STATE OF

DIGITAL TRUST

2022

An ISACA Global Research Report

Contents

Abstract

The future of digital transformation is dependent on a focus on trust among all parties of online transactions. Digital trust reinforces enterprise innovation, economic expansion and value creation for all parties in an interaction. To better understand attitudes and growth factors of digital trust, ISACA® conducted the State of Digital Trust global survey in the second quarter of 2022. This report on the survey findings defines digital trust and explores areas such as familiarity, prioritization, maturity and obstacles. It discusses who holds the responsibility for digital trust within an organization and describes a void in enterprise digital ecosystems that has created opportunities for professionals to become leaders in the digital trust arena. The report includes five key takeaways to help organizations advance digital trust, as well as steps to take to improve digital trust maturity.

Executive Summary

Trust is the foundation of all relationships. It is especially critical now in the expanding digital world where multiple parties may never meet in person to share sensitive and private information needed to complete a transaction. Every interaction must reinforce that the organization cares about—and has instituted effective practices in—all areas of digital trust.

Trust must be clearly and repeatedly earned, communicated and supported. This creates a fertile environment to conduct business, which in turn reinforces innovation, economic expansion and ultimately the creation of value for all parties involved in the interactions.

Digital trust is a major driver when consumers[1] and enterprises are deciding with whom they want to conduct business. They consider many key factors when determining the trustworthiness of an organization, and all are critical to establishing and upholding digital trust.

All of these elements need to be present to show that an organization is committed to creating a business environment where customers, partners and other stakeholders can be confident that their information is secure and that the company will act ethically and deliver on promises.

Integrating these factors as disparate elements has been shown to help organizations minimize risk. But the modern and future digital-dominant business environment requires a more all-encompassing approach. All of these aspects need to be interconnected in a comprehensive ecosystem of digital trust.

Even though it may take different shapes and forms for each enterprise, digital trust needs to be enshrined into the day-to-day practices of all organizational stakeholders in all industries. Everybody has an opportunity to make an impact.

1 Consumers includes customers, users and any party to a digital interaction.

Key factors that contribute to digital trust include:

- **Quality**—Quality must meet or exceed consumer expectations.

- **Availability**—Consumers need to be able to access accurate information in a timely manner.

- **Security and privacy**—Consumers expect the data they share will be protected and kept confidential.

- **Ethics and integrity**—Enterprises should live up to their promised values.

- **Transparency and honesty**—Consumers should be informed about how their information is being used. If personal information has been compromised, consumers should know how the enterprise is addressing the situation and what it is doing to prevent it from happening again.

- **Resiliency**—Enterprises need to provide assurances that they are stable and secure, and can withstand adverse circumstances while also being able to evolve to leverage new technologies and advancements.

What Is Digital Trust?

According to ISACA, **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. It addresses ethical behaviors and expectations among all parties engaged in a transaction. Establishing a baseline of trust is integral to all digital and online interactions.

Why Is Digital Trust Important?

Trust is the bedrock of all transactions and relationships. This has become even more critical as people and enterprises increasingly rely on digital devices, technologies, services and processes.

Only 54 percent of Americans trust technology companies to do the right thing, down three percentage points from last year and down 19 points since 2019. The decline in trust was seen across a number of the most talked-about topics, including 5G, artificial intelligence (AI), the Internet of Things (IoT) and virtual reality.[2]

Any breach of trust has far-reaching consequences that can tarnish reputations and cause long-lasting customer and stakeholder distrust. Compound that with the lightning speed of communications and social media, and even areas of an organization that have nothing to do with an incident can suffer potentially devastating reputational, regulatory and financial effects.
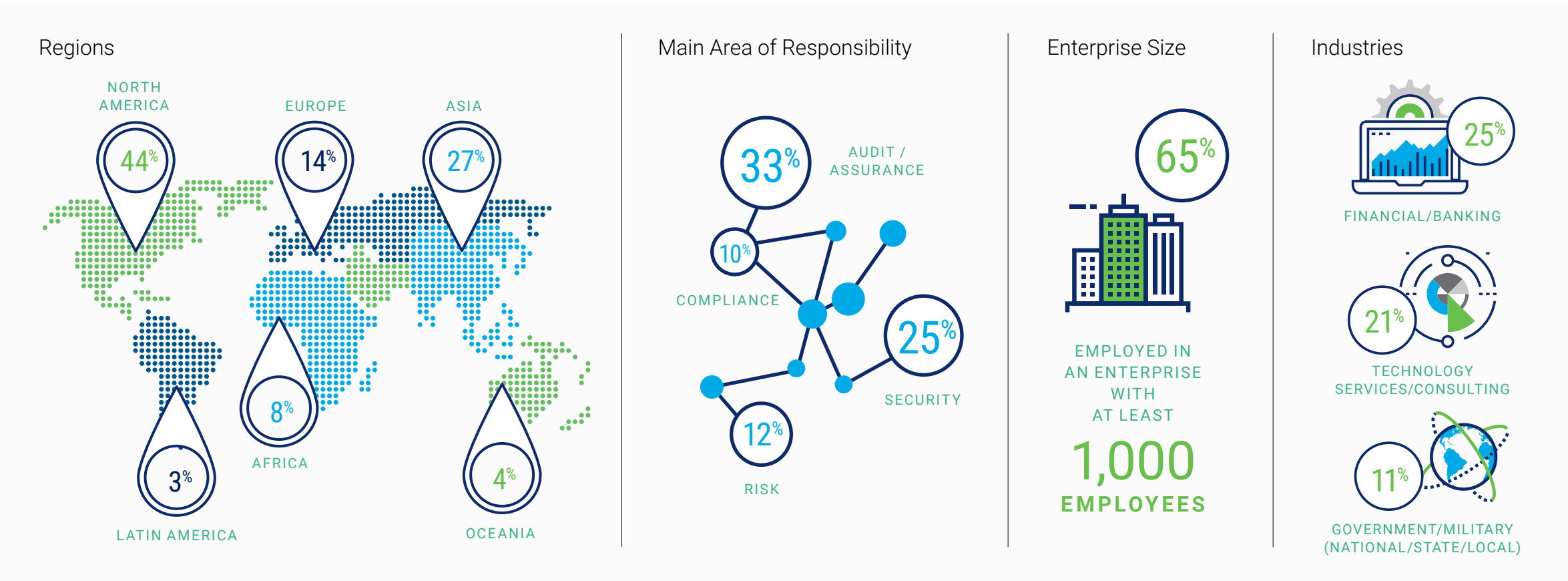
2 Edelman, "2022 Edelman Trust Barometer," **https://www.edelman.com/trust/2022-trust-barometer**

Survey Methodology

In the second quarter of 2022, ISACA sent an online survey to approximately 50,000 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 2,755 respondents completed the survey, for a margin of error of +/- 1 percentage 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

Regions

NORTH AMERICA 44%

EUROPE 14%

ASIA 27%

LATIN AMERICA 3%

AFRICA 8%

OCEANIA 4%

Main Area of Responsibility

AUDIT / ASSURANCE 33%

COMPLIANCE 10%

SECURITY 25%

RISK 12%

Enterprise Size

65%

EMPLOYED IN AN ENTERPRISE WITH AT LEAST 1,000 EMPLOYEES

Industries

FINANCIAL/BANKING 25%

TECHNOLOGY SERVICES/CONSULTING 21%

GOVERNMENT/MILITARY (NATIONAL/STATE/LOCAL) 11%

Survey Results and Insights

A broad set of factors support a business relationship and the trust needed to keep it thriving in today's increasingly digital-dependent economy. Building trust and developing trusted partnerships are strong elements as enterprises continue to lay the groundwork for digital transformation and innovation. To provide the latest actionable insights into digital trust, results of the ISACA State of Digital Trust 2022 survey are organized into seven sections:

1. Familiarity With Digital Trust

2. Importance and Prioritization of Digital Trust

3. Confidence and Maturity Related to Digital Trust

4. Obstacles to Attaining Digital Trust

5. Responsibility for Digital Trust

6. Digital Trust and Digital Transformation Tools and Frameworks

7. ISACA's Position in the Digital Trust Space

Familiarity With Digital Trust

Thinking of, and acting on, digital trust as a cohesive and comprehensive strategy is in its infancy. It is a new approach for many organizations, even though many of its components have been in practice for years.

For example, the top three most important components of digital trust according to the survey respondents are security, data integrity and privacy, but **only half (50 percent) of respondents agree that there is sufficient collaboration at their organization among professionals who work in these fields**. All of these are important, but digital trust becomes even more comprehensive and effective when they are interwoven, along with other top components such as risk management, governance, quality, assurance, resilience and ethics. Each of the components makes a strong contribution to earning trust, but it is even more impactful when they are considered and managed within the context of the enterprise's whole digital trust strategy.

This is a significant concern that is beginning to be addressed among global enterprises. The World Economic Forum established a Digital Trust Initiative to identify "steps to improve the trustworthiness of digital technologies through security and responsible technology use…Stakeholders from a cross-section of industry must come together to rebuild confidence in the people, processes and technologies it takes to build a secure digital world" and "drive the adoption of more secure and trustworthy technologies to circumvent the 'distrust trap' for citizens, businesses and governments."[3]

3   World Economic Forum, Why we must rebuild digital trust for a cyber-inclusive future, https://www.weforum.org/agenda/2021/11/rebuilding-digital-trust-for-a-cyber-inclusive-future/

When respondents were asked, without prompts or definitions, if they were familiar with the term "digital trust," only 29 percent were very or extremely familiar. At 50 percent, respondents in India were more familiar with the term than in the US. In addition, respondents from Latin America (37 percent), Africa (35 percent) and Europe (34 percent) also indicated a higher familiarity than the total of respondents. When viewed by industry, those in consulting (35 percent) were more familiar with the term than those working in finance/banking (28 percent).

Respondents were then provided with the definition "Digital trust is the confidence in the relationship and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, process, information and technology to create and maintain a trustworthy digital world." After being exposed to the definition to clarify their understanding, respondents' familiarity jumped to 52 percent.

In addition to sparking familiarity, this definition itself seems to resonate with respondents. When asked how well that description matches their understanding of digital trust, 51 percent said it mostly matches and 21 percent said it completely matches. Only 1 percent said that it did not match at all.

This underscores the importance of having a consistent understanding of what digital trust encompasses among global enterprises, and even within a single organization, including at the team or department level. Until now digital trust has been more like appreciating fine art—something that many people say they "know it when they see it." This approach must change. These vital functions can no longer be run as disparate groups that operate independently—they need to be coordinated within an enterprise's digital trust ecosystem.

For businesses to succeed in the growing digital-dominated environment, it is critical that people, both internal and external to an organization, understand and actively address the trust factors that enable safe, private and reliable digital transactions.

Importance and Prioritization of Digital Trust

Clear alignment and agreement on the definition among professionals is an important first step in improving digital trust and achieving its benefits. If it is not defined, then no matter how beneficial it is, it becomes harder to prioritize, and prioritization of digital trust is absolutely critical for organizations that want to remain viable and relevant.

While 85 percent of respondents say that digital trust is extremely or very important to organizations today, and 63 percent say that digital trust is extremely or very relevant to their job role, only 66 percent say that their organization prioritizes digital trust in line with its level of importance. This will be a growing concern, as four out of five respondents (82 percent) believe that digital trust will be more important in five years than it is today.

Across the regions, respondents from Africa (93 percent) had the highest response rate indicating digital trust being extremely or very important. Following closely are respondents from Latin America (86 percent), Oceania (85 percent), Europe (84 percent), North America (84 percent) and Asia (82 percent).

When asked about how their organization prioritizes digital trust corresponding to its level of importance, results showed a difference among industries. Seventy-two percent of respondents in finance and banking, 70 percent in consulting and 57 percent in government and military feel it is prioritized.

"When I hear the term 'digital trust,' I think 'ISACA'– it's been in our DNA throughout our 50-plus year history. As an article in Wired magazine said, 'If the lifeblood of the digital economy is data, its heart is digital trust.' The work performed by ISACA's professional community in areas such as information security, data privacy, IT audit, risk management, governance and securely implementing emerging technology gives organizations the confidence and permission needed to thrive in the digital economy. The most effective professionals in each of these career fields have a holistic understanding of multiple digital trust professions on top of their vertical expertise."

DAVID SAMUELSON
Chief Executive Officer, ISACA

Survey respondents also opined on the impact digital trust has on certain aspects of their organizations. **Figures 2** and **3** details these results.

FIGURE 2 – Digital Trust-related Benefits

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

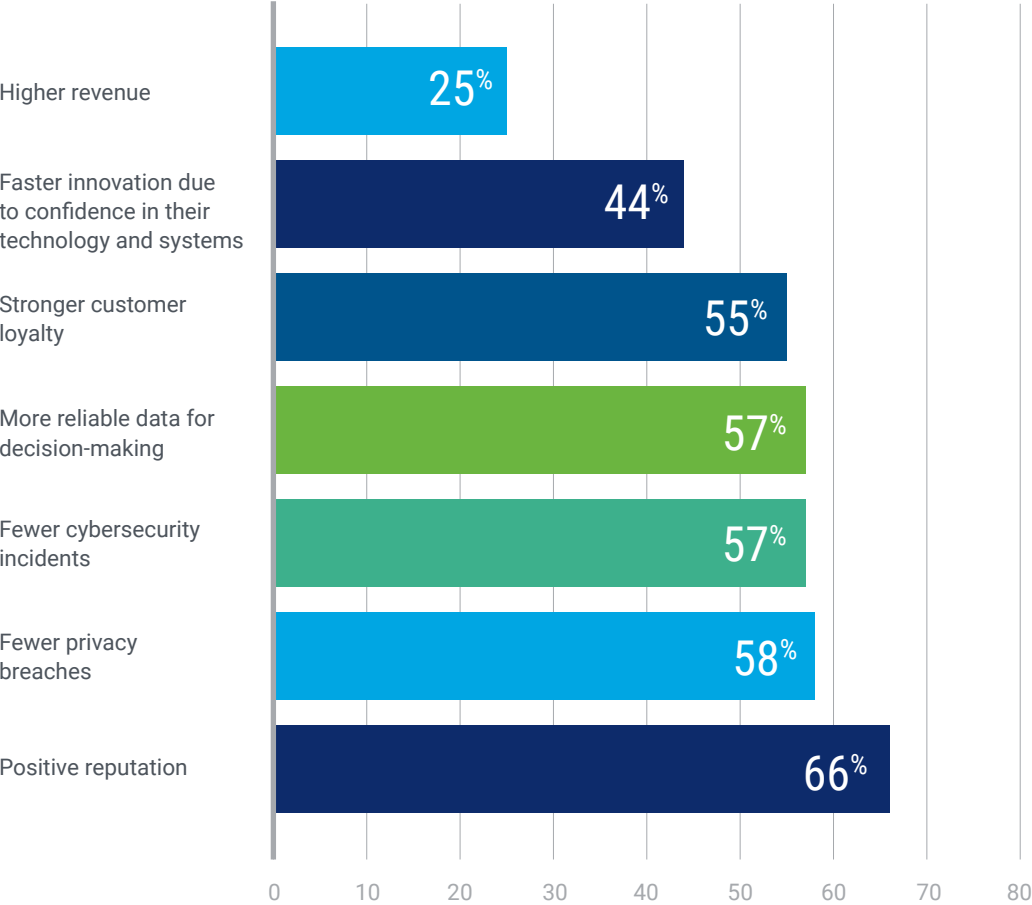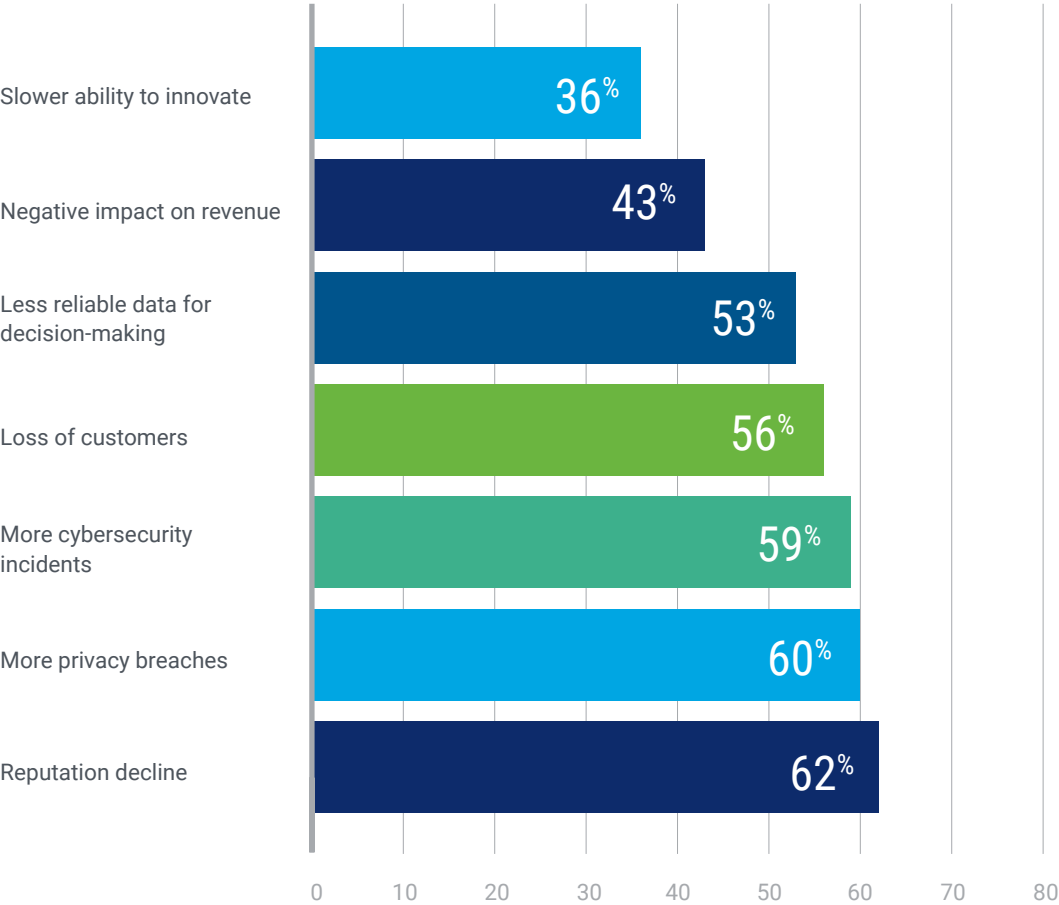| Benefit	Percentage
Higher revenue	25%
Faster innovation due to confidence in their technology and systems	44%
Stronger customer loyalty	55%
More reliable data for decision-making	57%
Fewer cybersecurity incidents	57%
Fewer privacy breaches	58%
Positive reputation	66%

FIGURE 3 – Consequences of a Lack of Digital Trust

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

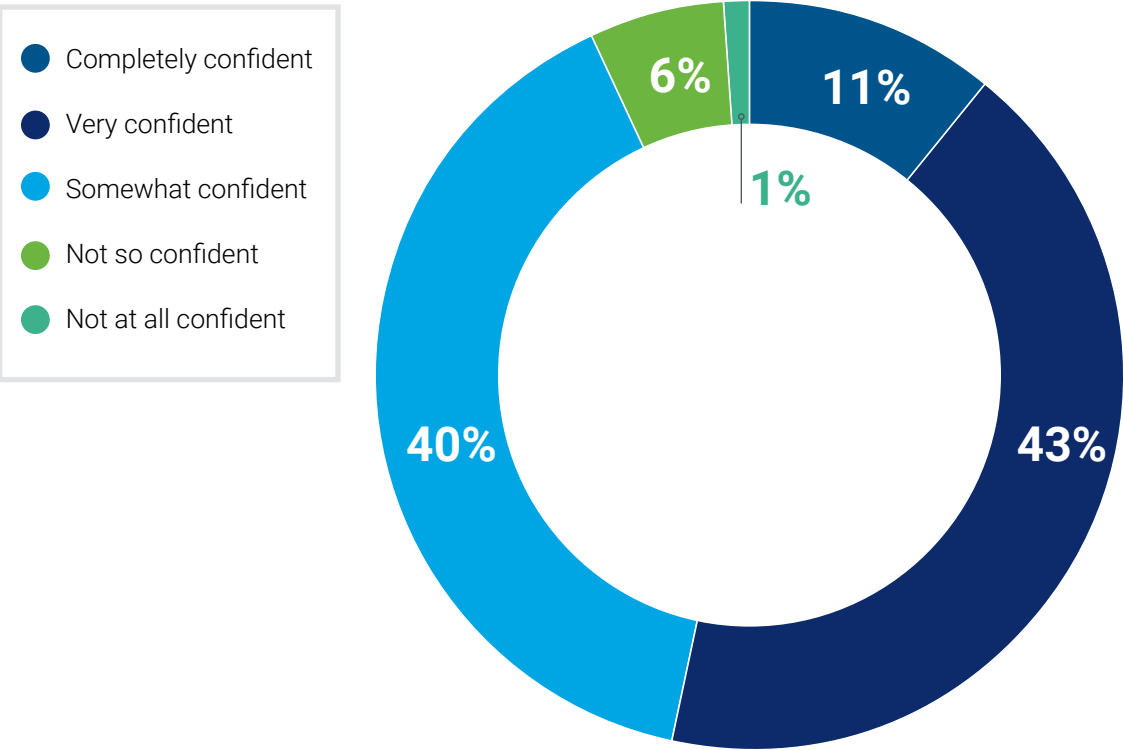| Consequence	Percentage
Slower ability to innovate	36%
Negative impact on revenue	43%
Less reliable data for decision-making	53%
Loss of customers	56%
More cybersecurity incidents	59%
More privacy breaches	60%
Reputation decline	62%

Confidence and Maturity Related to Digital Trust

More than half (54 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, confidence jumps to 81 percent.

FIGURE 4

How confident are you the digital trustworthiness of your organization?

Legend:
- Completely confident
- Very confident
- Somewhat confident
- Not so confident
- Not at all confident

Chart values: 11%, 1%, 43%, 40%, 6%

Around the world, confidence is higher in India (76 percent) than in the US (52 percent). Across industries the results were very similar with consulting (61 percent), finance and banking (59 percent) and government and military (43 percent).

While that is promising, it is concerning that fewer than one in four (23 percent) say that their organization currently measures the maturity of its digital trust practices even though 68 percent believe it is extremely or very important to measure this maturity.

Those that measure digital trust reported two things in common—most have a board of directors that has prioritized digital trust and most use a digital trust framework.

When it comes to external assessments, only 26 percent say that they measure their organization's level of digital trust among customers. Thirty-six percent do not measure this at all and 41 percent were unsure, which shows another area of potential improvement.

Those that measure digital trust reported two things in common—most have a board of directors that has prioritized digital trust and most use a digital trust framework. There is a higher prevalence of this in Asia and Africa.

Addressing digital trust and safety in a holistic manner that accounts for the technical and human aspects is part of the maturity process as organizations

increasingly transition from in-person transactions that may use an element of technology to relationships that rely mostly or fully on digital technology.

Measurement is a factor that reflects importance an organization places on digital trust, as 93 percent of those currently measuring digital trust maturity say that digital trust is extremely or very important to their organization today.

One of the ways that organizations show commitment to strengthening digital trust is through a high score or rating from an independent third-party assessment. Of the respondents, 82 percent agree that organizations that can achieve a high score will ultimately be more successful. Again, measurement makes a difference; this figure jumps to 92 percent among those who currently measure digital trust maturity.

Organizations use a variety of ways to measure digital trust. According to respondents, 43 percent perform an internal review of trust-related practices and 33 percent use customer/client research including surveys and focus groups. Thirty-two percent benchmark against similar enterprises, but unfortunately, 33 percent say they do not measure digital trust.

Measurement can help an organization see where its current position is in relation to industry benchmarks. It is a good start, but to make concrete improvements, the organization needs to ensure all stakeholders are also continually improving and working toward the same goal.

One of the strongest benefits of measuring maturity is that it creates a repeatable process so an organization can have confidence in its results. It is positive to

see that enterprises are recognizing the many values of maturity and yet it is not surprising that some have not yet fully thought through how they will measure maturity and other achievements. Creating a digital trust maturity roadmap is a start and is a key part of getting to their desired destination.

Obstacles to Attaining Digital Trust

One of the most effective ways of achieving goals is to understand—and address—what is blocking the path forward. **Figure 5** shows the most significant obstacles to attaining high levels of digital trust within an organization, according to the survey.

FIGURE 5 – Obstacles for Attaining Digital Trust
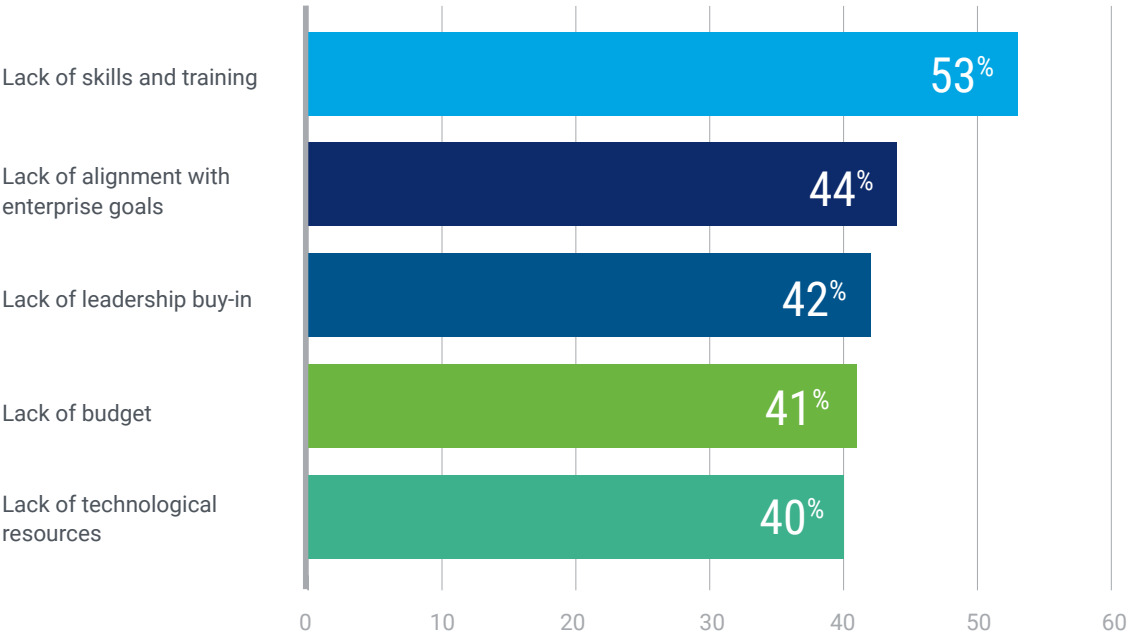
Only 29 percent say that their organization has offered digital trust training to staff. In addition, only 28 percent say they "completely understand" how their role impacts digital trust, even though 63 percent indicate that digital trust is extremely or very relevant to their job today.

Lack of leadership buy-in is higher in India (49 percent) than in the US (37 percent), with similar numbers being reported about lack of technological resources.

The results present an interesting viewpoint from the respondents. While a lack of training opportunities and alignment with enterprise goals are serious considerations, it is worrying that, in many cases, there still is a lack of leadership buy-in. This concern stems from several reasons, including:

- Leaders should champion and support the pursuit of a digital trust ecosystem throughout the organization as part of their commitment and duties. They need to continually improve the trust factors and holistic approach that are important to stakeholders, that translate into customer attraction and retention, and that contribute to positive financial results.

- Focusing on digital trust can help an organization avoid or reduce fines and other negative consequences related to regulatory issues.

- With leadership buy-in, remaining obstacles can be more effectively addressed and appropriately funded. Organizational alignment, skills and training, and technology resources all fall into place and move forward when they receive support, funding and attention of executive leadership.

It also is interesting that lack of budget received such a high response (41 percent) because working toward effective digital trust does not need to be a major expenditure. On an optimistic note, 63 percent say that digital trust, as described in ISACA's definition, can be achieved in their organization.
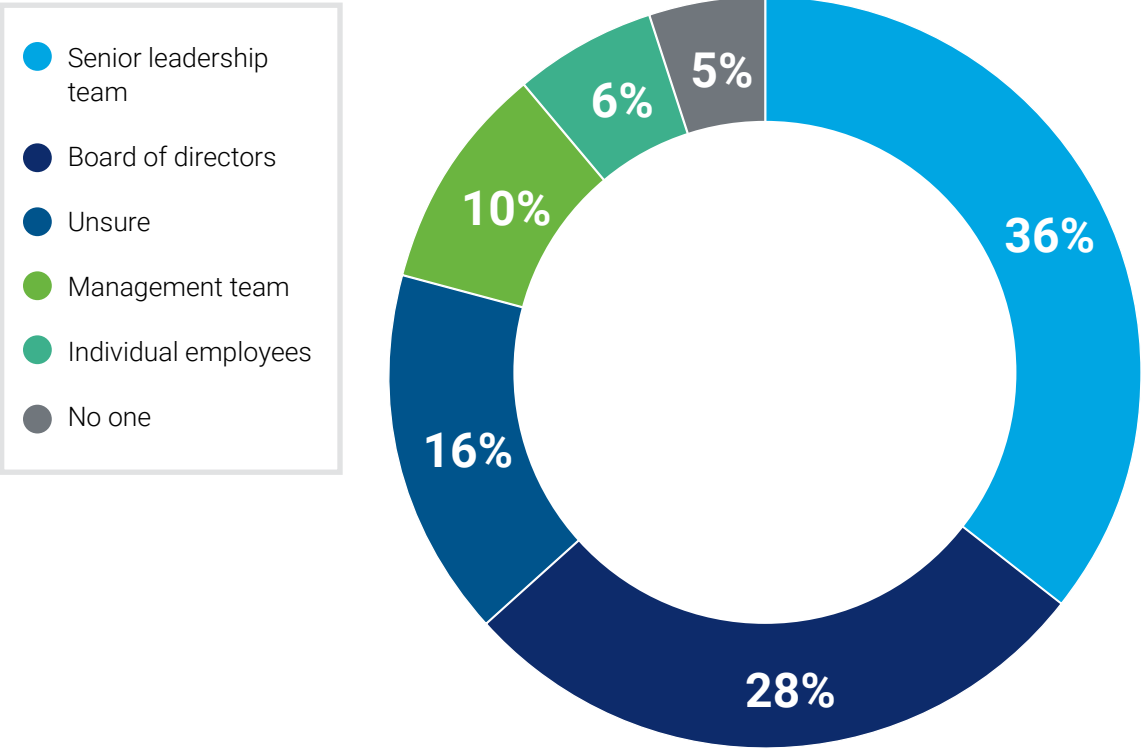
Responsibility for Digital Trust

Who is responsible for digital trust? Boards of directors and senior management have ultimate responsibility for the strategic direction, effectiveness, sustainability and long-term viability of an enterprise. While everybody in an organization has a role to play in ensuring the strength and benefits of digital trust, it does not mean that everyone is responsible. C-level executives are the drivers of digital trust and must ensure that it is a clear and supported priority in every aspect of operations.

Figure 6 shows those responsible for digital trust, according to survey respondents. Only 12 percent say that their organization has a senior staff role for digital trust, for example Chief Trust Officer or Director of Digital Trust.

FIGURE 6 – Digital Trust Responsibility in an Organization

Who is ultimately responsible for digital trust in your organization?

- Senior leadership team
- Board of directors
- Unsure
- Management team
- Individual employees
- No one

36%
28%
16%
10%
6%
5%

Respondents from India are more likely to say the board of directors (33 percent) than in the US (19 percent). US respondents are more likely to say it is the senior leadership team (46 percent). Those in Asia, Africa and Europe are more likely than respondents in North America to believe that the board of directors is more responsible for digital trust.

This indicates that enterprises do not necessarily need to create a new C-suite position with a sole focus on digital trust but should ensure that the chief executive officer (CEO), chief operations officer (COO) or similar executive has the responsibility to deliver on enterprise-wide digital trust. Care should be taken that it does not become a stovepipe where digital trust is an isolated objective. The goal is for it to be an integrated approach—as opposed to a designated role—where a member of the leadership team makes sure that all of the appropriate areas are coordinated and address digital trust in the most effective and optimal way.

The top three roles indicated as most critical for strengthening digital trust in an organization are IT strategy/governance (84 percent), security (80 percent) and information technology (74 percent). This is followed by risk and compliance (73 percent), audit (59 percent), compliance (59 percent) and privacy (54 percent).

While they do not have ultimate responsibility, all of these areas are critical to an organization's success, and they all will contribute even more significantly to improving digital trust maturity in the future. This also is a good opportunity for any one of these areas to step up and take more of a leadership role as digital trust grows as a multi-disciplinary imperative.

In addition, only 12 percent of respondents indicated that their organization had a dedicated staff role for digital trust. Of those who measure digital trust maturity, however, that percentage increases to 34 percent. Of those whose board of directors has prioritized digital trust, this increases to 43 percent having a dedicated staff role for digital trust.

Only 20 percent indicate that their board of directors has made digital trust a priority. There is more attention to this in India, where 34 percent say the board has made it a priority.

Digital Trust and Digital Transformation Tools and Frameworks

Digital transformation initiatives have long been a high priority for organizations. To obtain the highest level of benefits from these innovation efforts, they need to first establish and sustain strong digital trust among customers, employees and other stakeholders. For example, customers need to be assured that their money and payments are safe and will result in the products and services being delivered in an appropriate way.

Since 76 percent of respondents agree that digital trust is important to digital transformation, it is clear that this concept is well understood.

Respondents in Africa (92 percent) reported the highest level of the importance of digital trust to digital transformation, followed by Asia (76 percent), Europe (76 percent), North America (74 percent) and Oceania (70 percent).

When it comes to ensuring that digital trust is gained, only 19 percent say that their organization currently uses a management framework for digital trust and

40 percent are unsure if their organization uses a framework. Yet, more than half (55 percent) say having a digital trust framework is extremely or very important to their organization.

Of those that use a framework, 39 percent are unsure which one and 27 percent use COBIT®. Of those that measure digital trust maturity, that number rises to 41 percent who use COBIT, 23 percent use an internally developed framework and 21 percent use SAFE Identity Trust Framework..

Some of this disconnect may reflect the need for better understanding and agreement on the definition of digital trust and a digital trust framework. It is very possible that an organization is using a digital trust structure or framework but refers to it in different terms or uses a different description.

Digital innovation requires unique approaches—companies cannot do the same processes in a digital way and call themselves transformed. They need to keep their eyes open to the internal and external influences, triggers and signals that either subtly indicate, or loudly blare, that change is needed, and is even already underway.

Enterprises need to look beyond just digitizing the old ways of doing things and instead view previous processes from a new perspective. To do this they need a structure – not something rigid and monolithic with boxes to tick, but rather more of a scaffolding that organizations can use to develop, organize and communicate their digital transformation initiatives. This is the basis of ISACA's upcoming digital trust ecosystem framework. It focuses on non-technical, common-sense approaches that can be customized by organizations to best fit their goals.

Enterprises need to look beyond just digitizing the old ways of doing things and instead view previous processes from a new perspective. To do this they need a structure – not something rigid and monolithic with boxes to tick, but rather more of a scaffolding that organizations can use to develop, organize and communicate their digital transformation initiatives.

A framework needs to help enterprises address the full spectrum of factors, including regulatory compliance and contractual obligations. At the same time, it also needs to span dimensions of digital trust including user experiences, cultural nuances and human behavior. Frameworks are flexible to enable organizations to pull out the areas and guidance that applies to their specific needs.

"An effective digital trust dashboard should cover the organization's current state, concerns, opportunities and remediation options. Be sure to provide potential solutions to problems that are presented to the board and senior executives."

JO STEWART-RATTRAY
CISA, CISM, CGEIT, CRISC, Member of ISACA's Digital Trust Task Force and Director of Technology & Security Assurance at BRM Advisory

ISACA's Position in the Digital Trust Space

Effective governance over an enterprise helps drive digital trust. Organizations with robust security, privacy, IT risk, IT assurance, and information and technology practices are often considered digitally trustworthy. As industries progress and mature, there has become a critical—and growing—demand for digital trust to be measured, managed and prioritized in a strategic way throughout all aspects of every enterprise.

ISACA is addressing these needs through research and development of industry-leading tools, credentials, education and training. ISACA's global community of dedicated and experienced IT and business professionals work together to lead the growth, share knowledge and encourage the practices of digital trust in all industries.

Fifty-nine percent of respondents say that ISACA is a recognized leader in digital trust and 62 percent say that ISACA is an emerging key player in the space. This dual vision could be due to ISACA's extensive research and development in the digital transformation space and the new focus that some enterprises are putting on the importance of digital trust.

When it comes to gaining individual career-enhancement benefits from ISACA as a professional development association, 49 percent say that ISACA offers a recognized credentialing program in digital trust, 60 percent say that ISACA has the tools and resources available for IT professionals to successfully deliver digital trust, 78 percent say that ISACA enables them to be successful in their profession, 82 percent say that ISACA enables them to stay current with industry trends and 73 percent say that ISACA provides opportunities for them to be recognized as a thought leader.

Getting Started on a Digital Trust Ecosystem

Three Steps to Improve Digital Trust Maturity

As organizations progress further in digital transformation, they need to ensure that they are at an appropriate level of digital trust maturity and that they are positioned for the future. It is critical to understand stakeholder culture, values and behaviors to learn where to shore up practices and gain the benefits of digital innovation. Three steps to get started along this path are:

1 UNDERSTAND

Understand what the organization wants to accomplish and learn how digital trust can contribute to its goals. Start by defining what customers, employees and stakeholders expect of each other. Measure the current state and benchmark against industry good practices.

2 OUTLINE

Outline the desired state and begin developing the road map to achieve it. Understand the priority issues being faced by senior leadership, how digital trust will resonate within their focus areas and provide potential solutions. It also is important to understand the human element of trust. For many years organizations focused on technical upgrades and services – for example, card scanning and self-checkouts. While efficiencies were created, true digital innovations are achieved by also addressing the nuances of human behavior and attitudes.

3 FOCUS

Focus on a mindset of continuous improvement as it pertains to security, quality, reliability, compliance and customer experience. Ask questions such as: How can we do better? How can we be more consistent and responsive? How can we share lessons learned and find new ways to improve?

5 Key Takeaways

1

Successful digital transformation requires that organizations maintain a strong bedrock of digital trust. Business transactions increasingly require that sensitive and private information be shared online among multiple parties. In the growing digitally focused marketplace, it is critical that enterprises earn the trust of their stakeholders every day and with every interaction. Digital trust is the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. Any breach of digital trust can have far-reaching negative consequences to an organization's or an industry's reputation, value and financial viability.
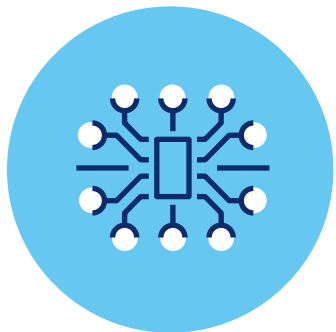
2

Digital trust has many facets that need to be integrated within a cohesive organization-wide strategy and approach. Factors that influence digital trust include quality, availability, security and privacy, ethics and integrity, transparency and honesty, and resiliency. Enterprise areas most involved in digital trust include IT strategy/governance, information technology, risk management, assurance, compliance and resilience.

While all of these areas are critical individually, they also must be managed in a comprehensive trust environment aligned with the organization's digital strategy. This creates an opportunity for professionals in these areas to step up, share their expertise and exhibit leadership within this cohesive overarching strategy.
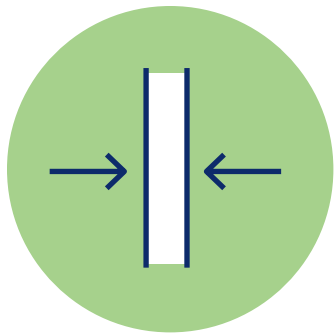
3 **Senior executives must clearly define, prioritize, measure and align digital trust throughout organizations.** While all employees have a role, an organization's senior executive team has the primary responsibility to support and prioritize digital trust that drives digital innovation and transformation. The ISACA survey shows that there is a potentially harmful disconnect between the perceived importance of digital trust and its current priority within organizations. This will need to change for organizations to be viable, competitive and trusted leaders that reap the benefits of digital transformation.

Senior executive support also helps address the survey's most frequently mentioned obstacles to digital trust, which include lack of skills and training, lack of alignment with organizational goals, lack of budget and lack of technical resources. With leadership support, these areas can be effectively addressed and funded.

4 **Measurement of digital trust is critical to improving the organization's maturity and its ability to achieve the rewards of digital transformation.** There are many ways to measure digital trust, which in turn can help improve organizational maturity and lead to value creation. Some tactics include doing internal reviews, third-party assessments, surveys, focus groups and other customer/client research. Information gained can then be used for benchmarking against similar enterprises and other analysis purposes.

Organizations can establish dashboards that cover their current state, the pulse of the marketplace, current concerns, solutions to issues and new potentially unexplored opportunities. These activities can lead to benefits including enhanced reputations, fewer privacy breaches and cybersecurity incidents, more reliable data for improved decision-making, higher customer attraction and retention rates, stronger customer loyalty, faster innovation due to confidence in the organization's technology and systems, and higher revenues.

5 **Digital trust is a journey.** Trust must be assured and earned every day with every digital interaction. This is not a one-and-done goal. For enterprises to grow and succeed, they need to understand that digital growth must address ongoing technological advancements as well as the nuances of human needs, culture and attitudes. If organizations will be asking for more trust from their stakeholders, then they must understand how to earn that trust within the stakeholders' comfort levels.

Conclusion

Digital trust must go hand-in-hand with plans and goals of digital transformation. It must be a priority that is championed by leadership and supported throughout all levels the organization. Organizations need to be open and equipped to find new ways to look at new challenges.

When asked if there is significant collaboration at their organization among professionals who work in digital trust fields (such as security, risk, governance, assurance, privacy and quality), responses showed that there is room for improvement. Only 12 percent said they strongly agree and only 38 percent said they agreed.

As a whole, these results show a void in the current status of a digital ecosystem and create opportunities for professionals in these areas to step up and exhibit leadership in the comprehensive digital trust arena.

The future of increased enterprise focus on digital trust looks promising. Eighty-two percent of respondents say that in five years, digital trust will be much more important in their organization. In addition, 28 percent say they do not currently have a senior staff role dedicated to digital trust but will likely have one in the next five years.

Establishing a strong digital trust ecosystem is a continual evolution in a team environment; it doesn't stop when a project is completed. Organizations need to understand why they need to change and then identify what needs to change and how they plan to make the change. Only then will they be in a position to truly reap the benefits of digital innovation and transformation.

Trust reduces several types of friction in a transaction between givers (e.g., users) and guarantors (e.g., enterprises, laws and regulations that make the online experience seamless and convenient). This friction can be infrastructural (due to poor design or functionality), systemic (due to regulatory or legal requirements) and caused by uncertainty (for example, between parties to the transaction). The ultimate goal ought to be "intelligent friction": balancing a seamless experience with proper protections.

SOURCE: Harvard Business Review, "The 4 Dimensions of Digital Trust", February 19, 2018. **https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries#:~:text=We%20considered%20four%20key%20dimensions,Attitudes%2C%20Environment%2C%20and%20Experience**

For more information on the State of Digital Trust, **visit www.isaca.org/state-of-digital-trust.**

Acknowledgments

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

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
Former President and Chief Executive Officer,
Diebold Nixdorf, 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 Former Chief Risk
Officer, Hudson City Bancorp, USA

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 165,000 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 Survey Report 2022* (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