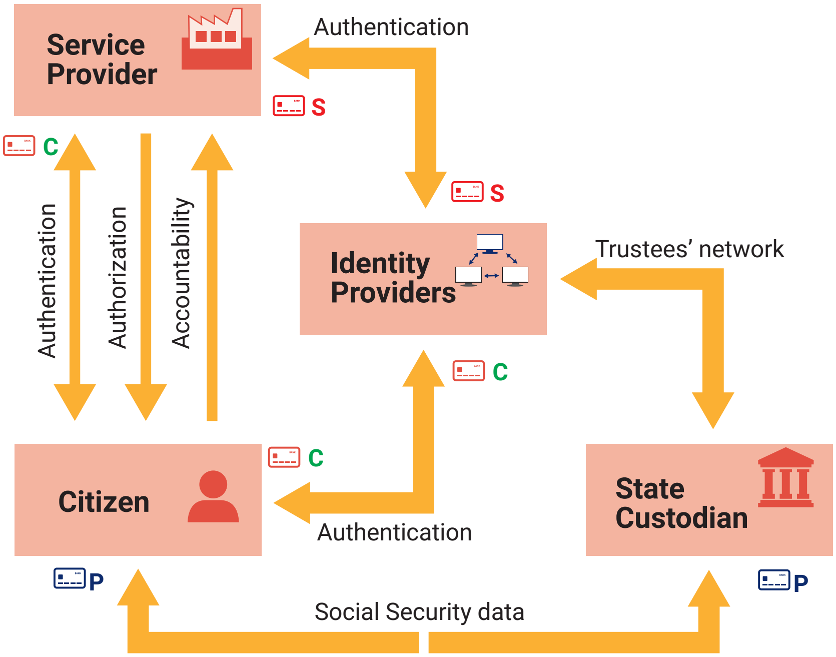
the legal digital identity of citizens to release the personal digital certificate (**figure 2**) and guarantee confirmation of legal identity to the subjects who require it for a legitimate reason.

Schema of an I-Identity Solution

Technically, to securely recognize a user on the Internet with a mechanism that guarantees reliability and practicality, it is necessary to resort to federated digital identity systems. They must be built on open authentication standards, for example OpenID Connect 1.0 (OIDC),[3] which adopts the OAuth 2.0 authorization protocol based on the exchange of tokens,[4] but there must be the possibility of adding appropriate extensions, such as the categorization of identity providers. Suppose a person (i.e., citizen) needs to create a user profile to access a new service (i.e., service provider). As an alternative to the classic

FIGURE 2

Scheme of Identity Recognition on the Internet



submission of personal data with a copy of an identity card repeated on each website accessed, it is more efficient to have an online mechanism entirely based on digital certificates issued by a certification authority (i.e., identity provider) that guarantees the integrity of the information received by a public authority (i.e., a state custodian). Each person would need a personal digital certificate (P) to manage relations with the public administration and one or more common digital certificates (C) for daily activities. The digital certificate is a mix of information about the person, the device and the trusted organization that issues it and signs it by encryption.

The personal certificate (P) is issued by a public authority (i.e., state custodian) following physical recognition by a local authority relevant to the residence of the citizen. The state custodian can be thought of as a tree structure: The top are the data and the roots are the government agencies that provide the private certificates, including the authorization of access to personal data categories based on the applicant's authorization profile. For example, for roadside control, all of a driver's personal data relating to demonstrating the ability to drive a vehicle should be available to law enforcement. In general, all the data necessary for public social and civil services would be available to the respective public control bodies. A centralized blockchain records all the identification queries for any forensic analyses, while analysis tools of network traffic verify the certificate by combining applicant, authorization class, device, type of data and data classification information to create alarms and report excesses or data processing abuses.

The common certificate (C) is then issued by its public identity trustee (i.e., identity provider) following online recognition by the public authority (i.e., state custodian). The state custodian, as guarantor of the highest-level identity, interacts with public identity providers on a special overlay network. They return a class of personal data following the authentication of the private certificate. This allows the identity provider to create the username and certificate to use in public and send it to the applicant. It is likely that this operation would require a payment.

With the public username and the common certificate, a person can create a profile with the service provider. In the registration form, the username and, as an alternative to the password, the common certificate can be used with a selection of personal data communicated automatically (e.g., name, address, birthdate, gender). The data available are restricted to those owned by the identity provider that do not exceed those present in the physical identity card. To send more data, it is necessary to define a broader mechanism, which would be regulated by an international standard created for the circumstance and involve a state custodian.

The service provider automatically sends the applicant's certificate (C) to its identity provider in addition to its own certificate (S). This validates the identity of both the applicant and the service provider. Therefore, the applicant is automatically informed of the registration of activities to demonstrate the legitimacy of the actions carried out. At this point, the service provider system grants privileges and permissions to access the data.

This identification scheme is secure because it is based on the recognition of the device (included in the certificate), the network address of the applicant (included in the authentication package), the ability to contact the certificate issuer (for integrity verification) and the robustness of cryptographic keys (encryption of the communication channel and data). The strength of the mechanism is linked to the possibility of making immediate controls for these factors with a choice of technology adequate to each of them. It is a form of defense in depth (DiD), with verification of the origin of the request (device, address), the identity of the issuer (certificate), the correctness of the recipient (consent) and the integrity of the messages (encryption). The effort is focused on the contrast of false identities.

This identification scheme can be generalized by removing the constraint of the identity provider for applicant and service provider. Both can authenticate themselves on their own identity providers and almost nothing will change except for an exchange of certificates between the two identity providers to ascertain the validity of the certificate issued by the other provider.

Schema of an I-Voting Solution

Another possible application relating to the certification of a person's identity is online secure voting. In general, electronic voting (evoting) presents various methods aimed at simplifying the expression of the vote and the rapid counting of votes through electronic and/or computer technologies. Among these are the methods that are implemented through the Internet (I-voting), with the aim of proposing a process that combines the most widespread communications medium in the world, the Internet, with the basic requirements of a public vote. The four primary requirements to vote are the right to vote, freedom of expression of the vote, the certain identity of the voter and the secrecy of the vote. The right to vote requires that there are no impediments to the vote itself. The difficulty in accessing the site and where the electoral booth is installed can make a difference in participating in the vote. Developing an application to vote via the Internet (I-voting) based on digital identity certified by a network of identity trustees requires more than just a technical effort; it must be combined with remote control procedures managed by operators.

The main components are all available, they just need to be put together. There are protocols to manage authentication and there are also artificial intelligence (AI) programs to recognize a person via webcam; however, the requirement linked to the freedom of expression of the vote still requires human judgment. The software should be open source, and remote human control should guarantee aspects related to the freedom of the vote. A voting application available to download to a smartphone could have several features (**figure 3**) to safeguard the criteria required for a safe and effective voting process.

The proposed mechanism at the device level could work as follows. The voter, through the smartphone application and using an encrypted connection, is authenticated with the personal digital certificate issued by the state custodian. The facial recognition software, drawing on the custodian's personal data, evaluates the physical identity and acts as the first filter to allow access to the virtual electoral office. This is a call center of selected people with the same criteria as a physical electoral station. Each operator can interact with more voters simultaneously and has at least one supervisor who monitors their activities. A brief set of text instructions informs the voter of the need to enable the operator to take control of the device—in particular, the room and microphone, but without being able to see the contents of the virtual voting card. If the voter agrees, control of the voter's environment, including the camera and microphone, is enforced and the vote begins.

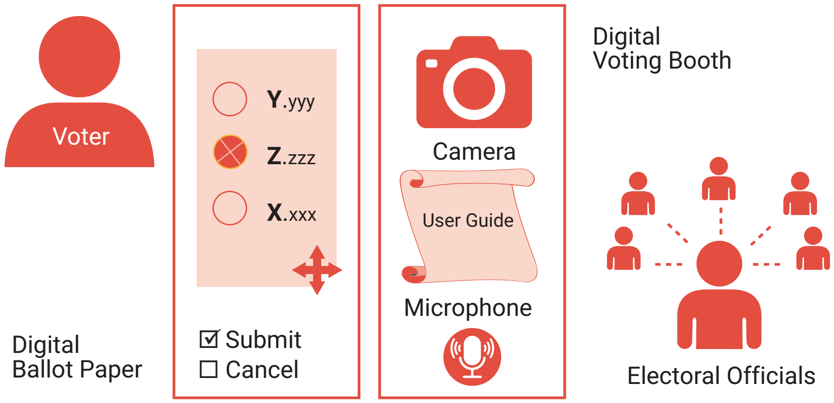
This proposed solution has many similarities to physical voting. The voter is recognized before accessing the vote, and the virtual electoral office, through the control obtained by operating the device, guarantees that the voter is free to act without the influence of others. The remote operator is always prevented from viewing the operations on the voter's screen, guaranteeing confidentiality. As a further guarantee, it would be appropriate to allow the voter to change the presentation layouts of candidates to prevent an external observer from inferring the selections of the voter by observing the voter's hand movements. The operator can block the voting operation in the event of an infringement of the electoral rules. After completing the selections and confirming the vote, the smartphone is unlocked and the voter can use it again with full freedom.

Options for the Electoral Station

Even if a smartphone application were created, an in-person voting option would still be necessary for anyone facing obstacles such as cost, lack of familiarity with the use of smartphones, or distrust in the application solution, or simply because a backup solution is necessary. To set up an electronic voting booth, desktops, laptops or tablets can be used with a version of the software that, if present,

FIGURE 3

Voting Scheme via Smartphone Application



> The proposed mechanism of digital identification aims for a balance between the complexity of the necessary technological components, the process of managing identity providers and ease of use for the user.

disables the camera, microphone and keyboard, but enables the mouse (or touchscreen). Deactivation works because the control is implemented by the electoral officials, while the software module of the voting event remains unchanged. To be able to use any computer without changing its configuration, the software must be installed on a removable and bootable device, managed by authorities only to avoid tampering with a voting booth identifier certificate. The voting operation is activated by the electoral officials sending an enabling message to the voting booth (e.g., via wireless Bluetooth) composed of the identification code of the voting booth, the SSN of the voter and the certificate of the electoral official. When establishing the polling station, the devices used by the electoral personnel and the necessary digital certificates are distributed.

To facilitate anyone unable to access the polling station, a mobile voting booth can be created using a tablet or a laptop in accordance with the procedure for setting up a polling station. The dedicated electoral staff should reach and recognize the voter, enable the voting device, deliver it to the voter (or their legal trustee) and ensure the confidentiality of the vote. At the polling station, it is also useful to prepare a simulation booth of the voting operations to aid situations in which there is a lack of digital culture.

Conclusion

To effectively manage the identity of a person on the Internet, a solution must be easy to use, and it must be secure to avoid counterfeits. It cannot always be entrusted exclusively to technology because sometimes human input is required, as in the example case of I-voting. At the same time, the solution must guarantee a legitimate level of anonymity to avoid excessive use of personal data, to limit the impact of identity theft, and to be compliant with privacy regulations. For physical documents, the origin of personal information is under the protection of government agencies so that there is a referee who can enforce regulation in the event of disputes and, similarly, protect the party that provides services.

The proposed mechanism of digital identification aims for a balance between the complexity of the necessary technological components, the process of managing identity providers and ease of use for the user. The use of a government agency as a custodian of the original data related to the identity of a person is nothing new. Such a practice should not be considered a loss of individual freedoms, because it is analogous to what already exists and is the basis of the organization of social life. Technology is simply an excellent means to make this process of using a digital identity more efficient. The use of digital documents is a sustainable solution in terms of resources and practicality and is suitable for use on the Internet. For daily network activities that do not require the certainty of identity, it is possible to use simplified identities (managed by identity providers) in addition to the legal personal identity (managed by the custodian). The management of this process does not require a complex system. It only requires a network of identity trustees capable of providing flexibility to accommodate the peaks of demand, ensuring the resilience of the service and guaranteeing security.

This ecosystem of technological infrastructures, protocols and operators, guaranteeing the reliable and practical recognition of a person, allows for better security on the network, lower costs and fewer disputes. In general, the reliability and security of a digital identity system can also be a boost to create new egovernment services to include citizens in a more eco-sustainable and efficient technological environment.

Endnotes

1 Sbriz, L.; "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 1," *ISACA® Journal,* vol. 2, 2022, *https://www.isaca.org/archives*

2 Sbriz, L.; "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 2," *ISACA Journal,* vol. 2, 2022, *https://www.isaca.org/archives*

3 OpenID, Specifications, *https://openid.net/developers/specs/*

4 OAuth, OAuth 2.0, *https://oauth.net/2/*

Extending Zero Trust to the End-User Ecosystem

Trust is at the heart of every relationship between an organization and its end users. Customers choose the organizations with which they do business based on their perception of an organization's trustworthiness. Regardless of whether business is conducted in person or digitally, trust is often measured by an organization's performance, history and reputation.

There are significant gaps in current approaches to achieving digital trust. To address these gaps, organizations need to ensure that security parameters align with a digital trust framework such as ISACA's Digital Trust Ecosystem Framework.[1]

What Is Digital Trust?

In the digital world, trust has become complex. Digital trust is defined as:

> *Digital trust is the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, processes, information and technology to create and maintain a trustworthy digital world.*[2]

ISACA® notes that "The objective of establishing digital trust for an organization is to positively impact its relationship with its clients."[3] When measures that enhance digital trust are implemented, they help create a safe environment that protects the organization's digital assets and the users' data of the organization's digital ecosystem.

As opposed to taking place in writing, for example, digital online interactions occurs via emails, text messages and websites. Multiple industry studies conclude that whether it is via phishing, smishing, site impersonation or spoofing, the end user is the number one vulnerability and the initial attack surface for the majority of online fraud, malware insertion and ransomware attacks.[4, 5, 6] When an attack occurs, it decimates the attacked customers' trust, and the impact is amplified and spread to many other customers who hear about such attacks and fear they will be next.

Existing Approaches: How They Fall Short

With digital trust being a relatively new concept, existing enterprise-centric approaches are insufficient. Once trust has been established, it can easily be eroded by phishing and other impersonation attacks. While the concept of zero trust—never trust, always verify—is core to modern information security practices and technologies, it does not fully cover the multiple types of communications and transactions between customers and organizations that digital trust encompasses.

Specifically, end users have few effective ways of verifying whether they can trust the digital entity with which they are engaging, while organizations can verify customer identities by using passwords and multifactor authentication (MFA). Knowing this gap exists, organizations attempt to educate users on impersonation risk, sharing strategies for identifying phishing attacks. However, education is far from effective and might even result in the opposite of the desired outcome, as one study shows:

> *Students who identified themselves as understanding the definition of phishing had a higher susceptibility rate than did their peers who were merely aware of phishing attacks, with both groups having a higher susceptibility rate than those with no knowledge whatsoever. Approximately 70% of survey respondents who opened a phishing email clicked on it, with 60% of students having clicked overall.*[7]

Customers are already educated about the threats facing their online transactions but few implement the

GIDEON HAZAM

Is cofounder and chief operating officer (COO) of MEMCYCO. He has more than 30 years of experience in the cybersecurity and global high-tech industries. He has held senior positions in business and enterprise development, customer success, and global sales, mostly in emerging technology and solutions for Fortune 500 companies.

complex steps needed to stay safe online. They look to organizations to take proactive steps to protect their digital assets. Further, online fraud awareness can backfire on an organization as it can create phishing fear syndrome. This phenomenon occurs when consumers are fearful that their personal and financial information will be compromised, so they choose not to engage with digital communications and ecommerce.[8] This can negatively impact the effectiveness of digital advertising campaigns and online revenue.

When communicating with their users, many organizations embrace the zero-trust model for end-user access, often implementing MFA. Many have the false impression that when doing so they are also protecting themselves from impersonation because MFA does not work with an impersonation site. However, sophisticated cyberattackers have learned to bypass MFA with methods such as two-factor relay and short-lived domains, which are fake domains that stay live for no more than several hours.

Antiphishing software, also widely used, relies on blacklists that are not updated in real time, but rather when a new phishing source is discovered. These blacklists are not able to keep pace with ever emerging, evolving threats.

Smishing attacks leveraging text message communications are increasingly used to direct unsuspecting end users to fraudulent sites and log-in screens.

To combat these attacks, suspicious site identification and takedown also is commonly employed by threat intelligence enterprises. The issues with this method are time lag and completeness. This method cannot identify all fake sites as it relies mostly on finding similarly named domains, while attackers often use nondescript uniform resource locators (URLs). An attack can occur in the time between the organization requesting takedown of the fake site and it being taken down.

The Effect of Ineffective Approaches

Regardless of the method used, attacks succeed by misdirecting users to counterfeit, fraudulent websites where their personal and financial information and login credentials are stolen. This information is later used to steal money, execute fraud, steal identities and perpetrate many other types of scams. This results in harm to the consumers who were attacked and the organization with which they interacted. Organizations are often forced to spend time investigating reported attacks, verifying damages to customers, and reimbursing defrauded customers in increasing amounts and frequencies, either directly or indirectly via discounts.

Moreover, it has become popular for legislators to enact regulations that put the responsibility on the organizations to take proactive actions to protect their customers.[9] Cyberattacks erode the digital trust of the defrauded customers and those who hear about these attacks—including legislators—negatively impacting the essential trust relationship with the brand.

> Customers are already educated about the threats facing their online transactions but few implement the complex steps needed to stay safe online.

Existing security approaches have proven inadequate because by the time threats are discovered and mitigating actions are taken, the damage typically has already occurred. Customers who fall victim to phishing traps often blame the impersonated organization, which can be detrimental to maintaining digital trust. One study found that an average of 44 percent of customers have stopped transacting with an organization due to a lack of trust resulting from cyberattacks.[10]

Achieving Digital Trust

To achieve digital trust, any approach to security should include real-time capabilities, full visibility for the organization and its end users, and proactive damage prevention. Because threats continue to evolve in sophistication, solutions need to be equally sophisticated and adaptive, incorporating artificial intelligence (AI) when possible.

When an organization is attacked, it should ideally have a layer of security that warns its customers and prevents them from entering sites that are impersonating the brand. Assuming that not every attack can be stopped in real time, which depends on the specific techniques used by attackers, the organization's security team needs to quickly assess the nature of the attack, the target of the attack and the scope of the damage. This information enables the security team to implement a timely response to stop the attack before it can do further damage and to alert impacted end users of the threat.

To foster confidence in the legitimacy of an organization's online presence, there should be a method for the organization to provide clear proof to end users that the site they are visiting is indeed a brand-authentic digital presence. Such proof should be unforgeable, clearly visible and intuitive. It should allow end users to immediately differentiate fake sites from authentic ones. This extends the enterprise's zero trust concept model, which significantly enhances digital trust by showing customers that the organization is taking a proactive and personalized approach to securing the enterprise ecosystem.

Currently, the only ways for end users to know whether a website is legitimate are by inspecting the lock icon next to the browser's address bar and by visually comparing the displayed URL with the known legitimate URL of the organization. These methods are impractical and ineffective as they place the authentication burden on the end user.

To be effective, any security approach should be:

- Easily accessible and understandable to customers without requiring them to significantly change their behavior or invest time in education
- Affordable for organizations of any size
- Automatic and transparent to end users
- Easy to implement and manage
- Independent of but compatible with existing solutions, including security information and event management (SIEM) systems
- Include real-time identification and alerts
- Able to identify and stop existing, new and emerging threats (-1, 0, +1 day)
- Able to provide the end user with visual confirmation of website authentication

Solutions that meet these criteria would contribute significantly to achieving digital trust since end users could be confident that they are accessing a legitimate digital presence of the organization with which they intend to interact.

> There should be a method for the organization to provide clear proof to end users that the site they are visiting is indeed a brand-authentic digital presence.

Practical Approaches to Achieving Digital Trust

Most impostor attacks direct end users to counterfeit websites and login and password reset pages. Effective approaches to limit this exposure include:

- Scanners and crawlers that constantly scan the web can be used to detect imposter sites. While these can be effective, they are not 100 percent accurate and can return false positives. When an impostor site is found, there is a takedown process. The impersonated organization needs to file a takedown request with the domain registrar and provide proof that the site is a phishing site. The domain registrar then informs the hosting organization that the site is indeed a fake. A response typically takes two to three weeks.
- Organizations and individuals buy website domains from providers. Domain Name System (DNS) providers use application programming interfaces, (APIs) to determine which domains are similar to authentic domains and may be attempting to impersonate them. This is a semimanual process. As soon as a pattern is detected, a manual takedown process is initiated.
- Instead of looking for DNS vulnerabilities or scanning for impostor sites, the Proof of Source Authenticity (PoSA)[11] approach is end user-centric. Since imposter attacks are continuously evolving and primarily target end users, this approach provides real-time automatic assurance of authenticity to all end users. This approach is agentless and implemented by the organization by installation on its website. It identifies when the site is being copied and launched from a domain that is not an authentic domain; presents users with a red alert on fake sites to warn users against accessing it; notifies the security team of the attack; and presents a digital watermark on the authentic site that proves to users that it is indeed the destination they desired to reach. With this approach, end

LOOKING FOR MORE?

- Read *Beating the Adversary at Their Own Game With Zero Trust.* *www.isaca.org/zero-trust*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

users can be sure they are always interacting with the authentic source and not a criminal impostor. Further, this approach provides real-time alerts to the organization as to the source, the nature of the attack, and which users have been targeted.

Conclusion

The digitization of the world has forced a fundamental shift in how organizations, their customers and other third-parties interact to ensure the essential trust relationship. When digital trust is not prioritized, an organization's brand and business health can be severely impacted. Without digital trust implementation, a single well-publicized attack could not only diminish the return on the organization's security investments but also damage its reputation, thus critically endangering customer relationships. Therefore, new methods are needed to address the complexity of the threats targeting digital interactions.

Organizations that hope to be at the forefront of the digital trust transformation should extend their enterprise zero trust models to include all members of their end-user ecosystem by implementing solutions that can provide real-time detection, protection and visibility.

Endnotes

[1] ISACA®, *Digital Trust: A Modern-Day Imperative*, USA, 2022, *https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/digital-trust-a-modern-day-imperative_whpdt_whp_eng_0322.pdf*

[2] *Ibid*.

[3] *Ibid*.

[4] Singleton, C. *et al*.; *X-Force Threat Intelligence Index 2022*, IBM Security, February 2022, https://*www.ibm.com/downloads/cas/ADLMYLAZ*

[5] *Help Net Security*, "Phishing Reaches All-Time High in Early 2022," 13 June 2022, *https://www.helpnetsecurity.com/2022/06/15/2022-total-phishing-attacks/*

[6] AARP, "Half of U.S. Adults Have Been Targeted by Impostor Scams, Says AARP Survey," 19 February 2020, *press.aarp.org/2020-2-19-AARP-Survey-Shows-Half-of-US-Adults-Targeted-by-Impostor-Scams*

[7] Diaz, A.; A. T. Sherman; A. Joshi; "Phishing in an Academic Community: A Study of User Susceptibility and Behavior," *Cryptologia*, vol. 44, iss. 1, August 2019, *https://www.researchgate.net/publication/335162516_Phishing_in_an_academic_community_A_study_of_user_susceptibility_and_behavior*

[8] Hazam, G. *et al.; How to Protect Your Brand and Customers Against Impostors Using Proof of Source Authenticity (PoSA)*, MEMCYCO, Israel, 2022, *https://www.memcyco.com/home/wp-content/uploads/2022/10/Memcyco_White_Paper.pdf*

[9] United Kingdom Parliament, Online Safety Bill, United Kingdom, 2 November 2022, *https://bills.parliament.uk/bills/3137*

[10] PricewaterhouseCoopers (PwC), "The Complexity of Trust: PwC's Trust in US Business Survey," United Kingdom, 2021, *www.pwc.com/us/en/library/trust-in-business-survey.html*

[11] *Op cit* Hazam *et al.*

Looking Inside the Magical Black Box

A Systems Theory Guide to Managing AI

Artificial intelligence (AI) algorithms show tremendous potential in guiding decisions; therefore, many enterprises have implemented AI techniques. AI investments reached approximately US$68 billion in 2020.[1] The problem is that there are many unknowns, and 65 percent of enterprises cannot explain how their AI tools work.[2] Decision makers may be overly trusting the unknown components inside what is referred to as the AI magical black box and, therefore, may unintentionally expose their enterprises to ethical, social and legal threats.

Despite what many believe about this new technology being objective and neutral, AI-based algorithms often merely repeat past practices and patterns. AI can simply "automate the status quo."[3] In fact, AI-based systems sometimes make problematic, discriminatory or biased decisions[4] because they often replicate the problematic, discriminatory or biased processes that were in place before AI was introduced. With the widespread use of AI, this technology affects most of humanity; therefore, it may be time to take a systemwide view to ensure that this technology can be used to make ethical, unbiased decisions.

Systems Theory

Many disciplines have encouraged a systems theory approach to studying phenomena.[5] This approach states that inputs are introduced into a system and processes convert these inputs into outputs (**figure 1**).

An algorithm is defined as "a standard procedure that involves a number of steps, which, if followed correctly, can be relied upon to lead to the solution of a particular kind of problem."[6] AI algorithms use a defined model to transform inputs into outputs. British statistician George E. P. Box is credited with saying "All models are wrong, but some are useful."[7] The point is that the world is complex, and it is impossible to build a model that considers all possible variables leading to desirable outcomes. However, a model can help decision makers by providing general guidance on what may happen in the future based on what has happened in the past.

AI algorithms either use predefined models or create their own models to make predictions. This is the basis for categorizing AI algorithms as either symbolic or statistical.[8] Symbolic algorithms use a set of rules to transform data into a predicted outcome. The rules define the model, and the user can easily understand the system by reviewing the model. From a systems theory perspective, the inputs and processes are clearly defined. For example, symbolic algorithms are used to develop credit scores, where inputs are defined *a priori* and processes (calculations) are performed using

FIGURE 1

Systems Theory View of AI

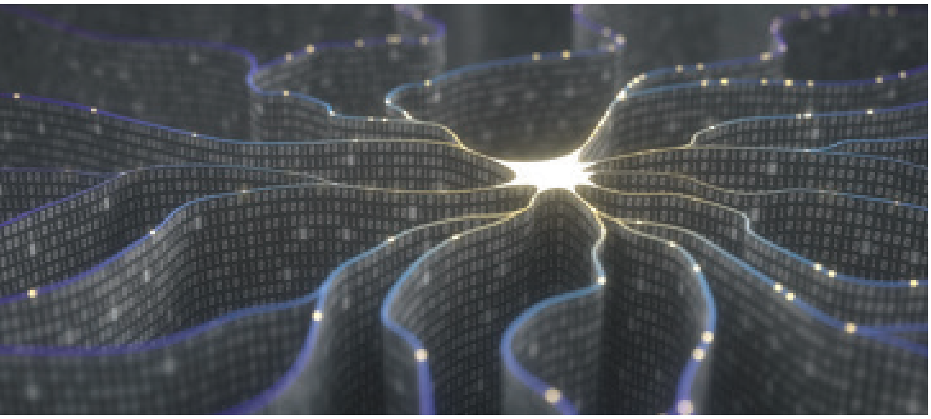
Inputs
Processes
Outputs

SIMONA AICH

Is an undergraduate student at Ludwigshafen University of Business and Society (Ludwigshafen, Germany) in a cooperative study program with SAP SE, a market leader for enterprise resource planning (ERP) software. She has completed internships in various departments, including consulting and development. Her research interests include the impact of algorithms, a topic she plans to pursue in her master's degree studies.

GERALD F. BURCH | PH.D.

Is an assistant professor at the University of West Florida (Pensacola, Florida, USA). He teaches courses in information systems and business analytics at both the graduate and undergraduate levels. His research has been published in the *ISACA® Journal*. He can be reached at gburch@uwf.edu.



associated weights and formulas to arrive at an output. This output is then used to decide whether to extend credit.

Statistical algorithms, in contrast, often allow the computer to select the most important inputs to develop a new model (process). These models are usually more sophisticated than those developed by symbolic algorithms but still predict outcomes based on inputs. One issue associated with the use of statistical algorithms is that the user may not know which inputs have been chosen or which processes have been used to convert inputs into outputs, and, therefore, may be unable to understand the model they are utilizing to make decisions.

A model can help decision makers by providing general guidance on what may happen in the future based on what has happened in the past.

Systems theory shows that the output of these models depends heavily on the inputs (data) provided and the types of algorithms (processes) chosen. Subsequent use of the AI model's outputs to make decisions can easily lead to bias, resulting in systematic and unknowing discrimination against individuals or groups.[9]

Computer System Bias

The systems theory discussion of AI algorithms can be extended by considering how biases affect outcomes. Bias has been defined as choosing one generalization over another, other than strict consistency with the observed training instances.[10] This is often seen where one outcome is more likely to be from one set of functions than from another. Bias is often seen either in the collection of data, where a non-representative sample is taken, which affects the outcome, or by the algorithms themselves, which lean toward one outcome. Decisions based on an AI algorithm's outputs are often of great interest to the general public because they can have a major impact on people's lives, such as whether they are selected for a job interview or whether they are approved for a home loan. In IT, three categories of bias can be distinguished: preexisting, technical and emergent.

Preexisting Bias

Sometimes, a bias established in society (preexisting) is transferred into software. This can happen either explicitly, such as when a discriminatory attitude is deliberately built into the algorithm, or implicitly, such as when a profiling algorithm is trained with the help of historical data based on bias. Preexisting bias is often introduced at the input stage of the system. One example of a preexisting bias is use of the classic Fair Isaac Corporation (FICO) algorithm to calculate a creditworthiness score. In this case, cultural biases associated with the definition of traditional credit can result in discrimination because some cultures place more emphasis on positive payment.[11]

Technical Bias

Technical bias is often the result of computer limitations associated with hardware, software or peripherals. Technical specifications can affect a system's processes, leading to certain groups of people being treated differently from others. This may occur when standards do not allow certain characteristics to be recorded, or it can be the result of technical limitations related to the software or programming of algorithms. These defects in the algorithm are often seen in the processing stage of the system. An example of technical bias is the inability to reproduce an answer using an AI algorithm. This might occur when the data being used to train (or develop) the model are altered slightly, resulting in a different model being produced. Being unable to reproduce a model with the same or similar data leads to doubt about the model's overall validity. An example of this type of bias occurred at Amazon, when women's résumés were excluded based on the

LOOKING FOR MORE?

- Read *Audit Practitioner's Guide to Machine Learning, Part 1: Technology.* *www.isaca.org/audit-practitioner-guide-to-ML-part-1*
- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

system's selection of words in applicants' résumés. Amazon tried to remove the bias but eventually had to abandon the AI algorithm because it could not identify the underlying technical logic that resulted in discriminatory outputs.[12]

Emergent Bias

Emergent bias happens due to the incorrect interpretation of an output or when software is used for unintended purposes. This type of bias can arise over time, such as when values or processes change, but the technology does not adapt[13] or when decision makers apply decision criteria based on the incorrect output of the algorithm. Emergent bias normally occurs when the output is being converted into a decision.

An example of emergent bias is the use of Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), which is used by some US court systems to determine the likelihood of a defendant's recidivism. The algorithms are trained primarily with historical data on crime statistics, which are based on statistical correlations rather than causal relationships. As a result, bias related to ethnicity and financial means often results in minorities receiving a bad prognosis from the model.[14] A study of more than 7,000 people arrested in the US State of Florida evaluated the accuracy of COMPAS in predicting recidivism. It found that 44.9 percent of the African Americans defendants labeled high risk did not reoffend. Making decisions using this model's outcomes would, therefore, negatively affect nearly 45 percent of African American defendants for no valid reason. Conversely, only 23.5 percent of white defendants labeled as high risk in the study did not reoffend.[15] Knowingly using biased outcomes to make decisions introduces emergent bias that may lead to negative outcomes.

These forms of bias can occur in different combinations,[16] and they point to the mystery hidden inside the AI black box (**figure 2**). The AI system can result in outcomes that are unethical or discriminatory. Therefore, it is critical that decision makers understand what happens inside the box—at each step, and with each type of bias—before using AI outputs to make decisions.

Conducting correlation studies of the variables before introducing them into the system may provide an early indication of potential discrimination problems.

Analyzing the AI Black Box and Removing Bias

After understanding how bias can find its way into the AI black box, the goal of managers is to identify and remove the biases. As shown in **figure 3**, there are five steps to avoid bias and discrimination.

Step 1: Inputs

The goal of AI algorithms is to develop outputs (predictions) based on inputs. Therefore, it is possible that AI algorithms will detect relationships that could be discriminatory based on any given input variable. Including inputs such as race, ethnicity, gender and age authorizes the system to make recommendations based on these inputs, which is, by definition, discrimination. And making decisions based on these factors is also discrimination. This is not an admonishment to never use these inputs; rather, it is a warning that discrimination could be claimed. For example, automobile insurance models predict accident rates based on age and gender. Most people would probably agree that this is fair, so including age and gender would be appropriate inputs

FIGURE 2
AI Black Box

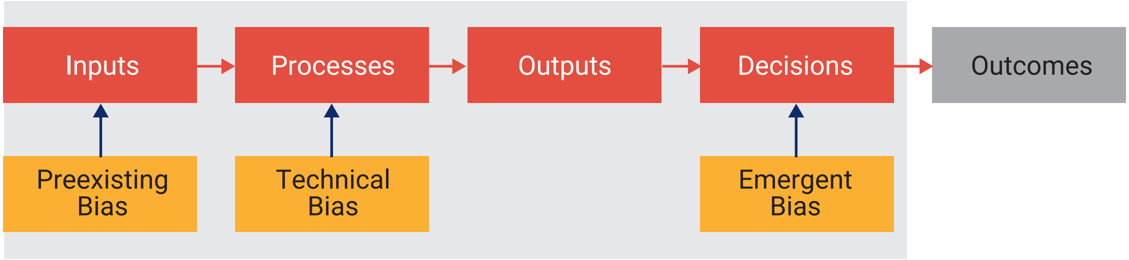
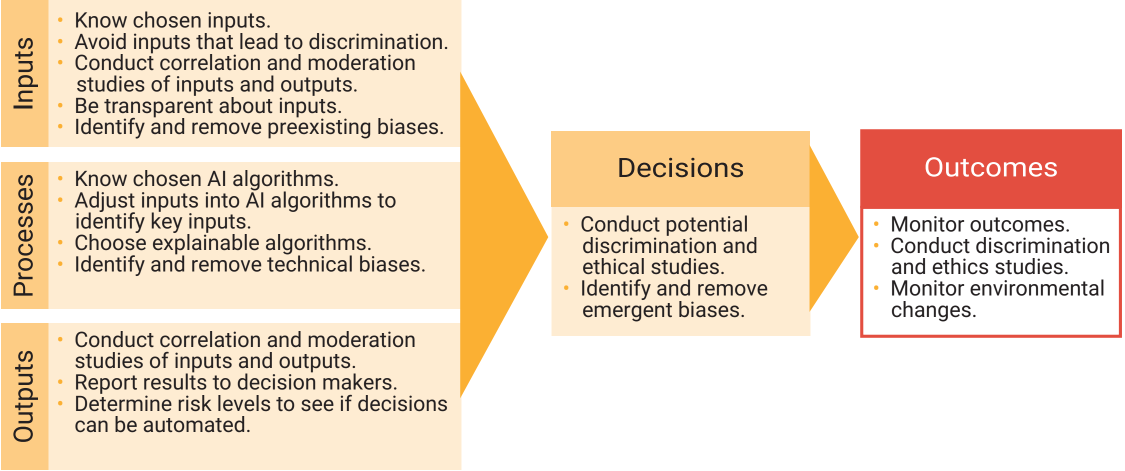


FIGURE 3

How to Avoid AI Algorithm Bias and Discrimination



Inputs

- Know chosen inputs.
- Avoid inputs that lead to discrimination.
- Conduct correlation and moderation studies of inputs and outputs.
- Be transparent about inputs.
- Identify and remove preexisting biases.

Processes

- Know chosen AI algorithms.
- Adjust inputs into AI algorithms to identify key inputs.
- Choose explainable algorithms.
- Identify and remove technical biases.

Outputs

- Conduct correlation and moderation studies of inputs and outputs.
- Report results to decision makers.
- Determine risk levels to see if decisions can be automated.

Decisions

- Conduct potential discrimination and ethical studies.
- Identify and remove emergent biases.

Outcomes

- Monitor outcomes.
- Conduct discrimination and ethics studies.
- Monitor environmental changes.

in an accident risk model. But enterprises should be transparent about their inputs to ensure that the public is aware of what factors are considered in the decision-making process. Conducting correlation studies of the variables before introducing them into the system may provide an early indication of potential discrimination problems.

Preexisting bias can also be introduced with inputs. This can be done by choosing to include potentially discriminating inputs or by choosing other inputs that may act as proxies for gender, age and ethnicity, such as choosing personal economic variables as inputs due to socioeconomic relationships. Decision makers must know which inputs are being used by the AI algorithms.

Step 2: Processes

The algorithms used to convert inputs to outputs must be understood at the highest possible level of detail. This is easy for symbolic algorithms, but much more difficult for some statistical AI techniques. Decision makers should request that the inputs used in developing and training statistical AI models be identified to determine which variables are being used. Another consideration is to ascertain why a particular AI technique was chosen and to determine the incremental explanatory power of a model that cannot be explained vs. one that can be explained. Different AI algorithms should be tested to determine the accuracy of each one, and further investigation into inputs is warranted when unexplainable models significantly outperform explainable models.

Investigating multiple models can also help identify technical bias. For example, gone are the days when weather forecasters relied on just one model. It is much more common now for spaghetti models to be used, giving an overview of what many models are predicting instead of relying on just one.

After an algorithm has been developed, user acceptance testing (UAT) is an important step to ensure that the algorithm is truly doing what it was designed to do. UAT should "examine all aspects of an algorithm and the code itself."[17] For nondiscriminatory AI applications, it is important to consider justice as a target value and to provide people disadvantaged by an AI-based decision with the ability to enforce their rights.[18]

Step 3: Outputs

This is the last step before a decision is made. Correlation and moderation studies of the outputs and the most common inputs associated with discrimination (e.g., gender, race, ethnicity) should be conducted. The results should be reported to decision makers to ensure that they are aware of how inputs are related to outputs.

Step 4: Decisions

The AI system is reconnected to the outside environment during this step. Decision makers must understand that decisions made using AI have consequences for the people or systems associated with those decisions. It is very important at this point to analyze whether discrimination can result from the decisions being made. This is especially important when the decision is directly connected to the output without any human intervention. However, it is important to note that human interaction does not eliminate the possibility of emergent bias, as human beings are inherently biased.[19]

Step 5: Outcomes

At this point, the decisions have interacted with the environment and the effects are known—but only if the enterprise follows up and measures the actual outcomes. Too often, enterprises do not monitor what has happened and continue to use the same inputs and processes, unknowingly allowing biases to shape the outputs that influence the decision-making process.

Too often, enterprises do not monitor what has happened and continue to use the same inputs and processes, unknowingly allowing biases to shape the outputs that influence the decision-making process.

The Final Check: Ethics

Understanding inputs, processes, outputs, decisions and outcomes may ensure that bias has been removed from an AI algorithm and potential discrimination has been identified. However, enterprises can follow all these steps and still have ethical issues associated with the decision-making process. The life cycle model for developing ethical AI is a great approach for identifying and removing ethical AI issues.[20] What decision makers may still be missing is a framework for deciding what is unethical.

There are many frameworks that address the ethical aspects of algorithms. Some of these frameworks are specialized, covering a particular area such as healthcare.[21] Two frameworks—the PAPA model[22] and the AI4People model[23]—have gained widespread application. They present an interesting contrast since the former was developed at the end of the 1980s and the latter was developed in 2018, in a completely different world of technology.

PAPA Model

The PAPA model identifies four key issues to preserve human dignity in the information age:

1. **Privacy**—The amount of private information one wants to share with others and the amount of information that is intended to stay private
2. **Accuracy**—Who is responsible for the correctness of information
3. **Property**—Who owns different types of information and the associated infrastructure
4. **Accessibility**—How information is made available to different people and under what circumstances access is given[24]

AI4People Model

The AI4People model is much more recent. It was developed by analyzing six existing ethical frameworks and identifying 47 principles for making ethical decisions.[25] Five core principles emerged:

1. **Beneficence**—The promotion of well-being and the preservation of the planet
2. **Nonmaleficence**—The avoidance of personal privacy violations and the limitations of AI capabilities, including not only humans' intent to misuse AI but also the sometimes unpredictable behavior of machines
3. **Autonomy**—The balanced decision-making power of humans and AI
4. **Justice**—The preservation of solidarity and prevention of discrimination.
5. **Explicability**—Enabling of the other principles by making them understandable, transparent and accountable[26]

Figure 4 compares these models and presents ethical AI algorithm considerations for decision makers.

These two ethical models show that enterprises should consider other outcome variables that can determine the ethical implications of their decisions. This should be done not only by the software developers, but also by the stakeholders involved in the algorithm.[27] Decision makers should evaluate each of the areas listed in **figure 4** and determine which additional outcome variables they should collect and track to ensure that their AI algorithms are not negatively impacting ethical interests. The limited views of one decision maker may be inadequate for

FIGURE 4

Comparison of Ethical Models and AI Algorithm Considerations

PAPA	AI4People	AI Algorithm Considerations
Privacy	Nonmaleficence	Avoid violations of personal privacy, security and possible protective measures; do no harm.
Accuracy	Justice	Produce nondiscriminatory outputs and preserve solidarity by using accurate data.
	Explicability	Provide understandable and transparent inputs and processes with associated accountability for outputs, decisions and outcomes.
Property	Not addressed	Identify ownership of information and related infrastructure.
Accessibility	Not addressed	Discuss how information is made available to different people and under what circumstances.
	Beneficence	Promote human well-being and planet preservation.
	Autonomy	Balance decision-making power between humans and AI.

this task. One option is to assemble a diverse board to evaluate these areas and make recommendations about which outcomes to track. This may help expose initially unidentified concerns that can be incorporated into the AI algorithms' redesign to ensure that ethical issues are addressed.[28]

> The prerequisites for an ethical AI algorithm are unbiased data, explainable processes, unbiased interpretation of the algorithm's output and monitoring of the outcomes for ethical, legal and societal effects.

Conclusion

The use of AI algorithms can contribute to human self-realization and result in increased effectiveness and efficiency. Therefore, this technology is already being applied in numerous industries. However, there are risk factors and ethical concerns regarding the collection and processing of personal data and compliance with societal norms and values. The prerequisites for an ethical AI algorithm are unbiased data, explainable processes, unbiased interpretation of the algorithm's output and monitoring of the outcomes for ethical, legal and societal effects.

AI algorithms can improve organizational performance by better predicting future outcomes. However, decision makers are not absolved from understanding the inputs, processes, outputs and outcomes of the decisions made by AI. Taking a systems theory approach may help enterprises ensure that the legal, ethical and social aspects of AI algorithms are examined. Outcomes based on AI algorithms must not be assumed to be rigid and finite because society and technology are constantly changing. Similarly, ethical principles may change too. When the environment for an algorithm changes, the algorithm must be adapted, even if it requires going beyond the original specifications.[29]

Endnotes

1 Zoldi, S.; "It's 2021. Do You Know What AI Is Doing?" FICO Blog, 25 May 2021, *https://www.fico.com/blogs/its-2021-do-you-know-what-your-ai-doing*

2 *Ibid.*

3 O'Neil, C.; "The Era of Blind Faith in Big Data Must End," Ted Talks, 2017, *https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end*

4 Zielinski, L. *et al*.; "Atlas of Automation—Automated Decision-Making and Participation in Germany," Algorithmwatch, 2019, *https://atlas.algorithmwatch.org/*

5 Johnson, J. A.; F. E. Kast; J. E. Rosenzweig; "Systems Theory and Management," *Management Science*, vol. 10, iss. 3, January 1964, p. 193–395, *https://www.jstor.org/stable/2627306*

6 Haylock, D.; F. Thangata; *Key Concepts in Teaching Primary Mathematics*, Sage, United Kingdom, 2007

[7] Horruitiner, C. D.; "All Models Are Wrong," *Medium*, 13 January 2019, *https://medium.com/the-philosophers-stone/all-models-are-wrong-4c407bc1705*

[8] Pearce, G.; "Focal Points for Auditable and Explainable AI," *ISACA® Journal*, vol. 4, 2022, *https://www.isaca.org/archives*

[9] Friedman, B.; H. Nissenbaum; "Bias in Computer Systems," *ACM Transactions on Information Systems*, vol. 14, July, 1996, p. 330–347, *https://doi.org/10.1145/230538.230561*

[10] Mitchell, T. M.; *The Need for Biases in Learning Generalizations*, Rutgers University, New Brunswick, New Jersey, USA, 1980, *https://www.cs.cmu.edu/~tom/pubs/NeedForBias_1980.pdf*

[11] Scarpino, J.; "Evaluating Ethical Challenges in AI and ML," *ISACA Journal*, vol. 4, 2022, *https://www.isaca.org/archives*

[12] *Ibid*.

[13] *Op cit* Friedman and Nissenbaum

[14] Angwin, J.; J. Larson; S. Mattu; L. Kirchner; "Machine Bias," *Propublica*, 23 May 2016, *https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing*

[15] *Ibid*.

[16] Beck, S. *et al*.; "Künstliche Intelligenz und Diskriminierung," 7 March 2019, *https://www.plattform-lernende-systeme.de/publikationen-details/kuenstliche-intelligenz-und-diskriminierung-herausforderungen-und-loesungsansaetze.html*

[17] Baxter, C.; "Algorithms and Audit Basics," *ISACA Journal*, vol. 6, 2021, *https://www.isaca.org/archives*

[18] *Op cit* Beck

[19] *Op cit* Scarpino

[20] *Ibid*.

[21] Xafis, V.; G. O. Schaefer; M. K. Labude *et al*.; "An Ethics Framework for Big Data in Health and Research," ABR, vol. 11, 1 October, 2019, p. 227–254, *https://doi.org/10.1007/S41649-019-00099-x*

[22] Mason, R.; "Four Ethical Issues of the Information Age," *MIS Quarterly*, vol. 10, 1986, p. 5–12

[23] Floridi, L.; J. Cowls; M. Beltramelti *et al*; "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations," *Minds and Machines*, vol. 28, December 2018, p. 689-707, *https://doi.org/10.1007/S11023-018-9482-5*

[24] *Op cit* Mason

[25] *Op cit* Floridi *et al.*

[26] Barton, M. C.; J. Pöppelbuß; "Prinzipien für die ethische Nutzung künstlicher Intelligenz," *HMD*, vol. 59, 2022, p. 468–481, *https://doi.org.10.1365/S40702-022-00850-3*

[27] Häuber, H.; "Data Ethics Frameworks,". *Information*, *Wissenschaft and Praxis*, vol. 72, iss. 5-6, 2021, p. 291–298, *https://doi.org/10.1565/iwp-2021-2178*

[28] van Bruxvoort, X.; M. van Keulen; "Framework for Assessing Ethical Aspects of Algorithms and Their Encompassing Socio-Technical System," *Applied Science*, vol. 11, 2021, p. 11187, *https://doi.org/10.3390/app112311187*

[29] Pearce, G., M. Kotopski; "Algorithms and the Enterprise Governance of AI," *ISACA Journal*, vol. 4, 2021, *https://www.isaca.org/archives*

Performing a Cybersecurity Audit of an Electric Power Transmission Systems Operator

日本語版も入手可能
www.isaca.org/currentissue

Electricity is the lifeblood of many modern technologies and one of the often overlooked services that makes life easier. Many people, especially in developed countries, can hardly imagine life without it. Water supplies, heating, cooling, food processing, telecommunications and many other goods and services are fundamentally dependent on electricity. Most countries in the world consider electricity transmission and distribution infrastructure and services fundamental parts of their critical infrastructures. For example, the Republic of Slovenia (Slovenia) declared the electric power transmission organization a crucial element of its infrastructure.

Because power transmission infrastructures are critical, protecting the organizations that run these services from cyberthreats is also crucial, especially because cyberthreats and cyberattacks are increasing.[1] A study from 2021 found that 83 percent of critical infrastructure organizations experienced operational technology breaches in the prior 36 months.[2] One of the first large-scale, well-known cyberattacks on a power grid occurred in Ukraine in December 2015.[3] It set a precedent for the security of power grids around the world.[4] Cybersecurity organizations such as the European Union Agency for Cybersecurity (ENISA), ISACA®, the International Organization for Standardization (ISO) and the US National Institute of Standards and Technology (NIST) issued guidelines, methods and approaches to address the problem and increase awareness of preparedness against cyberattacks. In the European Union, the ENISA reviewed the status of awareness of cybersecurity among member states.[5] The main purpose of ENISA report is to assist member states in building their cybersecurity capacities by analyzing best practices for raising citizens' awareness of cybersecurity. The report also offers recommendations in four areas:

1. Building capacities for cybersecurity awareness
2. Regularly assessing trends and challenges
3. Measuring cybersecurity behavior
4. Planning cybersecurity awareness campaigns

Nearly every country has a Supreme Audit Institution (SAI), which is an independent national institution that conducts audits of government activities, and nearly every SAI in the world is a member of the International Organization of Supreme Audit Institutions (INTOSAI), which works to establish and disseminate international standards and good practices.

The SAI of Slovenia carried out an audit to assess the cyberthreat preparedness of an organization that operates critical infrastructure for electric power transmission. Understanding how to perform an IT performance audit, report on an organization that is part of a nation's critical infrastructure, and mitigate any possible negative effects of such incidents are critical. Incidents can adversely affect many other services and organizations—and the nation as a whole.

The Audit Environment

The Court of Audit of Slovenia is the highest audit body for supervising state accounts, the state budget and all public spending in Slovenia.[6] The Court of Audit performs all forms of audits (i.e., compliance, financial, performance) in accordance with domestic legislation and INTOSAI standards. The Court of Audit

BOSTJAN DELAK | PH.D., CISA

Is an assistant professor at the Faculty of Information Studies (Novo Mesto, Slovenia). Previously he worked as an information system auditor at the Supreme Audit Institution of the Republic of Slovenia. His research interests include information system analysis, due diligence and knowledge management.

MIROSLAV KRANJC | PH.D.

Is a supreme state auditor and founding leader of the Department for Performance Audit at the Supreme Audit Institution of the Republic of Slovenia. He is passionate about IT and environmental auditing and lectures on various topics related to performance auditing.

of Slovenia audits various types of entities including entities that provide public services or provide goods to the public on a concession basis.[7]

ELES, Ltd., Electricity Transmission System Operator (ELES), a state-owned legal entity, is the operator of the electric power transmission network of Slovenia.[8] ELES has been providing safe, reliable and uninterrupted electric power transmission throughout Slovenia and across its borders for 90 years. ELES endeavors to strategically, responsibly, and sustainably plan, construct, and maintain Slovenia's high-voltage transmission network at three voltage levels: 400 kV, 220 kV and partly in 110 kV.

The electric power transmission network cannot be operated on its own. It must be connected to networks in neighboring countries and integrated into a wider electric power system; therefore, ELES closely cooperates with the neighboring system operators and actively participates in many regional and international associations. ELES, as the only Slovene electric power transmission operator, is actively involved in the design and development of a unified European market through the professional association the European Association for the Cooperation of Transmission System Operators for Electricity (ENSTO-E)[9] and various (inter)regional initiatives and projects.[10] **Figure 1** presents the position of ELES in relation to electricity generation, electricity distribution to end users, supply of electricity to major direct customers and the connection to international transmission networks.

Understanding how to perform an IT performance audit, report on an organization that is part of a nation's critical infrastructure, and mitigate any possible negative effects of such incidents are critical.

The Audit Motivation and Criteria

The motive of the Court of Audit was to assess the readiness of ELES as a critical infrastructure manager against cyberthreats and, thus, its potential to reduce the risk of interruptions in the distribution of electricity to consumers.

According to ISSAI 300, auditors should establish suitable criteria that correspond to the audit questions and are related to the principles of economy, efficiency and effectiveness.[11] In the case of auditing readiness of cybersecurity at a critical infrastructure organization, audit criteria were based on provisions of the Critical Infrastructure Act and the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Legislation

In 2018, Slovenia enacted the Critical Infrastructure Act[12] and the Information Security Act.[13] The Critical Infrastructure Act regulates the identification and determination of the critical infrastructure of Slovenia, the principles and planning of critical infrastructure protection, and the tasks of bodies and organizations in the field of critical infrastructure and information, including reporting, decision support, data protection and control. The act defines critical infrastructure as:

> *[T]hose capacities that are of key importance to the state and the cessation of their operation or their destruction would significantly affect and have serious consequences for national security, economy and other key social functions and health, safety, protection and well-being.*[14]

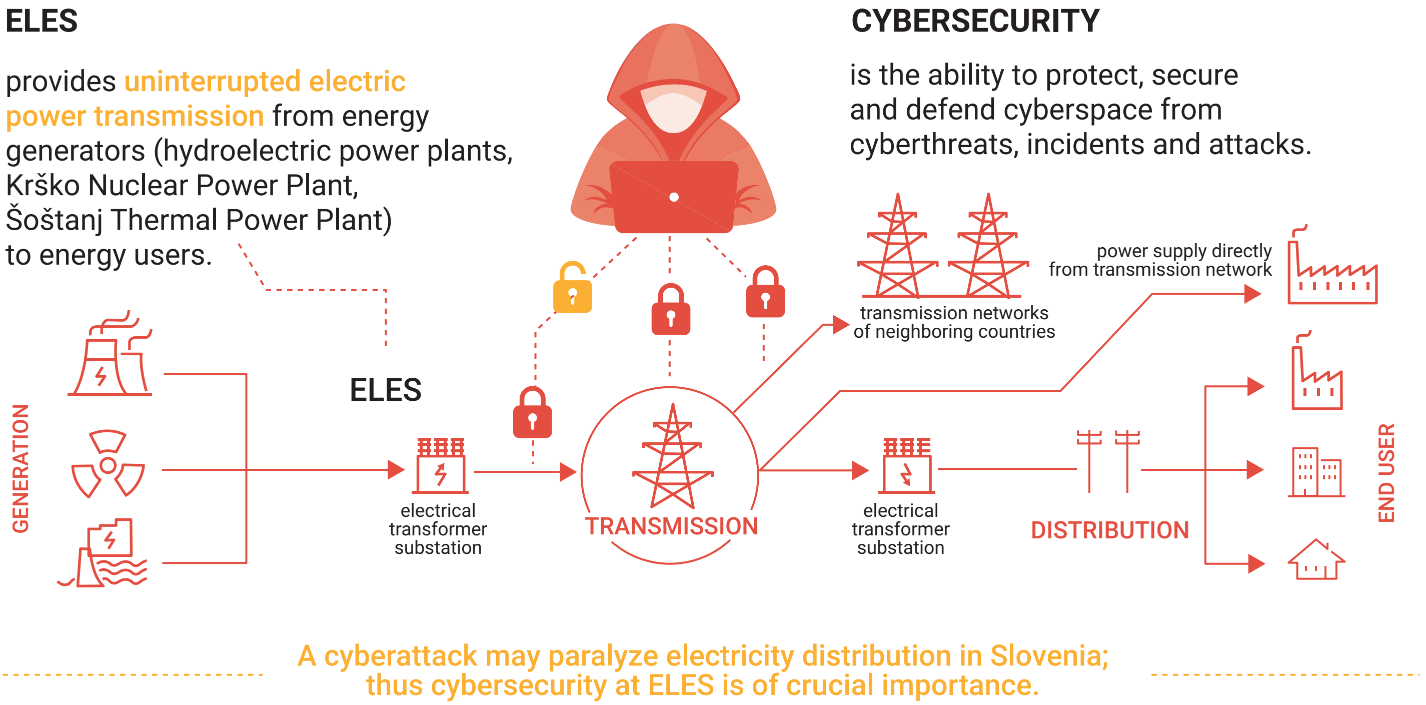
The Information Security Act regulates the field of information security and defines measures to achieve a high level of security of networks and information systems in Slovenia. These measures are essential for the smooth operation of the state in all security conditions and to provide essential services for

LOOKING FOR MORE?

- Read *Governance Roundup—What Are You Doing About Environmental, Social and Governance Factors in Your Enterprise?* *www.isaca.org/governance-roundup-esg*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 1

Role of ELES



ELES

provides uninterrupted electric power transmission from energy generators (hydroelectric power plants, Krško Nuclear Power Plant, Šoštanj Thermal Power Plant) to energy users.

CYBERSECURITY

is the ability to protect, secure and defend cyberspace from cyberthreats, incidents and attacks.

GENERATION
ELES
electrical transformer substation
TRANSMISSION
transmission networks of neighboring countries
power supply directly from transmission network
electrical transformer substation
DISTRIBUTION
END USER

A cyberattack may paralyze electricity distribution in Slovenia; thus cybersecurity at ELES is of crucial importance.

Source: Republic of Slovenia Court of Audit, *Audit Report: Efficiency of Managing Cybersecurity Risk of the ELES Company Critical Infrastructure*, 2021, Slovenia, *https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS_ELES_infografika-EN.pdf*. Reprinted with permission.

maintaining key social and economic activities. With the adoption of this act, Slovenia transposed into Slovenian legislation Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of security of networks and information systems in the European Union.[15]

Critical Infrastructure Act

The Critical Infrastructure Act includes provisions that require critical infrastructure organizations to develop and manage risk assessments and measures to protect critical infrastructure. The risk assessment must abide by the instructions for risk assessment of the operation of critical infrastructure, adopted by the Ministry of Defense of Slovenia. The assessment should also follow expert guidelines prepared for individual critical infrastructure sectors. Ongoing measures are being implemented in all situations, and, in the event of a crisis, emergency or increased threat to critical infrastructure, their implementation may be intensified. Additional measures shall be implemented in the event of an increased threat to critical infrastructure, an emergency or a crisis if ongoing measures, even if their implementation is escalating, are not sufficient.

NIST Framework for Improving Critical Infrastructure Cybersecurity

For the second set of criteria, the auditors chose the NIST Cybersecurity Framework (CSF) function Detect and Respond, as displayed in the shaded boxes in **figure 2**.[16]

The Identify and Protect functions are covered by the first audit criteria—provisions of the Critical Infrastructure Act. The auditors did not choose the last function, Recover, since ELES had no previous experience with cyberattacks.

The Audit Process

The audit was a performance audit based on INTOSAI standards and principles.[17] The main audit question was whether ELES had effectively managed cybersecurity in the area of critical infrastructures. The auditing period was from 1 January 2019 to 31 July 2020. The audit started in December 2019 and the final report was published in August 2021. The audit team consisted of one information system auditor and one state auditor with legal knowledge. The audit team prepared the audit plan, requested the documentation and questionnaires regarding critical infrastructure, completed more than 10 interviews and function tests (one-third live and the rest via videoconferencing systems due to COVID-19 restrictions) and reviewed several on-site locations. For NIST CSF functions testing, auditors used COBIT® 5 and ISO/International Electrotechnical Commission (IEC) standard ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements controls*.[18] The testing period was from 4 June 2020 to 24 September 2020. During the testing period, all 34 subcategories by informative references/controls were tested. After collecting enough information and evidence to present to the auditee, the team prepared a draft report, which was first coordinated with the Supreme State Auditor and legal service of the Court of Audit and agreed on with the responsible deputy auditor general. The official draft report was sent to ELES, followed by a clearance meeting with the auditee. After accepting comments and amendments from the auditee, the audit report proposal was prepared and issued to the auditee. At that point, there were no other objections, so after additional independent proofreading and review, the final audit report was sent to the auditee and Parliament and was published on the Court of Audit website.

Audit Findings

The Court of Audit found that ELES introduced risk management in 2009 and set up a comprehensive risk management system in the years that followed. ELES kept a computerized catalog of risk by field of operation and, in 2019, it also introduced records of risk in the field of critical infrastructure. ELES identified sources of risk to critical infrastructure operations, analyzed and evaluated risk to critical infrastructure operations, determined sources of risk, monitored the state of critical infrastructure, duplicated control centers and devised security plans, all in a timely manner. ELES also applied a documented information security management system and is certified in ISO/IEC 27001:2013. The organization was concluding the introduction of a business continuity management system at the time of the audit review. ELES's business continuity management system was used to carry out risk assessment of critical infrastructure and impose measures to protect critical infrastructure. In addition, ELES responded to the COVID-19 pandemic by adopting various measures, many of which related to the organization of human resources, such as the creation of a sealed control center, in which some employees lived and worked in two-week-long shifts; isolation of power transmission management support teams; and working from home. This ensured continuous operation of the processes related to the transmission of electricity.

FIGURE 2

NIST CSF Functions and Categories

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security and Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

Source: US National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, USA, 2018, *https://www.nist.gov/cyberframework*. Reprinted with permission.

Figure 3 presents several of the findings of the audit.

ELES efficiently detected cyberthreats by defining and analyzing security event roles and responsibilities. The organization followed established procedures for submitting information about detected events, continuously improved detection processes and built knowledge bases relating to security events. ELES had a plan for responding to cyberthreats. Its employees were appropriately trained in responding to and reporting on security events to relevant recipients within and outside ELES.

ELES also analyzed notices of security events and took measures to classify security incidents and understand their impact on the organization. It applied processes for monitoring, analyzing and responding to vulnerabilities and for limiting and mitigating security incidents. ELES had no established strategy specifically for the field of cybersecurity; however, it did establish policies pertaining to all segments of the integrated management system through management reviews subject to ongoing inspection and relevant updates.

There are several possibilities for improvements that ELES is aware of and has thus introduced:

- Full implementation of a business continuity management system
- Integration of all detected events to a single dashboard
- Execution of independent penetration tests after current IT projects are finalized
- Implementation of video surveillance of areas in which it does not currently exist

Opinion of the Court of Audit

According to the opinion of the Court of Audit, ELES was efficient in managing cybersecurity risk relating to critical infrastructure during the period covered by the audit.

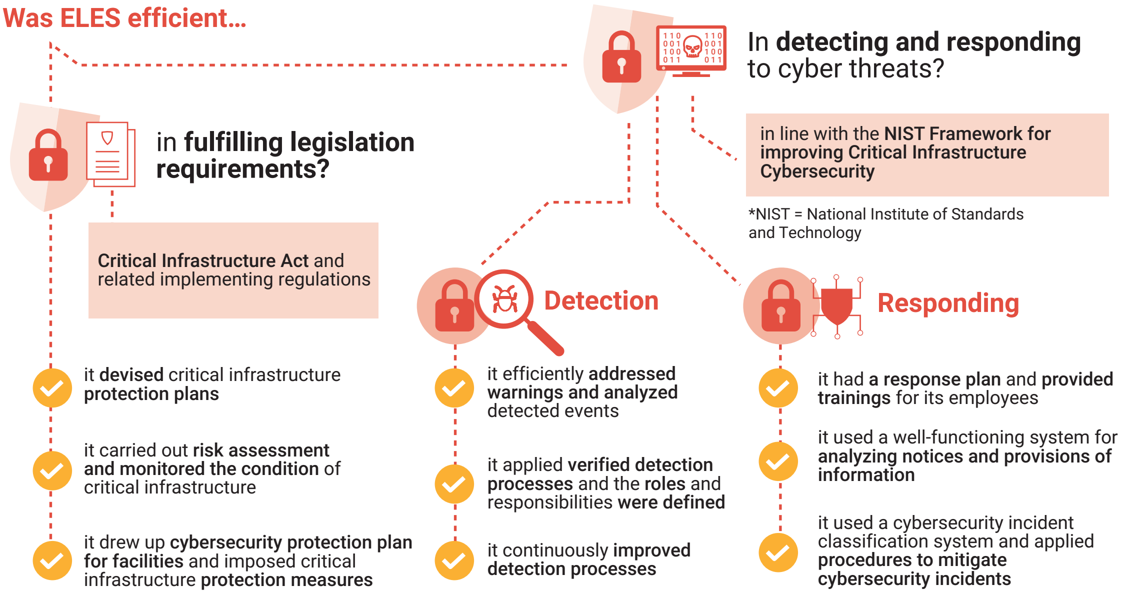
The Court of Audit did not demand that ELES submit a response report; however, it proposed several recommendations for further improvements:[19]

- Periodically manage the transmission of electricity from the reserve control center
- Regularly (e.g., annually) plan and conduct penetration testing
- Periodically test the process of reporting security events to external stakeholders
- Examine the possibility of establishing a common knowledge base on detected events and their resolutions

Figure 4 presents the opinion of the Court of Audit.

FIGURE 3

Audit Findings



Was ELES efficient...
in **fulfilling legislation requirements?**
Critical Infrastructure Act and related implementing regulations
In **detecting and responding** to cyber threats?
in line with the **NIST Framework for improving Critical Infrastructure Cybersecurity**
*NIST = National Institute of Standards and Technology
Detection
Responding

✓ it **devised** critical infrastructure **protection plans**

✓ it carried out **risk assessment and monitored the condition** of critical infrastructure

✓ it drew up **cybersecurity protection plan for facilities** and imposed critical infrastructure **protection measures**

✓ it efficiently **addressed warnings and analyzed** detected events

✓ it applied **verified detection processes** and the **roles** and responsibilities **were defined**

✓ it continuously **improved detection processes**

✓ it had **a response plan** and **provided trainings** for its employees

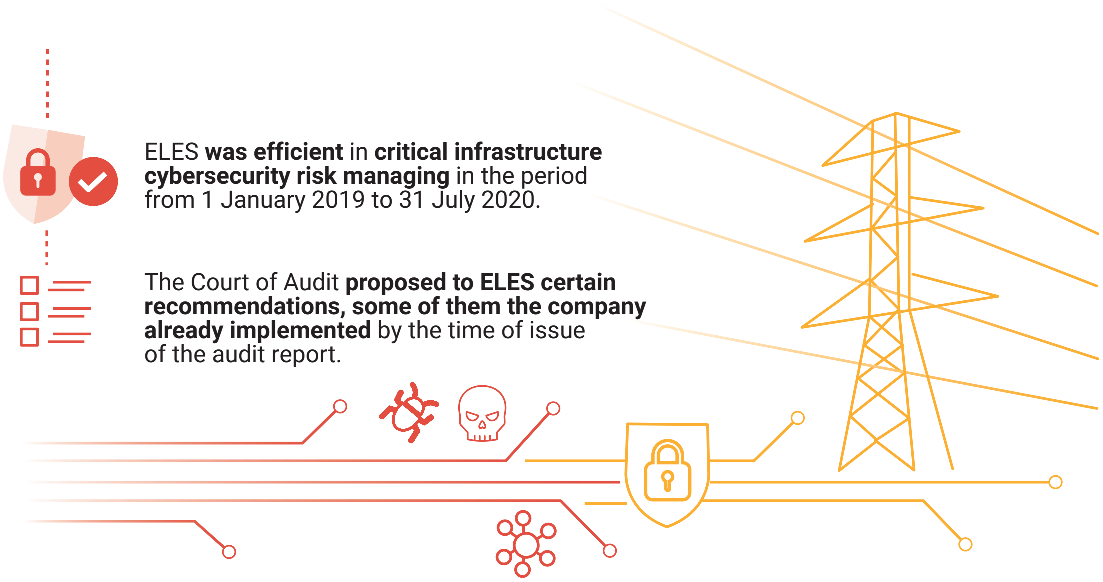
✓ it used a well-functioning system for **analyzing notices and provisions of information**

✓ it used a cybersecurity incident classification system and applied **procedures to mitigate cybersecurity incidents**

Source: Republic of Slovenia Court of Audit, *Audit Report: Efficiency of Managing Cybersecurity Risk of the ELES Company Critical Infrastructure*, 2021, Slovenia, *https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS_ELES_infografika-EN.pdf*. Reprinted with permission.

FIGURE 4

Opinion of the Court of Audit



ELES **was efficient** in **critical infrastructure cybersecurity risk managing** in the period from 1 January 2019 to 31 July 2020.

The Court of Audit **proposed to ELES certain recommendations, some of them the company already implemented** by the time of issue of the audit report.

Source: Republic of Slovenia Court of Audit, *Audit Report: Efficiency of Managing Cybersecurity Risk of the ELES Company Critical Infrastructure, https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS_ELES_infografika-EN.pdf*. Reprinted with permission.

Audit Limitations

Though it ultimately proved effective, the audit had several limitations of note. The audit did not include an assessment of the auditee's business continuity management system or the continuous operation of the auditee's information system. It also did not account for penetration tests.

Conclusion

The Court of Audit chose ELES as the subject of its first performance audit on cybersecurity of critical infrastructure because the organization operates the transmission of electricity from a source to larger customers. The audit showed that ensuring that the audit team included an expert in IT systems and information security and a legal expert was helpful. The selection of audit criteria was also beneficial for reviewing in detail the readiness of ELES for potential cyberattacks. This case study also shows that additional experts in the field of hacking and penetration testing should be included in the audit team to perform a more detailed cybersecurity audit. The Court of Audit will invest effort to continue to plan and perform cybersecurity performance audits of organizations that manage critical infrastructure to assess their cybersecurity risk management and confirm their decisions on spending public money to mitigate cyberthreats.

Endnotes

1 Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents Since 2006*, USA, 2021, *https://csis-website-prod.s3.amazonaws.com/s3fs-public/220104_Significant_Cyber_Events.pdf*

2 *Dark Reading*, "Eighty-Three Percent of Critical Infrastructure Organizations Suffered Breaches, 2021 Cybersecurity Research Reveals," 9 November 2021, *https://www.darkreading.com/vulnerabilities-threats/83-of-critical-infrastructure-organizations-suffered-breaches-2021-cybersecurity-research-reveals*

3 International Cyber Law: Interactive Tool Kit, "Power Grid Cyberattack in Ukraine (2015)," 4 June 2021, *https://cyberlaw.ccdcoe.org/wiki/*Power_grid_cyberattack_in_Ukraine

4 Zetter, K.; "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/*

5 European Union Agency for Cybersecurity (ENISA), *Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies*, Greece, 29 November 2021, *https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity*

6 Republic of Slovenia Court of Audit, *https://www.rs-rs.si/en/*

7 Republic of Slovenia Court of Audit, Court of Audit Act, Article 20, *https://www.rs-rs.si/en/about-the-court-of-audit/legal-basis/court-of-audit-act/*

8 ELES Company, *https://www.eles.si/en*

9 The European Association for the Cooperation of Transmission System Operators for Electricity (ENTSOE), *https://www.entsoe.eu/*

10 ELES Company, "About the Company," *https://www.eles.si/en/about-the-company*

11 International Organisation of Supreme Audit Institutions (INTOSAI), ISSAI 300: Performance Audit Principles, Austria, 2019, *https://www.intosai.org/fileadmin/downloads/documents/open_access/ISSAI_100_to_400/issai_300/ISSAI_300_en_2019.pdf*

12 National Assembly of the Republic of Slovenia, Critical Infrastructure Act, *http://www.pisrs.si/Pis.web/npbDocPdf?idPredpisa=ZAKO8464&idPredpisaChng=ZAKO7106&type=pdf*

13 National Assembly of the Republic of Slovenia, Information Security Act, *http://www.pisrs.si/Pis.web/npbDocPdf?idPredpisa=ZAKO8380&idPredpisaChng=ZAKO7707&type=pdf*

14 *Op cit* Critical Infrastructure Act

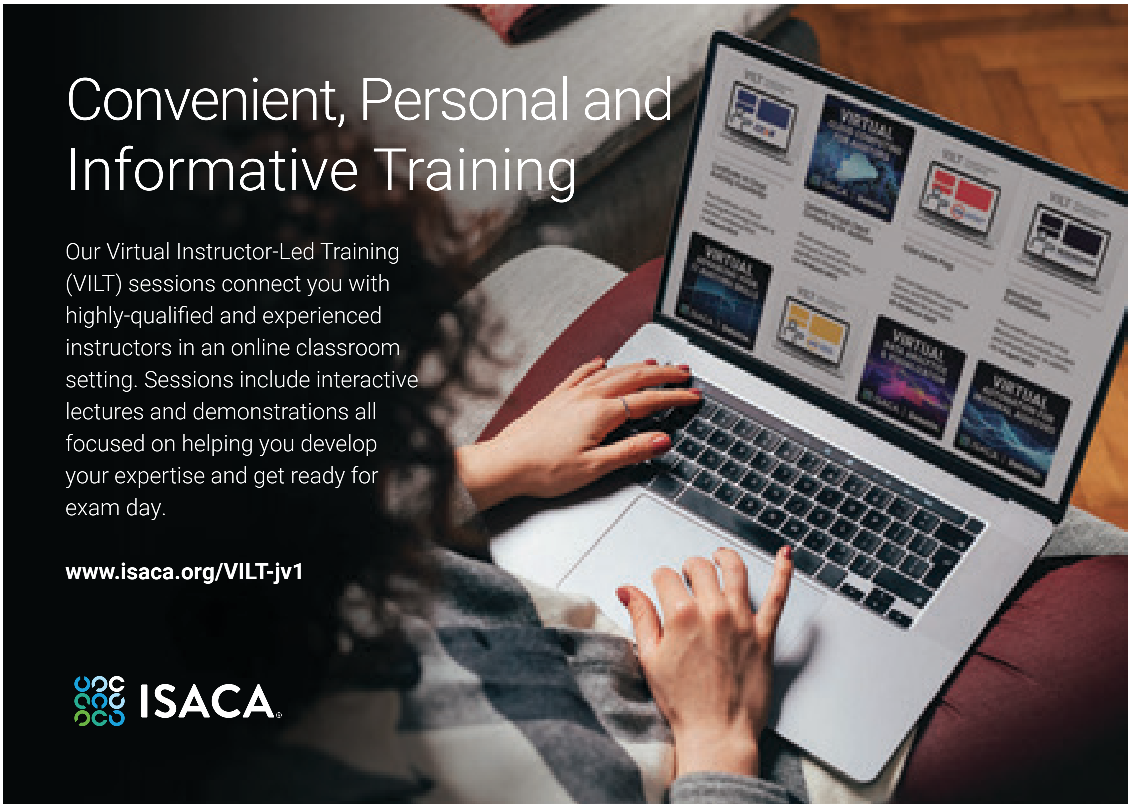
15 Directive (EU) 2016/1148 of the European Parliament and of the Council, *Official Journal of the European Union*, Belgium, 6 July 2016, *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN*

16 National Institute of Standards and Technology (NIST), NIST Cybersecurity Framework, USA, *https://www.nist.gov/cyberframework*

17 *Op cit* INTOSAI

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

19 Republic of Slovenia Court of Audit, *Audit Report 2021: Effectiveness of Cyber Security Management for the Field of Critical Infrastructure in ELES*, Slovenia, 2021, *https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/CS_ELES_RSP_RevizijskoP.pdf*



Business and Technology Drivers for Decentralized Cloud Systems

A major technological advance in the computing industry has been the adoption of cloud system models. The US National Institute of Standards and Technology (NIST) defines cloud computing as:

> *[A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*[1]

But what is the frontier of the current cloud systems model and its offerings, and how can the present cloud model mature to address continued access, security and privacy challenges? These challenges are the drivers for extending the boundaries of the current cloud model to conform to and mitigate industry and technological pressures.

In the competitive business market and with fast-moving technology advancements, cloud providers must respond to and comply with cost management, security and performance burdens placed on various business stakeholders due to the shortcomings of the classical centralized cloud model. This has led to the birth of a new derivative of centralized cloud systems: decentralized cloud systems.

Prior to the cloud, organizations had to commit to large investments in computing infrastructure, applications and extensive IT operations. The first phase of the cloud evolution (cloud 1.0) introduced Software as a Service (SaaS), which created a virtual place to store data and applications (apps), disrupting standard IT operations with à la carte business process applications built on virtualization with no upfront investment. Then, cloud 2.0 disrupted the IT infrastructure of application development with offerings of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Cloud 2.0 allowed organizations to take control of their data and introduced services such as big data, artificial intelligence (AI) and machine learning (ML), along with development concepts such as containerization.[2, 3]

Emerging cloud 3.0 technologies will be driven by the ability to compute anywhere and will use a scale-and-adapt approach. Cloud 3.0 will disrupt application development in organizations across all industries. It will be based on building high availability and decomposing software into loosely connected subcomponents called "microservices."[4, 5] It will lead to organizations adopting and migrating to the decentralized cloud.

A *Forbes* article notes that:

> *[The decentralized web] has led to the rise of distributed apps or decentralized apps (Dapps) where there will be no single point of failure and no central authority. They are transparent, have a greater level of encryption, have better heuristic methods to secure and are completely trustless.*[6]

ROBERT PUTRUS | CISM, CFE, PE, PMP

Is a professional with senior management experience in the areas of IT, cybersecurity, regularity and internal controls compliance, managed services, global transformation programs, portfolio and program management, and IT outsourcing. He has published many articles and white papers in professional journals, some of which have been translated into multiple languages. Putrus is quoted in publications, articles and books, including those used in Master of Business Administration programs in the United States. He can be reached at *https://www.linkedin.com/in/robert-putrus-cism-pmp-cfe-pe-8793256/.*

LOOKING FOR MORE?

- Read *Certificate of Cloud Auditing Knowledge Study Guide. www.isaca.org/CCAK-Study-Guide*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's *https://engage.isaca.org/onlineforums*

> Decentralized cloud systems are enabling the reconfiguration of the Internet to create a distributed global system that is less dependent on web platforms and data centers.

One of the most significant benefits of the decentralized web is the ability to access data from anywhere. One example of decentralized cloud computing is blockchain technology.

Blockchain

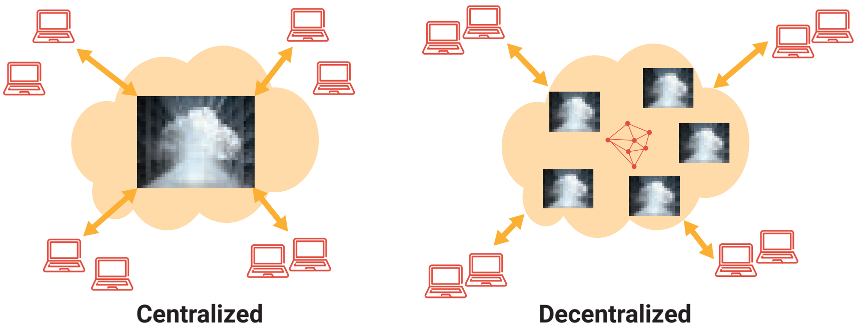
Blockchain is a decentralized system that stores data across multiple networks of computers. Blockchain applications are used in recording and storing transactions for cryptocurrencies. Blockchain can be applied to cryptocurrency, cybersecurity, accounting and record keeping, supply chain and healthcare.

A blockchain network is a technology infrastructure that is distributed and uses digital ledger technology to encrypt, track and secure all transactions on the network. Blockchain networks are immutable, meaning every transaction and record that is transmitted over a blockchain network is unable to be changed, altered or edited.[7]

In a decentralized blockchain network, no user has to know or trust any other user. Individual members on the network have a copy of the exact same data in the form of a distributed ledger. If a member's ledger is altered or corrupted in any way, it will be rejected by the majority of the members on the network.

FIGURE 1

Centralized vs. Decentralized Cloud Systems



Drivers of the Decentralization of Cloud Systems

The current cloud offers several advantages to organizations such as integration of centralized information systems, ease of access and cost effectiveness in investing and managing evolving technologies.

However, centralized cloud systems face major issues, most notably privacy and security. Centralized cloud systems are maintained by third parties that transfer and store data. The centralized cloud is vulnerable to several security threats such as malware, ransomware and man-in-the-middle (MitM) attacks.

Therefore, the market is witnessing a movement toward a decentralized cloud that supports multiple user access and ensures data security at the same time (**figure 1**). In a decentralized cloud system data are stored on multiple computers or on the entities taking part in the decentralized cloud. Data are encrypted, fragmented and then distributed across multiple hosting nodes (computers) worldwide.

The drivers of decentralized cloud systems relative to business and technology are privacy and security. Decentralized cloud systems are enabling the reconfiguration of the Internet to create a distributed global system that is less dependent on web platforms and data centers. The adoption of the decentralized cloud accelerated with the increase in remote work.[8]

The goal is to build a better Internet for the sake of creating automated services.

Data Privacy Concerns

Providers of centralized cloud services offer easy access to data and large data storage capacity. However, because only a small number of organizations control the major market share of cloud services, the risk to consumers includes price fixing, policy dictation, cyberattacks, loss of data and numerous privacy concerns.

Accessing data in a public cloud through the Internet introduces daunting uncertainties regarding where an organization's data are stored and by whom they are managed. There are also concerns about the lack of ownership and control when relying on third-party cloud service providers.

The primary function of decentralized cloud systems is to protect private and confidential data from unauthorized access and from transfer by external parties. Organizations cannot compromise on privacy. As such, many organizations are contemplating the adoption of emerging technologies such as blockchain as a viable solution.

Unlike in a centralized cloud, in a decentralized cloud with decentralized storage systems, multiple copies of the data are created, which eliminates the risk of data loss if a site goes down.

Security Concerns

The adoption of cloud models by various entities such as governmental agencies and public and private organizations has led to the institution of various compliance regulations with requirements for compliance.

The IT industry presented the decentralized cloud for consideration as an alternative to current cloud systems. Most decentralized clouds are based on blockchain technology, which offers transparency and reliability through cryptography.

Decentralized cloud systems implement client-side encryption enabling increasing security, privacy and control over users' data.

With a centralized cloud and in a given hosted facility, data are stored in a centralized location. In a decentralized cloud, the data are stored on the distributed nodes to ensure redundancy and avert server failure. In addition, the suspension of accounts and denials of services are significantly reduced. This eliminates a single point of failure and service interruption. Decentralized cloud systems store data in multiple computers connected through decentralized peer-to-peer (P2P) networks. These networks enable quicker data transfer in a decentralized cloud through nearby peers rather than through the servers hosted in a physical location.[9]

In a decentralized cloud, all data are encrypted. In addition, data are split and distributed over vast computers/nodes. It is close to impossible for any single node to access what is being stored on a decentralized computer network.

The Outlook for Decentralized Cloud Systems

Cloud computing and cloud storage have created many opportunities for organizations to save costs, increase security, increase flexibility, increase mobility, and enhance disaster recovery. However, the cybersecurity threats presented by a centralized cloud architecture have forced technologists to react to market demands for more robust protection. Some threats impact the core processes and foundations of data integrity, accountability, privacy, access control, authentication and authorization. Cloud decentralization is a solution that addresses the fundamentals of data privacy and security.

Blockchain has transformed the classical cloud architecture to create a market opportunity for more robust and predictable cloud outcomes with the implementation of an encryption algorithm. It complies with the market demand for assurance for data confidentiality, security and resilience concerning the cloud. In addition, blockchain technology, with its distributed ledger, enables many applications to ensure redundancy, confidentiality and transparency.

Making a comparative analysis of centralized vs. decentralized cloud systems may help organizations determine whether they can quickly adopt the new cloud model or if it makes more sense to stay with their current model. **Figure 2** illustrates an example comparison; however, the comparison can be amended based on similarities or differences in the attributes of both systems.

It is close to impossible for any single node to access what is being stored on a decentralized computer network.

Limitations of Decentralized Cloud Systems

Despite its potential, a decentralized cloud does have limitations. There are a number of challenges that need to be addressed, including:

- The technology is relatively new and will require time for adoption.
- Because the technology is relatively new, users may encounter problems when attempting to integrate multiple applications (and their data dependencies) in decentralized cloud systems.[10]
- A decentralized cloud lacks accountability for lost data or misplaced transactions.
- There is not a guarantee of privacy and security. A decentralized cloud will be a target of malicious actors who will form malicious nodes and execute hub attacks.

FIGURE 2

Comparative Attributes of Centralized vs. Decentralized Cloud Systems

Category	Centralized Cloud	Decentralized Cloud
Architecture	It provides scalability to infrastructure.	It provides scalability to infrastructure.
	Infrastructures have the entirety of data and resources stored in one geographical location.	Infrastructures have data and resources stored in a variety of different geographical locations.
	Networks are built based on traditional networks (i.e., data transmission takes place through a central server, becoming slow at the peak times).	Most infrastructures are built based on blockchain networks. Peer-to-peer technology is used to decentralize storage.
	Infrastructure requires that the enterprise trust the administration of the cloud provider because it is a centralized computer architecture.	No individual user has access to more permissions than another on a blockchain network. It is a distributed computer architecture.
	It relies on and trusts central providers.	No one has to know or trust anyone else. Decentralized clouds are based on blockchain, which offers transparency and reliability through cryptography.
Performance	The speed of data transfer relies on the servers hosted in a physical location, among other factors.	The speed of data transfer is higher in a decentralized cloud because it is based on peer-to-peer communication.
	It may impose capacity constraints and tends to have higher costs.	It is more cost effective because computing power and storage are not finite.
Security-General	A variety of security concerns include unauthorized access, malicious insiders, cyberattacks and insecure interfaces. It is also susceptible to data loss due to outages and has a single point of data failure.	Blockchain technology infrastructure is distributed and uses digital ledger technology. It is more resilient to outages due to geographical redundant technology.
Security-Cyberthreats	Data are susceptible to cybersecurity threats.	Security measures are inherited from the blockchain networks based on decentralized cloud computing infrastructures.
Security-Data Privacy	Data are not always encrypted.	Data are encrypted both in transit and at rest.
	Data can be encrypted using encryption software before being uploaded to the cloud. Data stored in the cloud are mostly encrypted.	Data are stored in a variety of geographical locations (geo-redundancy). Each piece of a data file is encrypted separately.
Security-Data Integrity	For redundancy, a multicloud solution that replicates data across multiple cloud computing providers can be used.	Geo-redundancy is the practice of storing data across a variety of locations.
	Physical integrity of the data is ensured due to physical security controls used at the cloud center. However, malicious insiders are a risk.	Data cannot be changed or edited by other users intentionally, in a malicious manner or by mistake.
	Computing infrastructures are easily affected by geographical outages or disasters.0	Cloud computing replicates resources and data across different locations automatically.
Cost Model	The cost model is scalable, easy to use and pay-as-you-go.	The cost model is scalable, easy to use and pay-as-you-go.
Use	It is the most widely used and accepted infrastructure.	It is less utilized by consumers and enterprises. Adoptability and acceptance are on the rise given the number of benefits that come with the decentralized cloud and its ability to protect and secure data.

- Compliance with laws and regulations is needed. A decentralized cloud requires a high degree of central support and monitoring to substantiate the evidence of IT controls.
- Developers are addressing rising performance-related challenges. For some, when data are dispersed across many storage devices, performance can be volatile.
- Users need to overcome the lack of trust when using P2P technology, bypassing centralized regulatory authorities.
- Security assurance continues to be a concern.

Conclusion

Decentralized systems change the game when it comes to cloud technology. They are a derivative of the current centralized cloud systems, but they offer a remedy for lack of data ownership and control, data breaches and security risk, increasing storage costs and low transmission speeds. Data privacy and data security are the main concerns when using centralized cloud systems, but in a decentralized cloud, data are more secure and kept private, file loss and data loss are diminished, download speeds are quicker, and it is easier to transfer files. In addition, in a decentralized cloud, there is no single point of failure, which increases reliability and redundancy in the event of failure.

For example, the transactions of digital currency are verified and the records are maintained by a decentralized system using cryptography rather than by a centralized authority. Cryptography provides secure communication techniques for the recipients in the presence of malicious adversaries.

The business demand for secure and inexpensive storage technology has paved the way for organizations to invest in and build momentum for decentralized cloud adoption, and blockchain has been a major factor in this change.

However, there are several challenges when integrating decentralized cloud systems,[11] including technology design and the need to further assure enterprises that privacy laws and IT security of the cloud can be guaranteed. The use of peer-to-peer communication in a decentralized network lacks accountability for lost data.

Decentralized cloud computing may present the solution to the challenges of the centralized cloud; however, the technology is still in the development stage and it may take several years to fully mature and be accepted by enterprise users.

> The business demand for secure and inexpensive storage technology has paved the way for organizations to invest in and build inertia for decentralized cloud adoption.

Endnotes

[1] Mell, P.; T. Grance; Special Publication (SP) 800-145 *The NIST Definition of Cloud Computing, National Institute of Standards and Technology (NIST)*, USA, September 2011, *https://csrc.nist.gov/publications/detail/sp/800-145/final*

[2] Fu, T.; "Top Three Challenges to Cloud 3.0," The New Stack, 20 May 2020, *https://thenewstack.io/top-3-challenges-to-cloud-3-0/*

[3] IQVIA, "Evolution to Cloud 3.0 and Roadmap for Adoption," 12 August 2019, *https://www.iqvia.com/library/white-papers/evolution-to-cloud-30-and-roadmap-for-adoption*

[4] *Op cit* Tu

[5] *Op cit* IQVIA

[6] Balanagu, R.; "The Evolution of Decentralized Cloud," *Forbes*, 23 February 2022, *https://www.forbes.com/sites/forbestechcouncil/2022/02/23/the-evolution-of-decentralized-cloud/?sh=37f381f03bcc*

[7] Liu, W.; "Research on Cloud Computing Security Problem and Strategy," Institute of Electrical and Electronics Engineers (IEEE) 2nd International Conference on Consumer Electronics, 17 May 2012, *https://ieeexplore.ieee.org/document/6202020*

[8] Beatrice, A.; "The Time Is Ripe for Companies to Adopt Decentralized Cloud Storage," Analytics Insight, 23 April 2021, *https://www.analyticsinsight.net/the-time-is-ripe-for-companies-to-adopt-decentralized-cloud-storage/*

[9] Arcana Network, "How Does Decentralized Cloud Storage Work?" *Medium*, 8 September 2021, *https://medium.com/arcana-network-blog/how-does-decentralized-cloud-storage-work-a4f36fe7dddc*

[10] Müller, A.; A. Ludwig; B. Franczyk; "Data Security in Decentralized Cloud Systems—System Comparison, Requirements Analysis and Organizational Levels," *Journal of Cloud Computing*, 28 June 2017, *https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-017-0082-3*

[11] Haritonova, A.; "Decentralized Data Storage: Pros, Cons and Prospects," Pixelplex, 16 August 2021, *https://pixelplex.io/blog/decentralized-storage/*

CROSSWORD PUZZLE

By Myles Mellor
www.themecrosswords.com

1	2	3		4		5		6	7	■	8	9		10
11			■		■		■	12		13	■		■	
14			■	15			■	16						
	■		■		■	17			■		■		■	
18							■	19					20	■
	■	■	■		■	■	21	■	■		■	22		
23		24		■	25			26	■	27				■
■	■		■	28		■	■		■		■	29		30
31									■	32			■	
	■		■		■	■	■	■	■		■	■	■	
33			■	34	35	36		37		■	■	38	39	
	■	■	■	40			■		■	■	■	41		
42		43								44			■	
	■		■		■		■		■		■	45	46	
47				■	48				■	49				

ACROSS

1. What information security companies have to deliver
8. Cyberspace location
11. Managed
12. Set of tools and parts
14. Access requirements, abbr.
15. A lady's
16. Sounded the alarm
17. Can
18. Attempts to breach a company or government system
19. Ignores, with 39 across
22. It crosses a column
23. Conn. University (USA)
25. The C in IAC
27. No longer carry out a function
28. Prefix for operates
29. Apex
31. Put together a system by supplying, arranging or connecting a specific set of internal or external components
32. Unit of sunshine
33. Numbers, abbr.
34. System infiltrator
38. See 19 across
40. Environmental watchdogs, abbr.
41. Try to gain the support of
42. Vital factor that establishes digital trust, 2 words
45. Large spreading tree
47. Make public confidential data
48. Authenticating mark
49. Computer programmers' expertise

DOWN

1. One of the key ISACA® disciplines
2. Atomic energy unit
3. Beginning
4. One of the key elements behind digital trust
5. Contract details
6. Signs off on
7. Zero
9. Honesty
10. Completes
13. Open source infrastructure-as-configuration software tool
20. Acting on one's own
21. Promotion piece
24. Computer connections
25. Machine piece
26. Watch closely
28. Messages in code
30. Delivers a promised product or service
31. The C in COBIT®
35. Mimic slavishly
36. Core group
37. Microsoft Office program
38. Possessed
39. Field Officer, abbr.
43. Hemingway title ending
44. It can be a pillar of digital trust, abbr.
46. __ Mans race

Answers on page 59

Take the quiz online.

https://bit.ly/3VXSCp8

Based on volume 5, 2022—People, Processes and Behaviors
Value—1 Hour of CISA/CRISC/CISM/CGEIT/CDPSE Continuing Professional Education (CPE) Credit

TRUE/FALSE

Pearce Article

1. Model drift occurs when changes in operating environment and models alter the underlying data, rendering the model no longer representational of the environment for which it was designed and tested.

2. Digital native environments are characterized by flexible/connected teaming, significant digital transformation risk, faster decision-making, and the establishment of an innovation department.

Alvero Article

3. In keeping with the importance of culture to short- and long-term organizational success, a survey from The Institute of Internal Auditors (The IIA) reported that 44 percent of audit effort in North America is being allocated to governance and culture.

4. According to the Return on Culture report, employees who consider their organization's culture extremely healthy are more like to remain with the organization for more than six years.

Dziwa Article

5. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAS) continue to excel at preventing robots from making false digital entries and restricting account access to authorized employees. They have proven themselves impervious to social engineering.

6. Typical users care more about technology's convenience than its security, a flawed mindset that is known to and exploited by threat actors.

Donina and Hartzel Article

7. Highmark identified four pillars to address its risk-related objectives, including quantifying risk at all levels and standardizing through RiskOps and The IIA's Three Lines Model.

8. To avoid previous logjams associated with the proliferation of committees and unclear lines of responsibility, Highmark used the RiskOps operating model to appoint a single individual to consistently measure, track and follow up on exceeded thresholds, using centralized monitoring dashboards.

Raphael, Celestin and Djiethieu Article

9. Boolean logic introduced the notion of automatism, which has progressed the computer to more than a calculator.

10. Each color in a colored bit model represents an electron at a specific energy level, which is useful in explaining how new electronic circuits built to simulate Pauli's energy level theory will work.

Ebersbach and Powers Article

11. Top and emerging risk is the most challenging of the risk elements because that type of risk is, by nature, more purely quantitative.

12. The control environment is typically defined by the control effectiveness score, calculated by dividing the number of risk elements by the number of effective controls.

Tomaselli Article

13. While US Sarbanes-Oxley Act of 2002 (SOX) section 302 requires an organization's principal executive and financial officers to establish, maintain, assess and certify the effectiveness of the enterprise's internal controls, it does not prescribe the specific controls or framework for doing so.

14. The US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 is a cybersecurity control framework consisting of more than 1,000 security requirements across 18 domains, assigned low, moderate and high baselines.

Renduchintala, Chowdhary and Sekar Article

15. An (ISC)^2 survey estimated that there are approximately 2.7 million vacant cybersecurity jobs. Most of the survey respondents did not feel that this shortage poses an extreme or moderate risk.

16. Employee retention strategies should invest in skill enhancement/development, employing upskilling programs, a formal mentorship program, and promotion of participation in external security industry forums.

Answers: Crossword by Myles Mellor. See page 58 for the puzzle.

1 P	2 R	3 O	T	4 E	C	5 T	I	6 O	7 N	■	8 S	9 I	T	10 E
11 R	A	N	■	T	■	E	■	12 K	I	13 T	■	N	■	N
14 I	D	S	■	15 H	E	R	■	16 A	L	E	R	T	E	D
V	■	E	■	I	■	17 M	A	Y	■	R	■	E	■	S
18 A	T	T	A	C	K	S	■	19 S	H	R	U	G	20 S	■
C	■	■	■	S	■	■	21 A	■	■	A	■	22 R	O	W
23 Y	A	24 L	E	■	25 C	O	D	26 E	■	27 F	A	I	L	■
■	■	I	■	28 C	O	■	■	Y	■	O	■	29 T	O	30 P
31 C	O	N	F	I	G	U	R	E	■	32 R	A	Y	■	E
O	■	K	■	P	■	■	■	■	■	M	■	■	■	R
33 N	O	S	■	34 H	35 A	36 C	K	37 E	R	■	■	38 O	39 F	F
T	■	■	■	40 E	P	A	■	X	■	■	■	41 W	O	O
42 R	I	43 S	K	R	E	D	U	C	T	44 I	O	N	■	R
O	■	E	■	S	■	R	■	E	■	A	■	45 E	46 L	M
47 L	E	A	K	■	48 S	E	A	L	■	49 C	O	D	E	S

ADVERTISERS/WEBSITES

AuditBoard	*https://www.auditboard.com/*	Back Cover

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 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 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

Leaders and Supporters

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/3w1MTnd

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®

FEATURED RESOURCES

CDPSE Review Manual

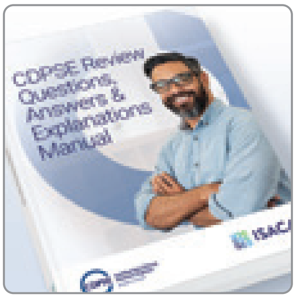
Print Product – Member Price $109/Non-member Price $139
eBook – Member Price $109/Non-member Price $139
Also available in Chinese, German and Spanish

The *CDPSE Review Manual* is a comprehensive reference guide designed to help individuals prepare for the CDPSE exam and understand technical privacy implementation and privacy principles. The manual represents the most current, comprehensive, peer-reviewed IT-related privacy review resource available.

The manual is organized to assist candidates in understanding essential concepts that can facilitate a common understanding of privacy best practices and ensure the proper integration of IT privacy solutions that mitigate risk while ensuring an optimal end-user experience. The exam and the manual are organized within three high-level domains.

- Privacy Governance
- Privacy Architecture
- Data Life Cycle

These domains are the result of extensive research and feedback from IT privacy subject matter experts from around the world. This manual, along with other training and review options, will help candidates prepare to take the CDPSE exam and provides a practical privacy desk reference for future use.



CDPSE Questions, Answers and Explanations Manual

Print Product – Member Price: $72/Non-member Price $96
Also available in Chinese, German and Spanish

The *CDPSE Questions, Answers & Explanations Manual* is designed to familiarize candidates with the question types and topics featured in the CDPSE exam.

The manual consists of 300 practice items covering the three domains (Privacy Governance, Privacy Architecture and Data Life Cycle) that are tested on the CDPSE exam.

These questions are not actual exam items but are intended to provide CDPSE candidates with an understanding of the type and structure of questions and content that has previously appeared on the exam. This publication is ideal to use in conjunction with the *CDPSE Review Manual.*

CDPSE Questions, Answers & Explanations Database

Online Database – Member Price $299/Non-member Price $399

CDPSE Questions, Answers & Explanations Database—12 Month Subscription is a comprehensive 300-question pool of items that contains the questions from the CDPSE Questions, Answers & Explanations Manual. The database is available via ISACA PERFORM, a web-based learning platform, allowing CDPSE candidates to log in at home, at work or anywhere they have Internet connectivity. Exam candidates can utilize an interactive planner to build a custom study plan, and a personalized dashboard serves as the primary method to navigate studies and track progress. Candidates will be presented with randomly selected practice question sets and be able to view the results by job practice domain, allowing for concentrated study in particular areas. Each question and answer set includes in-depth explanations for each answer choice, allowing the learner to fully understand the rationale behind each correct—and incorrect—answer choice.

Learners will have the ability to review previously answered questions, allowing CDPSE candidates to identify their strengths and weaknesses and focus their study efforts accordingly. Other features of the database include:

- The ability to select practice question sets by specific domain and sub-category and choose the length of study sessions, giving learners the ability to customize their approach to fit their needs
- Two full-length timed practice exams intended to mimic the blueprint and feel of an actual ISACA exam and help candidates manage their time when answering questions
- Flashcards and interactive games to help reinforce key terms and concepts

Order online at www.isaca.org/resources

5G Privacy: Addressing Risk and Threats White Paper

Free Digital Resource

This paper reviews 5G network architecture and examines the privacy features of this technology. This examination includes a high-level review of the 5G architecture and discussion of existing and emerging privacy threats. This paper introduces new 5G privacy features that mitigate both existing threats associated with 4G and previous generation cellular networks as well as emerging privacy threats around the 5G network itself. Lastly, it highlights existing 5G privacy threats that still need to be addressed.

2022 CPE on Demand: Variety Pack

Online Course – Member Price $1,050/Non-member Price $1,155

The 2022 CPE on Demand: Variety Collection provides timely, valuable insights for IT Audit, Security, and Risk professionals, and enables you to learn on your schedule while earning up to 21 ISACA CPEs. Access to the entire collection of recordings - each recorded at **ISACA Conference North America 2022** - is available for a 90-day period and includes downloadable presentation decks.

Session titles include:

- Quantum Threat Defense: Starts Now
- How to Centrally Manage Segregation of Duties Across Multiple Systems
- Supply Chain Regulation Is Coming: Are You Ready?
- Why Most KPIs Drive Internal Audit in the Wrong Direction
- Reporting Cybersecurity Risk to Directors and Senior Executives
- Audit and Compliance: Trends in Segregation of Duties Across Multiple Systems and User Access Management
- Architecture, Infrastructure and Operations: Lessons Learned from the FFIEC's New Booklet
- Preparing for War" - Defending Against Nation State Attackers and Political Cyber Retaliation
- Remote Browser Isolation – The key to eliminating ransomware and phishing
- The CISOs Role in Driving Trust: Why it Matters, How to Define it, and What Success Looks Like
- It's All About the Data: Governance, Protection and Audit in a Transformed Data Environment
- A Whole Lotta BS (Behavioral Science) About Cybersecurity
- What We Got Wrong in the Cloud: Eight Common Cloud Migration Failures
- Making Zero Trust a Reality - The why, what and how!
- True Enterprise Security and the Role Auditors Must Play
- Keeping Pace: How IT Governance can Support Innovation in the Digital Age
- How to Get Engineering to Care About Audit & Compliance - Stories from an Instacart's Compliance Leader
- Mastering Investigation in Modern Cloud Environments
- Analyst View: A Data-Driven Insider's Guide To Accelerating CyberSec/Risk/Privacy Governance Careers
- The growing problem of exposed secrets, uncovering 6 million credentials in 2021
- Are you a Good Witch Machine? Or a Bad Witch Machine? – Welcome to the Machine Identity World

Learners will have access to the course for three months from date of purchase and will earn 21 CPE upon completion. This course has a seat time of approximately 21 hours.

Identity and Access Management Audit Program

Free Digital Member Resource/Non-member Price $49

The security protocols associated with Identity Management and Access Management (IAM) address the provisioning of appropriate levels of access to the right users or devices. An increase in the number of applications and a shift toward an Internet-based perimeter have driven even more emphasis on IAM. ISACA's Identify and Access Management Audit Program provides IT auditors with a tool that lends assurance around the effectiveness of this critical operational.

-The audit program addresses the following: governance; identity management; authentication; authorization; access control; and monitoring. The controls, control objectives and testing in these areas position the Identity and Access Management Audit Program to facilitate auditors' assessment of the IAM control environment.

Risk Scenarios Toolkit White Paper

Digital Resource – Member Price $49/Non-member Price $79

Risk scenarios facilitate communication in risk management by constructing a narrative that can inspire people to act. The use of risk scenarios can enhance the risk management effort by helping the risk team understand and explain risk to business process owners and other stakeholders. Additionally, a well-developed scenario provides a realistic and practical view of risk that is more aligned with business objectives, historical events and emerging threats forecasted by the organization than would be found by consulting a broadly applicable standard or catalog of controls. These benefits make risk scenarios valuable as a means of gathering and framing information used in subsequent steps in the risk management process.

This toolkit includes 87 risk scenarios and a detailed guide to help navigate through a risk scenario.

How to Build a Risk Scenario Online Course

Online Course – Member Price $49/Non-member Price $79

One of the challenges for information and technology (I&T) risk management is to identify important and relevant risk. The use of risk scenarios can enhance the risk management effort by assisting the risk teams understanding and explain risk to the business stakeholders. Additionally, a well-developed scenario provides a realistic and practical view of risk that is more aligned with business objectives, historical events, and emerging threats.

ISACA has developed a brief course that will help break down each aspect of a risk scenario. By the end of this course, you'll be able to:

- Define IT risk scenario.
- Describe the benefits of using an IT risk scenario.
- Summarize the structure of an IT risk scenario.
- Explain the key points for developing an IT risk scenario.
- Explain the importance of the risk scenario technique.
- Examine the role of a risk register in a risk scenario.
- List the four major risk responses.
- Define and describe the importance of risk assessment and risk factors.

Demystifying Linux White Paper

Free Digital Resource

This paper explores what Linux is, how it works, and how practitioners can use it to their advantage. For those who are new to Linux, this paper's intent is to provide a very basic overview of what Linux is, how it came to be, and how it can be used in your day-to-day activities. Note that the paper will be staying at a very high level throughout this discussion—this is by design with the intent that practitioners can explore Linux more deeply using other ISACA's performance-based training (PBT) resources and in other venues.

ISACA
The Great Resignation: Business Challenges and Sustainable Solutions

The Great Resignation: Business Challenges and Sustainable Solutions White Paper

Free Digital Resource

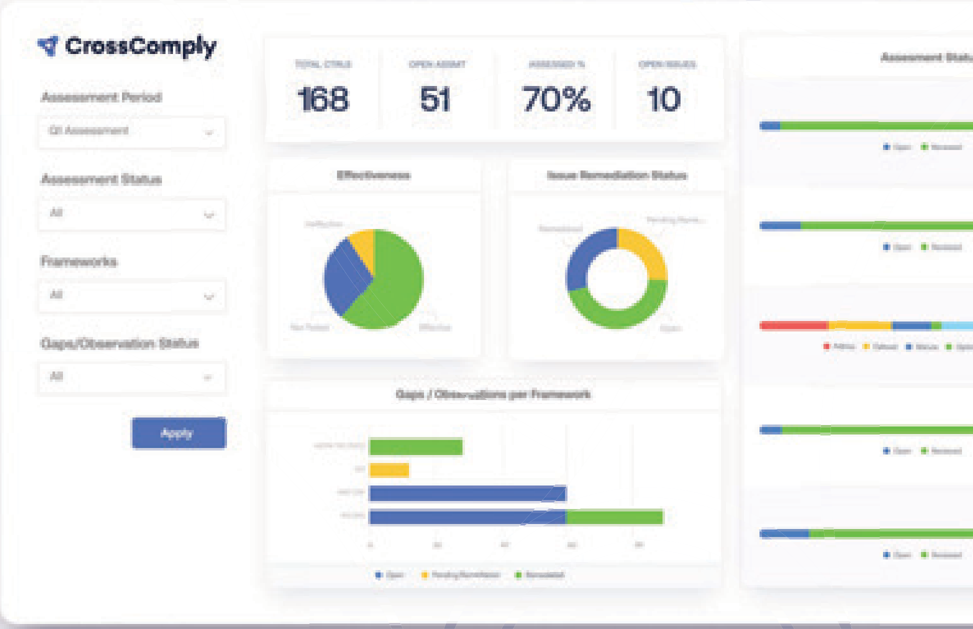
Recent workforce studies across the world highlight a considerable shift in employees' attitudes towards work exacerbated by the COVID-19 pandemic. In the United States, 47.4 million employees voluntarily left their jobs in 2021.[1] Coined the Great Resignation, this economic trend is challenging IT and business to develop a sustainable workforce-management solution. This whitepaper describes the reasons for the Great Resignation and the difficulties it creates for enterprises. Read this white paper to learn what industry leaders who have experience pivoting their mindsets and leadership to successfully navigate business disruptions have to say about this current challenge that enterprises are facing. You can use their recommendations to develop a sustainable and multipurpose workforce-management solution that does not rely on compensation as the main motivator to retain talent.

Order online at www.isaca.org/resources

Security Compliance, Accelerated.

Simplify and scale your compliance program with a platform that unifies SOC 2, ISO 2700x, NIST, CMMC, PCI DSS, and more across your organization.

- Assess Once, Comply With Many
- Automate Evidence Collection
- Get Real-Time Insights



Assessment Period: Q1 Assessment
Assessment Status: All
Frameworks: All
Gaps/Observation Status: All

- **Scale Quickly**
  Automatically map new frameworks to your controls with a Unified Compliance Framework® common control set.

- **Reduce Duplicative Work**
  Leverage the common controls crosswalk to visualize the overlap across frameworks and avoid audit fatigue.

- **Eliminate Manual Evidence Collection**
  Connect directly with your source systems to obtain the needed information and consolidate requests.

- **Track Issues in Real Time**
  Get visibility into identified issues, gaps, vulnerabilities, and action plans with dashboards and powerful reporting tools.

Top-Rated by Customers

Gartner peerinsights ★★★★★

g2.com ★★★★½

Capterra ★★★★½

Visit **auditboard.com/product/compliance-control** to learn more.

AUDITBOARD