STATE OF DIGITAL TRUST

2023

An ISACA Global Research Report

ISACA

Contents

Abstract

Digital trust can make or break an organization. It is fundamental to all enterprises and is a critical factor in the ability to innovate, expand and be resilient in a turbulent, highly connected global marketplace. Digital trust brings together many of the disciplines already vital to an organization—security, risk, privacy, quality, compliance, communications, information technology, marketing and operations. All these areas have a significant and direct impact on how others perceive an organization, especially its brand and reputation, and are integral to adding value to the organization and its future digital transformation initiatives.

To gain insights into global approaches and perceptions about digital trust, ISACA® conducted the State of Digital Trust 2023 survey in the first quarter of 2023. It is the second annual administration of this survey and contains both year-over-year and new data exploring areas such as familiarity, priority, confidence, maturity, obstacles and responsibility related to digital trust across the globe. In addition to survey data insights, the report also includes practical guidance and perspectives from industry professionals. It concludes with five key takeaways to help organizations strengthen digital trust as they move forward with digital transformation.

Executive Summary

Nearly everyone has received a phone call or message that their account has suspicious activity, someone is trying to open a credit card or apply for a loan in their name or a company that has their personal information has been hacked. Unfortunately, these increasingly common incidents demonstrate social engineering's ability to prey on people. Consumers are already dealing with the fatigue of seemingly never-ending end-user license agreements and other digital circumstances they cannot fully understand. They are tired of their web activity being aggregated and sold to others just to be incessantly marketed to across their apps and browsers. In our rapidly evolving regulatory landscape, these patterns call such market trends and marketing misalignments into question, as compromised pieces of information allow phishing, smishing and vishing attempts to become more realistic.

As a result, new and long-time customers, clients, vendors, employees, regulators, influencers and others start to mistrust organizations.

These challenges can lead to damaging and time-consuming problems, ranging from annoying to catastrophic, for both private- and public-sector organizations. They can result in disruption of services, education shutdown, inability to process payments, exposure of records, loss of customers, weakened market position, stock price declines, regulatory fines and sanctions, bond downgrades, shareholder unrest, disgruntled employees and high costs of remediation, among others.

When these problems occur, some companies suffer extensive financial and reputational fallout, while others weather the storm and retain, or even improve, their reputation and market position.

The difference between the two outcomes is how well an organization navigates digital trust. Trust is an essential component that must be addressed long before the customer relationship begins and must remain a top priority at all times. As face-to-face transactions become less common, the digital ecosystem is now the primary arena for conducting business. Customers want to know why they

KEY FACTORS THAT CONTRIBUTE TO DIGITAL TRUST INCLUDE:

- **Quality:** Assure products and services meet or exceed expectations.
- **Availability:** Enable access to information and services in a timely manner.
- **Security and privacy:** Ensure all data are protected and kept confidential.
- **Ethics and integrity:** Live up to all promises.
- **Transparency and honesty:** Be truthful in how information is used and if it is compromised.
- **Resiliency:** Take steps to ensure organizational stability and agility.

should trust an organization, and enterprises need to earn that trust with every interaction and transaction.

Results from the State of Digital Trust 2023 survey build upon and reinforce what was uncovered in the first report, conducted in 2022. Now that the survey is in its second year, it is interesting to see that many of the data-driven insights remain aligned with what was found previously and that trends can be tracked year over year.

Digital trust is a broad topic that goes beyond compliance. It involves treating siloed areas of an organization as part of a cohesive whole. Nearly all organizations are undergoing some level of digital transformation, so this is an ideal time to understand enterprise motivation and what is and is not working.

Woven throughout the survey's global responses is the knowledge that one of the most important initiatives with the biggest impact is also one with possibly the least budget outlay—digital trust.

Digital trust helps organizations ensure that everything they do contributes to others having trust in them—in good times and bad. This concept does not require significant new budget allocations or a new C-Suite position. It does recommend an umbrella approach over existing functions to ensure digital trust remains a cohesive focus in all areas.

What Is Digital Trust and Why Is It Important?

Every interaction with a company is unique. It may involve financial, demographic, personal or product information, but all transactions require that the parties establish and maintain trust with each other.

Customers, employees, suppliers and other stakeholders need to know that their online relationships with an organization are reliable and trustworthy. The tolerance for any breach of digital trust is near zero.[1]

GREG WITTE, *Senior Security Engineer at Huntington Ingalls Industries*

When transactions were mostly conducted in person, many felt that trust was built through eye contact, handshakes and physical signatures. At one time, these were enough, but with online shopping revenue in the U.S. expected to exceed US$1.7 trillion by 2027[2] and 51 percent of hybrid employees saying they are considering transitioning to fully remote employment in the year ahead,[3] digital-first work and transactions have become the normal way of conducting business.

Digital trust brings together many of the disciplines already critical to an organization, including compliance, security, privacy, communications, information technology, marketing and operations. Alignment should exist between these areas because all have a significant, direct impact on how others perceive the organization—especially its brand and reputation—and are integral to adding value to the organization itself and its future digital transformation initiatives.

Digital trust can make or break an organization. It is fundamental to all enterprises and critical in their ability to innovate, expand and be resilient in a turbulent, highly connected global marketplace.

1 Witte, G.; Your Top Digital Trust Questions Answered, ISACA, USA, https://www.isaca.org/resources/ebook/your-top-digital-trust-questions-answered

2 Statista.com, "Retail e-commerce revenue in the United States from 2017 to 2027, November 2022, https://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/

3 Microsoft, "2022 Work Trend Index: Annual Report," 16 March 2022, https://www.microsoft.com/en-us/worklab/work-trend-index/great-expectations-making-hybrid-work-work

STEPS THAT LEAD TO A TRUSTED DIGITAL RELATIONSHIP

Informed consumers often go through steps (also known as the digital trust hierarchy) on their journey to digital trust with a company, asking themselves:

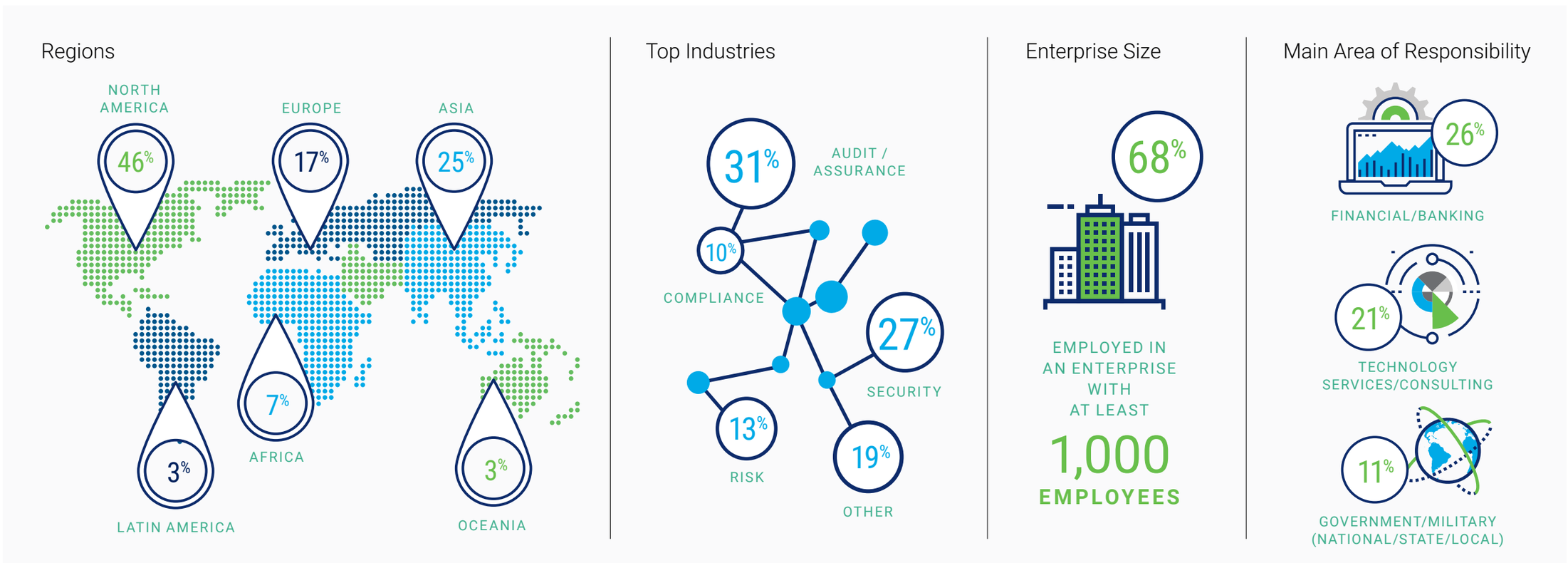
Do I trust the company enough to:

- Receive and open emails from it?
- Accept cookies from its website, thus beginning to trade privacy for convenience?
- Provide personal information to the company via its website?
- Download its mobile app?
- Pay it money, digitally, in exchange for a product or service, thus giving it access to credit card, online payment platform or other financial information?
- Embark on an ongoing, mutually beneficial relationship with it?
- Continue to work with—and trust it—even after it has been hacked or experienced a negative event?

Survey Methodology

To gain insights and gather data for the State of Digital Trust 2023 report, in January 2023, ISACA sent an online survey to approximately 131,000 individuals who are members of ISACA or who have earned one of ISACA's certifications or credentials (e.g., CISA®, CISM®, CRISC®, CGEIT®, CDPSE™ and CSX-P™). Responses were collected anonymously. A total of 8,185 respondents completed the survey, with a margin of error of +/- 1 point. Response rates varied by question. The survey used multiple-choice and Likert-scale formats. The demographic information is shown in **figure 1**.

FIGURE 1 – Survey Demographic Information



Survey Results and Insights

Digital trust as a cohesive approach is still emerging as a mainstream initiative among boards of directors, executives and professionals. For the past few years, it has been addressed in high-level discussions as a nice-to-have but it has ambiguous and difficult-to-achieve aspiration. Recent business challenges, including new technology, a dynamic regulatory landscape and worldwide shifts in labor force and consumer habits—along with the growing frustration of consumers, professionals and government officials over repeated breaches of trust—have spurred businesses to move digital trust into the realm of a must-have.

Recognizing this need, ISACA has taken steps to define digital trust in clear business language and work in partnership with leading experts to develop distinct, customizable guidance based on well-defined and executed research.

Familiarity With Digital Trust

Currently, digital trust as a concept has more recognition than digital trust as a term. Only 33 percent of survey respondents were extremely or very familiar with digital trust as a term prior to being shown ISACA's definition (see p. 9). After hearing the definition, recognition of the term digital trust jumped to 55 percent.

From a regional perspective, prior to being exposed to the definition, respondents from Africa (42 percent) were more familiar with the term digital trust than those from Europe (35 percent), Asia (32 percent) and North America (31 percent). Those in India (47 percent) were more familiar than those from the other largest countries represented in the sample: Canada (35 percent), the UK (33 percent), the US (31 percent) and Japan (13 percent).

After learning of ISACA's definition of digital trust, Africa (68 percent) remains more familiar with the term than Oceania (60 percent), Europe (56 percent), North America (54 percent) and Asia (51 percent).

Across industries, familiarity prior to learning the definition was the same among financial/banking (31 percent) and government/military (31 percent) professionals. Those in technology services/consulting (40 percent) were slightly more familiar. After learning the definition, numbers rose across the board with financial/banking (56 percent), government/military (54 percent) and technology services/consulting (60 percent) professionals.

This indicates that people are aware of the concept and underscores the need for greater exposure to a globally accepted definition. Having an agreed-on definition helps reduce confusion and supports common understanding. It is especially important as organizations around the world continue to move forward with accelerating digital transformation initiatives—61 percent believe that digital trust, as described in the ISACA survey, can be achieved in their organizations.

Importance and Prioritization of Digital Trust

While 84 percent of respondents feel that digital trust is extremely/very important to organizations today, and 75 percent feel it is relevant to their organization, fewer (64 percent) say their organization prioritizes digital trust corresponding to its level of importance. Interestingly, 91 percent of those currently measuring digital trust maturity feel digital trust is extremely/very important to their organization.

When asked if their organization currently prioritizes digital trust corresponding to its level of importance, respondents from North America (66 percent), Asia (65 percent) and Africa (65 percent) were similarly aligned than those from Europe (57 percent). The same question found that those in India (75 percent) are much more likely to prioritize digital trust than other regions.

More than three-quarters (76 percent) agree that digital trust is extremely or very important to digital transformation. As nearly all organizations are planning on increasing their pace of digital transformation, this is a positive sign that businesses clearly understand that these two concepts need to proceed in unison.

DIGITAL TRUST DEFINED

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.

SOURCE: ISACA

Many (82 percent) feel that in five years, digital trust will be more or much more important in their organization than it is today. Still, only 24 percent are planning to increase budgets for digital trust-related areas in the next year. This is understandable, as many digital trust initiatives are focused on breaking down barriers among established siloed areas and creating a cohesive lens, or umbrella, that ensures all areas are working together and the organization has a solid foundation of digital trust.

DIGITAL TRUST SCORING

Developing an independent, publicly available digital trust score for organizations is important. Global professionals across many organizations have been discussing the subject for a long time. This scale can serve as a valuable tool to hold organizations accountable for their actions, but it needs to have globally consistent review standards and scope, as well as an automated measurement mechanism. For example, a highly rated organization may have a serious negative incident that requires its score to drop several points in a matter of minutes. Assessment and review parameters have to be active in real time.

MARK THOMAS, *Escoute Consulting*

From a regional perspective, Africa (94 percent) shows the highest level of agreement that digital trust is important to organizations, closely followed by Oceania (91 percent). This is statistically significant over Latin America (86 percent), North America (84 percent), Asia (82 percent) and Europe (82 percent). Respondents in India (90 percent) rate digital trust as extremely/very important, which is higher than the other largest countries in the sample—Canada (85 percent), the UK (85 percent), the US (84 percent) and Japan (68 percent).

From an industry viewpoint, there is also a high level of importance attributed to digital trust among professionals in financial/banking (86 percent), government/military (84 percent) and technology services/consulting (84 percent).

When considering scoring, 70 percent indicate it is extremely/very important for their organization to be independently graded on digital trust practices with results made publicly available. In addition, 81 percent agree that organizations that can demonstrate their commitment to digital trust (e.g., with a high score or rating from an independent third-party assessment) will ultimately be more successful. This increases to 89 percent among those who currently measure digital trust maturity.

Why do some organizations recover and maintain loyalty after one, or even multiple, incidents that severely impact digital trust? For many, it relates directly to the company's actions and transparent communications before, during and after an incident. People tend to understand and forgive a company if they feel it took precautions and treated their information carefully. The same people may also become frustrated and less forgiving when they perceive carelessness, lack of attention and lack of communication.

Why do some organizations recover and maintain loyalty after one, or even multiple, incidents that severely impact digital trust? For many, it relates directly to the company's actions and transparent communications before, during and after an incident. People tend to understand and forgive a company if they feel it took precautions and treated their information carefully. The same people may also become frustrated and less forgiving when they perceive carelessness, lack of attention and lack of communication.

Questions to ask when determining why some companies fare better than others after an incident or attack that erodes digital trust include:

- Did the company have safety, security, privacy and related policies in place and were they followed?
- Did the company voluntarily disclose the incident and provide updates in a timely manner?
- Did the company provide remediations/solutions/compensation for customer losses?
- Does the company provide ongoing value and innovation to meet customer needs?

Survey respondents did identify certain trust-related benefits (**figure 2**) and consequences for not having a strong digital trust posture (**figure 3**).

The responses were similar to the ISACA *State of Digital Trust 2022* report, with a few benefits changing places in 2023. Positive reputation was the highest-ranked benefit in both years, but more reliable data ranked slightly ahead of fewer privacy breaches and fewer cybersecurity incidents in 2023.

FIGURE 2 – Digital Trust-related Benefits

Respondents report that high levels of digital trust can lead to the following benefits.

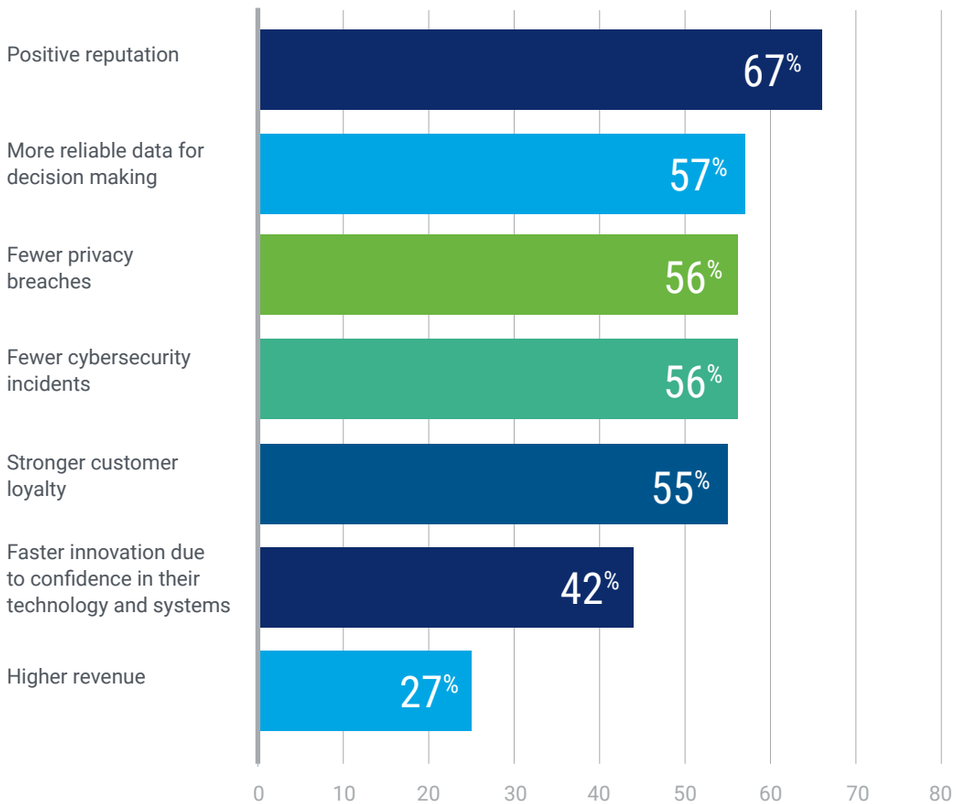
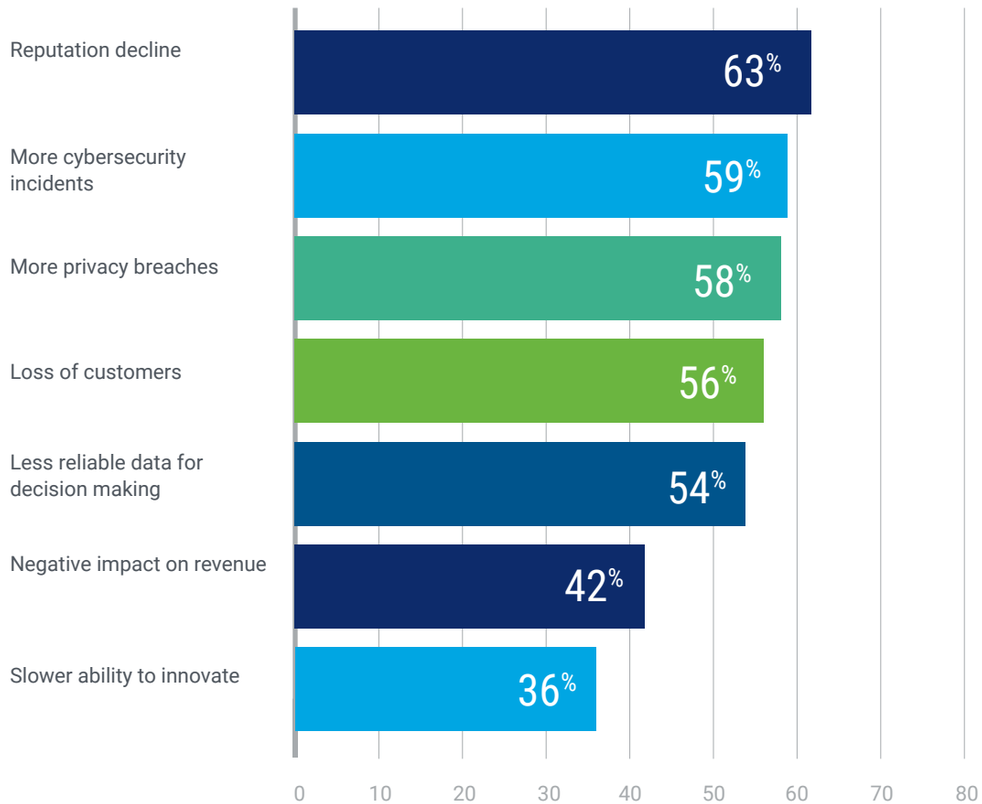


FIGURE 3 – Consequences of a Lack of Digital Trust

Respondents say organizations with a low level of digital trust often experience the following consequences.



The 2023 responses for the consequences of a lack of digital trust were similar to the 2022 report, with the only change that more privacy breaches ranked slightly higher than more cybersecurity incidents last year.

Confidence and Maturity Related to Digital Trust

More than half (53 percent) of respondents are completely or very confident in the digital trustworthiness of their organization (**figure 4**). Among those that already measure digital trust maturity, this confidence jumps to 81 percent.

From a regional perspective, Latin America (65 percent) has greater confidence in the digital trustworthiness of its organizations compared to all other regions: Africa (54 percent), North America (54 percent), Asia (53 percent), Europe (50 percent) and Oceania (43 percent).

Professionals' level of confidence in the digital trustworthiness of their organization varies by the industry: technology services/consulting (61 percent), financial/banking (59 percent) and government/military (44 percent).

Measurement of maturity is considered a standard business practice, but fewer than one in four respondents (24 percent) indicate their organization currently measures the maturity of its digital trust practices, even though 67 percent feel it is extremely or very important. Clearly, leadership is a driver of this, as among those that measure digital trust, 55 percent have a board of directors that prioritizes digital trust, and 59 percent use a digital trust framework. These figures are in line with the findings from the ISACA *State of Digital Trust 2022* report.

Respondents in Asia (28 percent) reported the highest level of digital trust measurement, with other areas following closely: Africa (26 percent), North America (23 percent), Oceania (21 percent) and Europe (19 percent). Those in India (40 percent) are overall more likely to say that their organization measures digital trust.

FIGURE 4 – Digital Trustworthiness of Organizations

How confident are you in the digital trustworthiness of your organization?

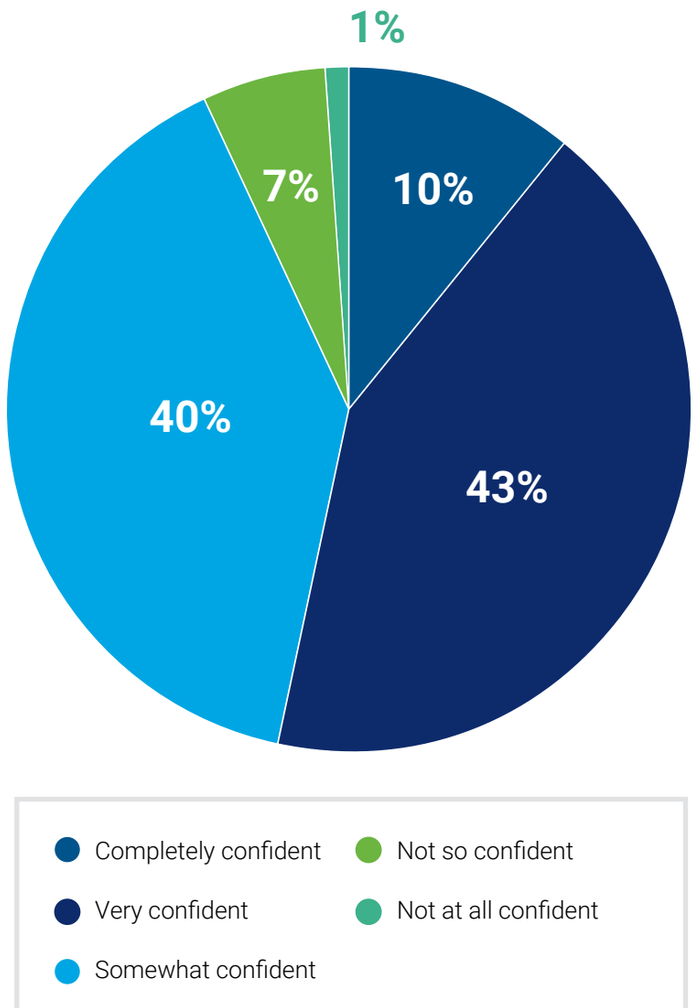


Figure 5 shows the common methods used to measure digital trust with customers, and **figure 6** shows methods used to measure digital trust within an enterprise.

FIGURE 5 – Popular Methods for Measuring Digital Trust

Ways digital trust is measured among customers

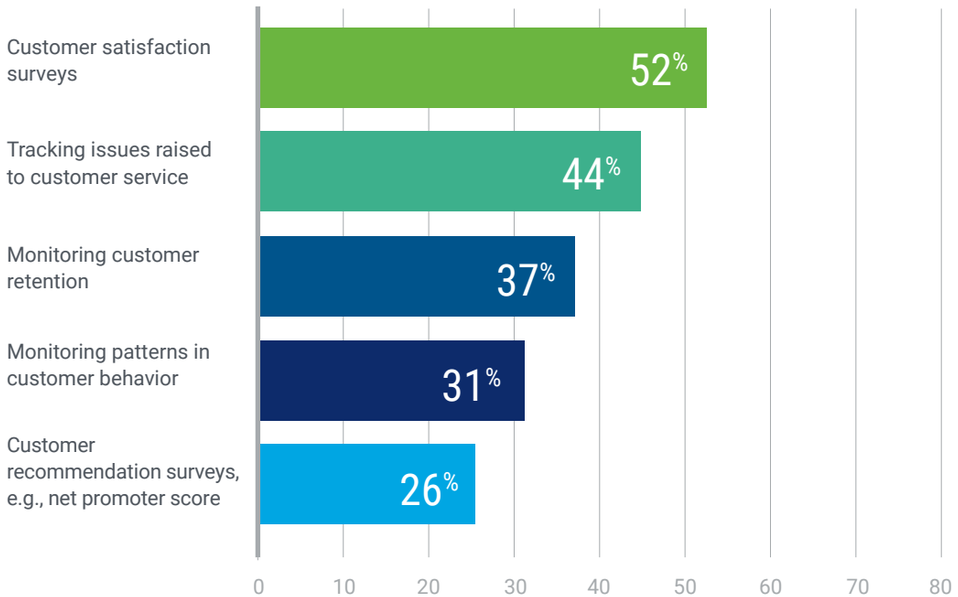
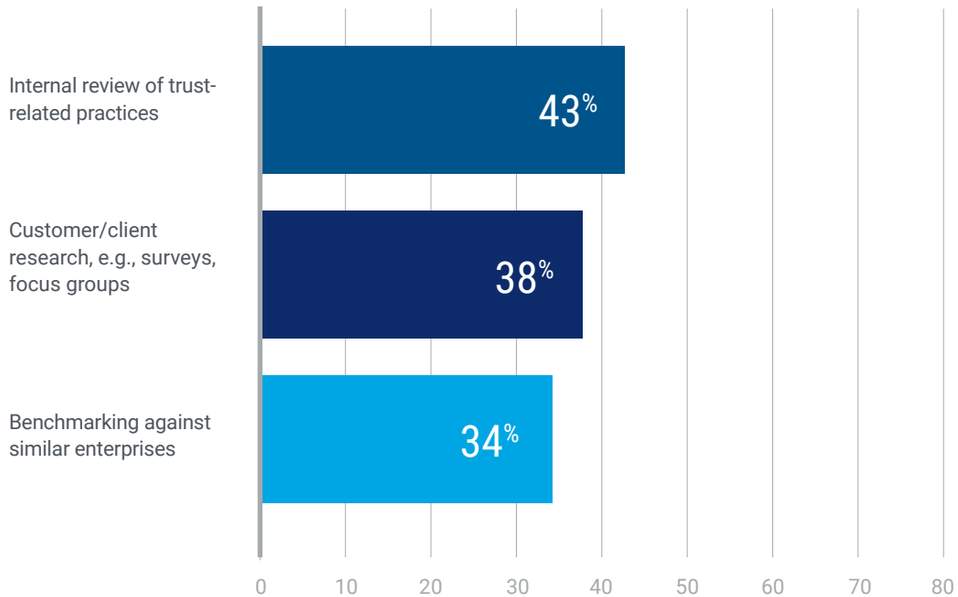


FIGURE 6 – How Digital Trust is Measured in Organizations

Ways digital trust is measured within the organization

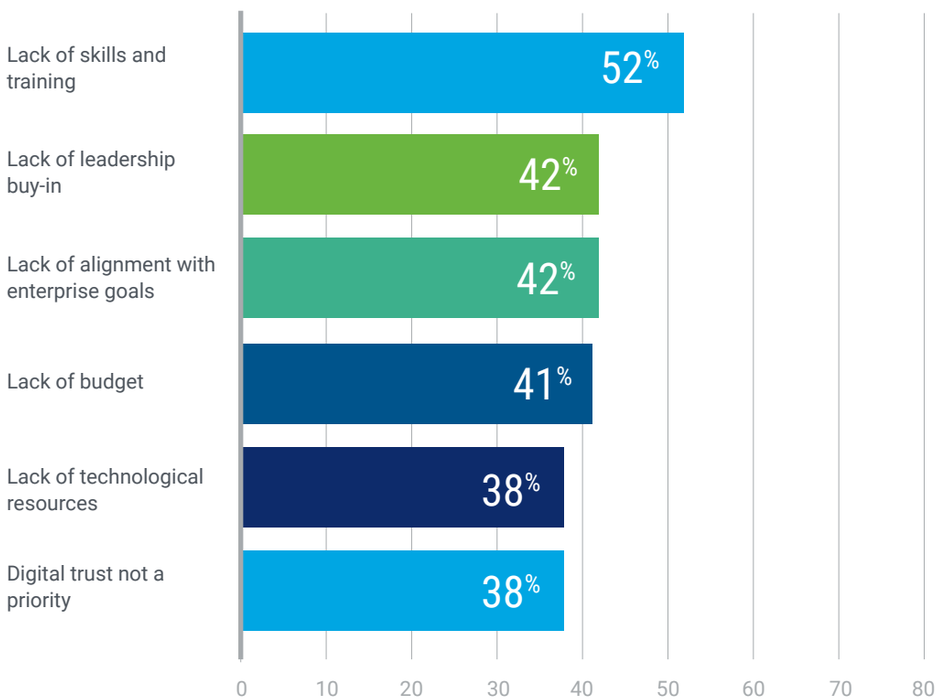


Despite the proven importance of measurement, 29 percent say that they do not measure digital trust within their organization at all. On the positive side, this is a slight improvement from the 2022 survey, which found that 33 percent of respondents did not measure digital trust.

Obstacles to Attaining Digital Trust

For every move forward, organizations face their own set of obstacles. One of the first steps toward business improvement is to find out what is hindering success and then outline a path to address or overcome these challenges. **Figure 7** provides a view into what respondents are experiencing as top obstacles to achieving digital trust in their organizations.

FIGURE 7 – Obstacles for Attaining Digital Trust



On a regional basis, overall, Africa reports more obstacles to overcome than other regions. It has the highest incidence in the categories of lack of skills and training, lack of leadership buy-in, lack of alignment with enterprise goals and digital trust not being a priority. Respondents from Oceania rank highest for noting the lack of budget.

The top obstacle reported by industry was lack of skills and training: financial/banking professionals (53 percent), government/military (54 percent) and technology services/consulting (48 percent).

When comparing responses year-over-year, there has been a positive increase related to the lack of skills and training obstacle, indicating an increased understanding and value of the benefits of digital trust.

- **In 2022**, only 29 percent said that their organization offered digital trust training to staff, and only 28 percent said they completely understand how their role impacts digital trust, even though 63 percent said digital trust is extremely or very relevant to their job.
- **In 2023**, 32 percent say that their organization offers digital trust training to staff, and 31 percent indicate they completely understand how their role impacts digital trust. In addition, 66 percent now say that digital trust is extremely or very relevant to their job today.

Responsibility for Digital Trust

Determining where day-to-day accountability resides for digital trust varies among organizations. There is currently no single job title or role focusing on digital trust that is appropriate for every organization—each has its own culture, structure and goals. **Figure 8** shows the top three roles that play a critical role in strengthening digital trust.

As part of their fiduciary duty to the organization, the board of directors and executive leadership clearly need to have ultimate responsibility for something as impactful and far reaching as digital trust. Yet, only 19 percent globally say that their board of directors has prioritized digital trust, and approximately one-third (34 percent) say that the senior leadership team is ultimately responsible for digital trust in the organization.

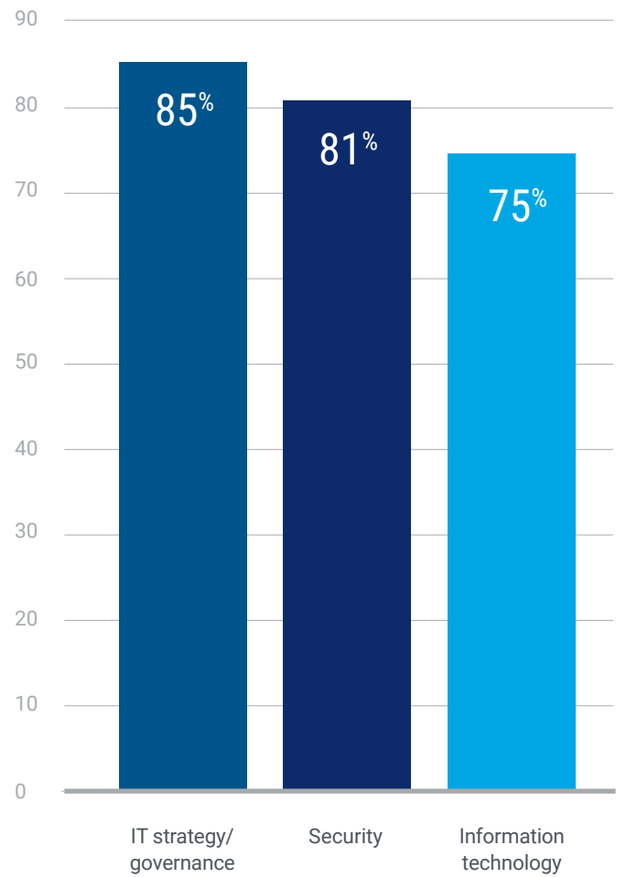
From a regional perspective, respondents from North America say senior leadership is responsible for digital trust, while other regions more often say that the board of directors is responsible. Respondents in India were more likely than those in other countries to say that individual employees are responsible for digital trust.

Professionals in financial/banking (34 percent) indicate the board of directors is most responsible, while professionals in technology services/consulting (34 percent) and government/military (41 percent) are more likely to say that the senior leadership team is responsible.

Although the position of Chief Digital Trust Officer (or similar) does exist at some forward-thinking organizations, at this time, many organizations do not have an appetite for creating this role. Only 13 percent say their organization has a staff role dedicated to digital trust. Among those that measure digital trust maturity, however, the number jumps to 38 percent that have a dedicated staff role. When the board of directors prioritizes digital trust, the number of those with a dedicated staff role increases to 46 percent.

Digital trust encompasses nearly all aspects of an organization. As it matures, it is more likely that the responsibility will reside with a leader who can approach digital trust as an umbrella that covers multiple areas, such as compliance, security, privacy, communications, information technology, marketing/branding and operations. This leader will need to be someone who knows each of

FIGURE 8 –
Top Three Roles Responsible for Digital Trust



Saying that digital trust is part of everybody's job is different than saying everybody is responsible for it. Someone needs to have accountability for digital trust, and this responsibility should be entrusted to a leader who has the skills to communicate with boards and executive leadership effectively, the knowledge to manage the many moving parts and the ability to motivate employees to excel in the daily activities that build and maintain digital trust.

MARK THOMAS, *Escoute Consulting*

these disciplines (and how they fit together) and contributes to a comprehensive approach toward digital trust.

These skills are especially critical, as only half (51 percent) agree that there is sufficient collaboration in their organization among professionals who work in diverse digital trust fields such as security, risk, governance, assurance, privacy and quality.

Digital Trust and Digital Transformation Tools and Frameworks

Digital transformation continues to progress and mature in nearly all sectors around the world. In recent years, the pace has increased dramatically as pressure from stakeholders and peers has intensified.

As organizations further commit to digital transformation—and implement innovative, digitally enabled services and processes—they must take equal time to understand the new vulnerabilities they are creating. This is similar to laying down a set of railroad tracks that need to operate side-by-side; they must deliver on ambitious goals and, at the same time, ensure digital transformation-related policies and procedures are in place.

When asked how important digital trust is to digital transformation, Africa (91 percent) and Latin America (86 percent) responded significantly stronger than Oceania (78 percent), Asia (77 percent), Europe (76 percent) and North America (73 percent).

This is where digital trust guidance will have a significant impact. Only 20 percent currently use a framework for their digital trust practices, even though 56 percent believe that it is extremely/very important for an organization to have this framework. Among those that do use a framework, COBIT® (27 percent) is the most popular, followed by the SAFE Identity Trust Framework (10 percent).

Asia (24 percent), Africa (24 percent) and Latin America (22 percent) report using a framework for digital trust more than respondents from North America (19 percent), Oceania (16 percent) and Europe (13 percent).

Respondents in India (34 percent) are more likely to have a framework and find it extremely/very important to have one in place (76 percent). India (85 percent) also had the strongest response among the top five countries when asked how important digital trust is to digital transformation.

ISACA's Position in the Digital Trust Space

Organizations and their employees need to be as prepared as possible for known issues as well as the unknown and unexpected attacks and incidents awaiting them in the future—basically, the things that keep many executives up at night. This is particularly important in the fast-moving arena of digital trust.

ISACA helps address these needs through the development of industry-leading tools, credentials, education and training. Respondents say that ISACA enables them to stay current with industry trends (84 percent) and be successful in their chosen profession (80 percent) and provides opportunities for them to be recognized as a thought leader (75 percent).

The rapid growth and challenges in the digital ecosystem mean that ISACA also needs to provide timely and effective guidance regarding digital trust. In this defined area, respondents say that ISACA is an emerging key player in digital trust (68 percent), has the tools and resources available for IT professionals to successfully deliver digital trust (66 percent), is a recognized leader in digital trust (66 percent) and offers a recognized credentialing program in digital trust (57 percent).

In its quest to inspire knowledge and confidence that enables innovation, ISACA's global community of skilled professionals volunteer their time to develop guidance and tools that will help others address current and future challenges. Among its work, ISACA is developing a new digital trust ecosystem framework to help organizations ensure that their digital trust initiatives are in line with their unique mission, vision, values, goals and objectives. The framework will help organizations focus on their individual goals as they build a structure that supports trust, agility and resilience.

Strengthening Digital Trust

While each organization has its own unique goals, strategies and culture, there are many ways to become better positioned for the future. Three steps that organizational leaders can take to ensure they are strengthening, focusing on and delivering the highest level of digital trust are:

1 ASK THE RIGHT QUESTIONS.

Business leaders should be sure they are asking the right questions. For example: Does my organization understand all the trust factors that go into what our customers and stakeholders expect? Are we as focused on process, culture and human factors as we are on the product or service? Do we really understand all the expectations and how we will measure whether we meet them? Do all employees receive training on digital trust? Do our customers know how to identify potentially fraudulent communications from us and who to contact if they are unsure or have issues?

2 ESTABLISH ENTERPRISEWIDE DIGITAL TRUST GUIDELINES.

Ensure that the organization has established digital trust as a holistic enterprise approach. Everything an enterprise does should foster or forward digital trust. This should extend to those who trust them, those who want to trust them and those who need to trust them. The approach should include all trust factors that enable customers and other stakeholders. Policies about trustworthiness are important, but enterprises need to go a step further and build digital trust into the fabric of the enterprise.

3 ENSURE ALL ROLES ARE INVOLVED.

Everyone has a role to play in ensuring digital trust. In addition to fostering trust, organizations need to understand expectations, not only as an enterprise but also as every individual associated with or employed by the enterprise. And organizations need to understand what it means to trust others—who do they trust, how do they trust them and what is an enterprise doing to ensure that trust is well-founded and maintained? In our times of increased outsourced data and growing supply chain issues, it is more important than ever to know what an organization should expect and how to measure, assess and monitor issues related to digital trust.[4]

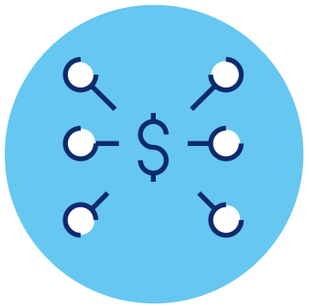
4 *Op Cit* Witte

Five Key Takeaways

1 **A generally accepted definition of 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.

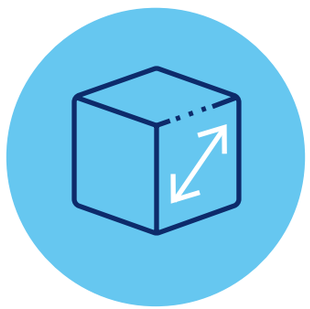
2 **Digital trust can make or break an organization.** It can be the factor that enables some organizations to recover after a major incident while others suffer from serious, time-consuming and expensive ramifications. As organizations increasingly move to a digital (or digital-first) business model, trust is an essential component that must be addressed before—and throughout—each stakeholder interaction.

Digital trust guidance should fit each organization's specific gaps and goals—big benefits can result from small changes.



3 **Digital trust does not necessarily require a significant budget allocation or the creation of a new C-suite position.** In many instances, digital trust can be approached as an umbrella that ensures existing functions are operating in the most optimal manner and that others have trust in the organization, even during negative situations. For some organizations, digital trust simply requires a new way of looking at what they are already doing. Big benefits can result from small changes.

4 **Today's 24/7 Internet-connected society means that one person's bad experience can be broadcast around the world in real time.** Serious financial, reputational, personal and regulatory repercussions can occur if transparency and digital trust are not built into—and enforced in—every area of an organization.



5 **Many organizations can benefit from digital trust-related guidance and frameworks by selecting the knowledge areas that directly benefit their unique context and business model.** Enterprises do not need to adopt full frameworks or use a prescribed, one-size-fits-all approach. Effective modern guidance is designed to be pulled apart and used as best fits the organization—the organization does not need to fit the guidance or framework.

Conclusion

There is little disagreement that new, serious and likely unexpected digital issues and incidents will continue in the future. People know that the "next big thing" (or multiple little things) is around the corner. Whether it be a pandemic, unrest, natural disaster, cyberattack or something not yet imagined, the keys to success revolve around digital trust, agility and resilience. Negative events and outcomes are inescapable in the business environment, but these three success factors can help organizations make needed changes quickly, strengthen their reputation and retain customer respect and loyalty.

Building digital trust involves more than just ticking a box on a checklist. It must also embrace the knowledge and empathy needed to address the important human, cultural, historical and experiential factors that enable trust. It goes beyond fulfilling expected or contractual obligations and extends into establishing a rapport that provides stakeholders with confidence and assurance.

Many organizations can increase their agility and ability to recover from attacks and other incidents if their commitment to digital trust is made clear, enforced, measured and communicated. Having digital trust firmly embedded throughout an organization helps it become more resilient when unavoidable and increasingly sophisticated attacks occur.

This creates the path that allows organizations to do the right thing in the right way—and achieve their strategy objectives.

SEVEN HABITS OF HIGHLY SKILLED DIGITAL TRUST PROFESSIONALS

Enterprises today often employ digital-first policies to achieve accelerated growth. Digital trust is the most critical factor in enabling and sustaining this growth. There are seven habits of digital trust professionals that can be derived from the habits first explored in the book ***The 7 Habits of Highly Effective People*** by Steven Covey.[5]

In an era of accelerating digital transformation, enterprises and professionals must address digital trust by selecting the right framework and implementing appropriate policies, procedures and practices. Digital trust professionals need to be creative problem solvers who can add value using relevant technology.

1. **Think from a macro perspective**—Digital trust professionals should identify a mission, vision and strategies per their career/enterprise objectives.
2. **Begin with the end in mind**—Envisioning what they want in the future allows them to plan and work toward achieving it.
3. **Learn to prioritize**—A framework should be developed for prioritizing work that is aimed at achieving both long- and short-term goals.
4. **Think as a team**—Developing an attitude of working in the spirit of teamwork and cooperation helps deliver beneficial solutions to all stakeholders.
5. **Understand and align with enterprise goals**—Developing communication skills with humility and empathy helps achieve common goals.
6. **Develop congruence between enterprise and career goals**—Personal goals should align with enterprise objectives and relevant stakeholders' needs.
7. **Implement a kaizen (continuous improvement) approach**—Developing a continuous improvement mindset in all spheres of activities—from planning to delivering results—leads to success.

5 Rafeq, A.; "Seven Habits of Highly Skilled Digital Trust Professionals," ISACA Now Blog, 22 February 2023, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-8/seven-habits-of-highly-skilled-digital-trust-professionals

Acknowledgments

ISACA would like to recognize:

Board of Directors

Pamela Nigro, Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

John De Santis, Vice-Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, Germany

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
NACD-DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Senior Information Systems Auditor–Advisory Consulting, KPMG Uganda, Founder, Encrypt Africa, Kenya

Gerrard Schmid
Former President and Chief Executive Officer, Diebold Nixdorf, USA

Bjorn R. Watne
CISA, CISM, CGEIT, CRISC, CDPSE, CISSP-ISSMP
Senior Vice President and Chief Security Officer, Telenor Group, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

Gregory Touhill
CISM, CISSP
ISACA Board Chair, 2021-2022
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick
ISACA Board Chair, 2020-2021 and Interim Chief Executive Officer

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM, NACD-DC
ISACA Board Chair, 2018-2019
Independent Director, Titus, Executive Chair, White Cloud Security, Managing Director, Clyde Consulting LLC, USA

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its more than 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *State of Digital Trust 2023* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

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

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

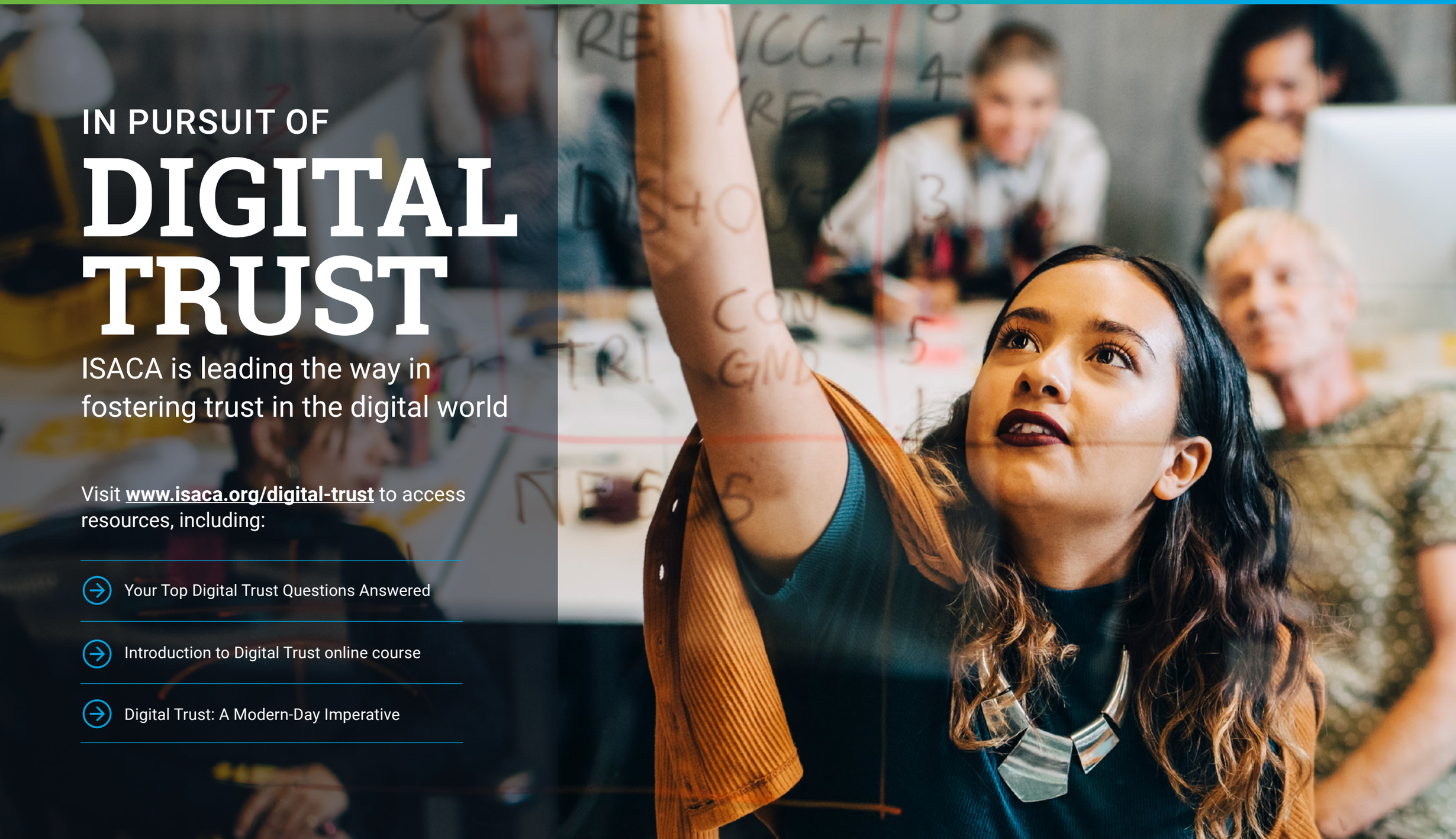
Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/



IN PURSUIT OF

DIGITAL TRUST

ISACA is leading the way in fostering trust in the digital world

Visit **www.isaca.org/digital-trust** to access resources, including:

- Your Top Digital Trust Questions Answered
- Introduction to Digital Trust online course
- Digital Trust: A Modern-Day Imperative