



Does your technology drive stakeholder trust?

A pragmatic guide to launching your
digital trust journey

Click to start



Tech drives the business. Does your tech also drive trust?



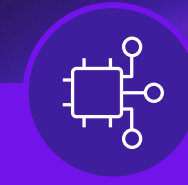
Embracing digital trust: The key to customer retention and growth

Organizations that demonstrate high levels of digital trust have become the preferred choice for customers. Those that ignore the digital trust imperative are most likely to see a lack of support over time if transparency is not provided or there are incidents that break the trusted relationship. Digital trust is essential for businesses to thrive in a fast-paced market, with a focus on addressing cybersecurity, data privacy, responsible artificial intelligence (AI), and information risk management.



Balancing innovation and compliance

Technological advancement is creating opportunities for organizations to generate new streams of revenue and evolve their business models. But new digital products also introduce new challenges around regulatory compliance and risk management. Technology risk can be mitigated—and digital trust enhanced—through an integrated and deliberate effort.



Closing the trust gap: The rising importance of digital trust in a transforming world

A 2023 ISACA survey reveals that:

84% of digital trust professionals consider it **highly important** today,¹

82% believe it will gain **even more significance** in the next five years. However, the complex and dynamic nature of digital trust presents significant challenges for most enterprises. It is vital for organizations to recognize and bridge the growing trust gap between the public and themselves, as emphasized in a World Economic Forum report² in collaboration with KPMG.

¹ "State of Digital Trust," ISACA, May 2023

² "Earning Digital Trust: Decision-Making for Trustworthy Technologies, Insight Report," World Economic Forum, November 2022

Digital trust imperative – Customer at the core

There is an intensifying demand for **customer trust, resilience, and transparency** in modern technology-enabled services. Digital trustworthiness must be core to the brand.

Customer use cases driving demand for digital trust

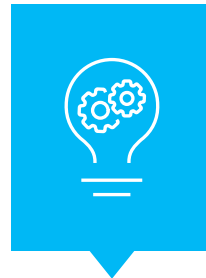
- Customer data collection
- Products with software embedded
- XaaS, SaaS, PaaS, and IaaS
- IoT, sensors, and mobile devices
- Financial services
- Online marketplaces
- Supply chains
- Data services/telemetry data

The digital trust mindset



Create transparency at the speed of digital

Digital is changing customer engagement end to end, and now more than ever, services and products are delivered via modern technologies. Adopt an open and clear communication approach to effectively build trust and confidence among your customers.



Reduce complexity and achieve commercial advantage

Unlock new growth opportunities with additional transparency with customers. Customers require evidence of a formal technology risk and cyber programs to expand the business relationship. Design and implement a repeatable framework to provide confidence that technology, data, and services are protected.



Chart your digital trust journey and channels

Driving a digital trust culture includes strong leadership support, understanding the trust priorities for your business, and identifying avenues to demonstrate commitment to your stakeholders. Enhance external communications, engage in professional and community activities, and obtain relevant certifications.

Have you considered the regulatory landscape?

Regulatory bodies at the local, state, national, and global levels are taking a more active role in regulating the usage of modern technology and generating greater checks and balances, adding to the already complex regulatory landscape.

The lack of digital trust programs can undermine brand reputation, customer loyalty, business relationships, and profitability.

As per the KPMG International 2022 cyber report, [Mission: Trust. How to unlock the true value of the CISO](#), concerns over data protection can significantly undermine stakeholder trust in businesses.³

This, in turn, can lead to challenges in closing deals efficiently and meeting stakeholder demands for increased transparency and proper governance.



Now is the time for business, IT, and security leaders to build, maintain, and enhance digital trust in all facets of their organization's activities. This document explains the concept of digital trust and shares leading-practice recommendations for developing a digital trust framework that helps drive growth and profitability in the tech-driven business world.

³ "Mission: Trust. How to unlock the true value of the CISO," KPMG International, 2022

Understanding digital trust

Digital trust is the expectation by individuals that digital technologies and services—and the organizations providing them—will protect all stakeholders’ interests and uphold societal expectations and values. It describes a digital ecosystem that enables all stakeholders to experience safe and secure interactions.

The following pillars support and help organizations earn digital trust:



Security, privacy, and reliability

Organizations protect enterprise data, processes, and technologies to maintain stakeholder confidence in business operations.



Inclusive, ethical, transparent, and responsible use

Organizations take responsibility for the storage, exchange, and treatment of their data and digital tools in alignment with societal principles of fairness, inclusivity, equality, and social responsibility.



Accountability and oversight

Governance, when designed effectively, ensures responsibility, regulatory compliance, certification, and trustworthiness in management functions that rely on digital tools.

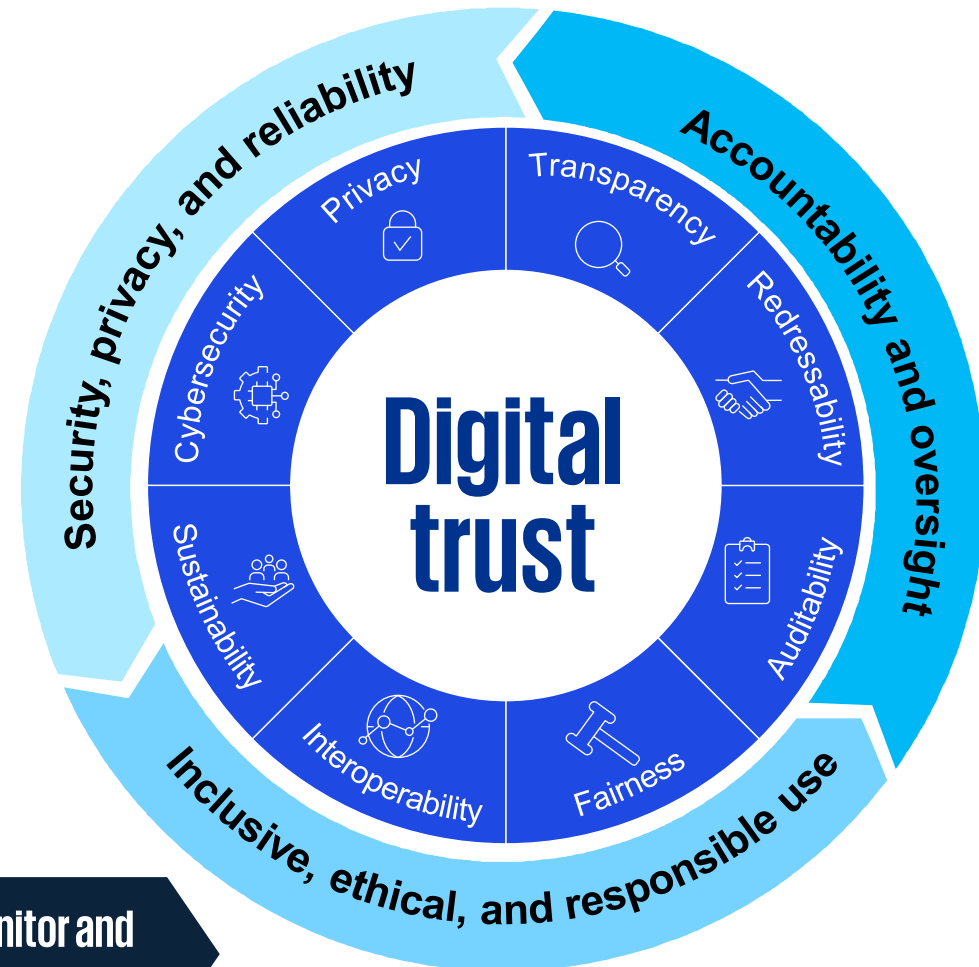


Benefits of a digital trust framework

Developing a robust digital trust framework can help an organization gain a competitive edge and lead to improved business relationships, strengthened brand reputation, increased customer loyalty, enhanced profitability, and efficient stakeholder management, enabling organizations to remain ahead of the competition.

By concentrating efforts on business areas where transparency and digital trust are essential, organizations can effectively enhance customer outreach and connection, resulting in improved customer experience.

Utilizing a digital trust framework aids in making informed decisions about the development, application, and utilization of modern technologies and services. The framework helps outline digital trust objectives and promotes a consistent approach across the organization as various technologies are assessed and integrated.



Source: World Economic Forum



Building a digital trust framework

The development of a digital trust framework encompasses four key areas:

1. Commit



Digital trust is everyone's job, starting at the top. Success requires the support, acceptance, and participation of employees and other stakeholders throughout the organization.

Key actions:

- Define what digital trust means for the organization based on the digital footprint, products, and services.
- Gain leadership support and identify an executive sponsor.
- Communicate the significance of digital trust to employees and stakeholders using clear language and storytelling.
- Set clear strategies and objectives.
- Establish a RACI matrix for key stakeholders, defining their roles and responsibilities as you outline the necessary steps in an action plan to foster and maintain digital trust.
- Identify key performance indicators (KPIs) and define targets for each KPI.
- Articulate desired outcomes and results that will be achieved with digital trust.

2. Identify and address gaps



Organizations must proactively identify the areas that necessitate focused digital trust initiatives, pinpointing products and services where customer transparency is essential and addressing the existing gaps accordingly

Key actions:

- Design the digital trust framework that matches the organization's business goals, regulatory requirements, and customer expectations.
- Identify potential risks to earning digital trust and establish approaches to alleviate those risks.
- Identify the core areas that require optimization, such as data privacy, product security, cybersecurity, resiliency, transparency, accountability, the user experience, and social responsibility.
- Create and implement customized solutions such as privacy policies, cybersecurity measures, employee training, and user experience—all designed in line with the organization's vision and values.
- Develop the communication and transparency plan with external stakeholders across a variety of channels and platforms.
- Identify leading frameworks and certifications, such as PCI DSS, HIPAA, SOC, ISO, and TISAX that can help attest to the organization's trust efforts.

Building a digital trust framework

3. Build and integrate



The development and implementation of an organization's digital trust capability requires actions in the areas of people, processes, technology, and governance.

Key actions:

- Build and integrate technology, processes, and personnel for a digital trust framework in alignment with the strategic goals of the organization.
- Hire or train employees to support optimal digital trust practices.
- Create and implement security and governance solutions for cybersecurity, product security, responsible AI, cloud platform governance, and technology resilience.
- Develop incident response plans to address digital trust risks that may arise.
- Build an external trust and transparency portal on organization's website.
- Obtain external assurance and certification to attest to the organization's trust efforts.
- Execute external communication plans including professional and community involvement (i.e., keynote speaker, panel discussions, podcast, etc.).

4. Monitor and improve



Once the digital trust framework has been implemented, organizations need to support future improvements and business requirements to maintain digital trust.

Key actions:

- Help ensure ongoing risk assessment, continuous improvement, and consistent communication with stakeholders.
- Regularly review and update frameworks, policies and procedures.
- Deploy tools to help detect potential digital trust risks and provide insights into trends and patterns that may indicate an increased risk.
- Conduct ongoing monitoring of key controls and practices.
- Gather feedback from stakeholders to help ensure that digital trust always remains a top priority for the organization.
- Provide continuous training and education to help ensure employees and stakeholders understand the importance of digital trust and are equipped with the knowledge and skills necessary to support it.

Digital trust in action

Transparency plays a crucial role in earning digital trust from key stakeholders such as customers, employees, partners, and investors. Here are some examples of how organizations have achieved this by being transparent.

Embracing transparency for enhanced trust and fairness

Google's Transparency Report: Google regularly publishes a comprehensive transparency report that includes information about government requests for user data, content removal requests, and traffic disruptions. By sharing this data, Google assures its users about the company's commitment to privacy and security.

Cloud service providers (CSPs) trust portals: Leading CSPs such as AWS⁴, Microsoft Azure⁵, and Google⁶ have established trust portals where customers can access comprehensive information about their security, privacy, resiliency, and compliance programs, including business continuity plans and penetration testing results.

S&P Global⁷ fosters transparency and trust through a comprehensive market intelligence platform, providing reliable data with AI-powered search, sustainability insights, and real-time visualization, backed by a \$50 reward for data errors or omissions.

Securing tech-driven products

Health-tech organizations showcase digital trust and regulatory compliance (GDPR and HIPAA) via certifications such as ISO 27001 and EU-US Privacy Shield. Displayed on websites or press releases, these certifications demonstrate how these organizations secure personal health data, maintain privacy, and protect critical information.

An automotive manufacturer with sales in Europe must adhere to UN Regulation No. 155 and obtain compliance with ISO 21434 for vehicle safety and reliability. These guidelines are designed to mitigate cybersecurity risks and boost resilience against cyberattacks. They foster supply chain cooperation and transparency while safeguarding vehicle security and consumer data privacy.

Financial services organizations emphasize transparency in data privacy policies for client trust and adhere to certifications such as PCI DSS and FFIEC guidelines to comply with GLBA and GDPR and manage personal data efficiently. Financial companies often feature a compliance section on websites to highlight privacy and security commitments.

⁴ "AWS Compliance Programs," AWS website

⁶ "Google Cloud Trust Center," Google website

⁵ "Service Trust Portal," Microsoft website

⁷ "S&P Capital IT Pro," S&P website

Digital trust in action

From breach to trust

In September 2017, Equifax, a consumer credit reporting agency, announced a data breach that exposed the personal information of 147 million people. The company agreed to a global settlement that included up to \$425 million to help people affected by the data breach.

In the years following the data breach, the organization overhauled its security controls, completed rigorous certifications of their programs, and implemented new services to strengthen security. The company has also worked to increase transparency about its efforts regarding improved digital trust.⁸

“We put \$1.5 billion into our security transformation,” explained Jamil Farshchi, CISO, Equifax in a public statement. “Our controls framework was maybe the most important investment of it all. Today, we’re making it available to everyone. For free. It’s the right thing to do, and it’s what’s necessary in order for businesses, government, and society to become more cyber secure.”⁹

⁸ “Equifax Data Breach Settlement,” U.S. Federal Trade Commission, December 2022

⁹ LinkedIn post, Jamil Farshchi, 2022

Corporate commitments to digital trust

In 2022, the 10 largest global companies by revenue went on record with commitments to protect consumer privacy and security.¹⁰

For example, Walmart promised responsible data stewardship and now posts on its website a statement about its ethical use of data and responsible use of technology.¹¹

ServiceNow made similar commitments. “Trust is foundational to everything we do at ServiceNow,” explained Bill McDermott, chairman and CEO. “With our highly secure, agile, cloud infrastructure, ServiceNow provides robust protection to our customers at every moment of their journey. Our continuous monitoring brings peace of mind so customers can focus on what they do best.”¹²

¹⁰ “Data Privacy: A Business Imperative for Boards & Leaders That May Contribute to Market Recovery,” NASDAQ, June 29, 2022











¹¹ “Digital Citizenship: Ethical Use of Data & Responsible Use of Technology,” Walmart website, accessed May 31, 2023

¹² “Partnerships built on trust and transparency,” ServiceNow Trust and Compliance Center

KPMG can help you put your digital trust strategy into action

Here are examples of practical actions you can take to provide transparency and gain digital trust.

KPMG is dedicated to helping you build a dependable digital trust framework. Our team of specialists offers customized support and guidance in crucial areas throughout the process.

- | | | | |
|---|---|---|---|
|  | Identify the appropriate certifications that will help you achieve your digital trust goals |  | Create a custom digital trust strategy for your business and a roadmap with actionable steps to achieve your goals |
|  | Conduct readiness assessments and support you in obtaining certifications and assurance, such as ISO 27001 or SOC 2 |  | Develop an external communication plan to drive brand recognition around trust |
|  | Build a publicly accessible digital trust platform and transparency portal that reflects your unique business requirements |  | Define key risk indicators (KRIs) and key performance indicators (KPIs) that help you measure the success of your digital trust program |
|  | Design and implement controls that help you manage risk while maintaining operational efficiency |  | Identify risks and gaps in your existing digital trust framework and implement measures to address these challenges |
|  | Conduct evaluations and other monitoring activities to help you maintain a high level of security and compliance across your digital trust assets |  | Develop tailored policies, procedures, standards, and playbooks that enable you to maintain high levels of digital trust; provide training around these policies, standards, and expectations |

KPMG can help you in your digital trust journey

- At KPMG, we understand how you feel about the opportunities and challenges of your digital trust journey because we've met them in our own transformation. We know firsthand the importance of creating and retaining stakeholder trust. Our business depends on it.
- Meeting you wherever you are on the journey, we combine deep business, industry, and technical knowledge to integrate risk and regulatory discipline into your digital transformation. As the ultimate business enabler, trust is your ticket to responsible growth, bold innovation, confident decision-making, and sustainable advances in performance.
- We provide a multidisciplinary view of risk, helping you to chart your digital trust journey in alignment with your business goals, regulatory requirements, and customer expectations.

Our commitment to quality, innovation, and collaboration helps ensure that you receive the support you need to build and maintain a digital trust framework that is secure, reliable, and aligned with your strategic business objectives.



Our client commitment



We deliver results that matter.



We know how your business works.



We know how to get things done.



We get the best out of technology.



We're on your side, all the way.

Would you like to learn more?



Talk with your KPMG representative today to learn more about digital trust and its potential benefits to organizations such as yours.



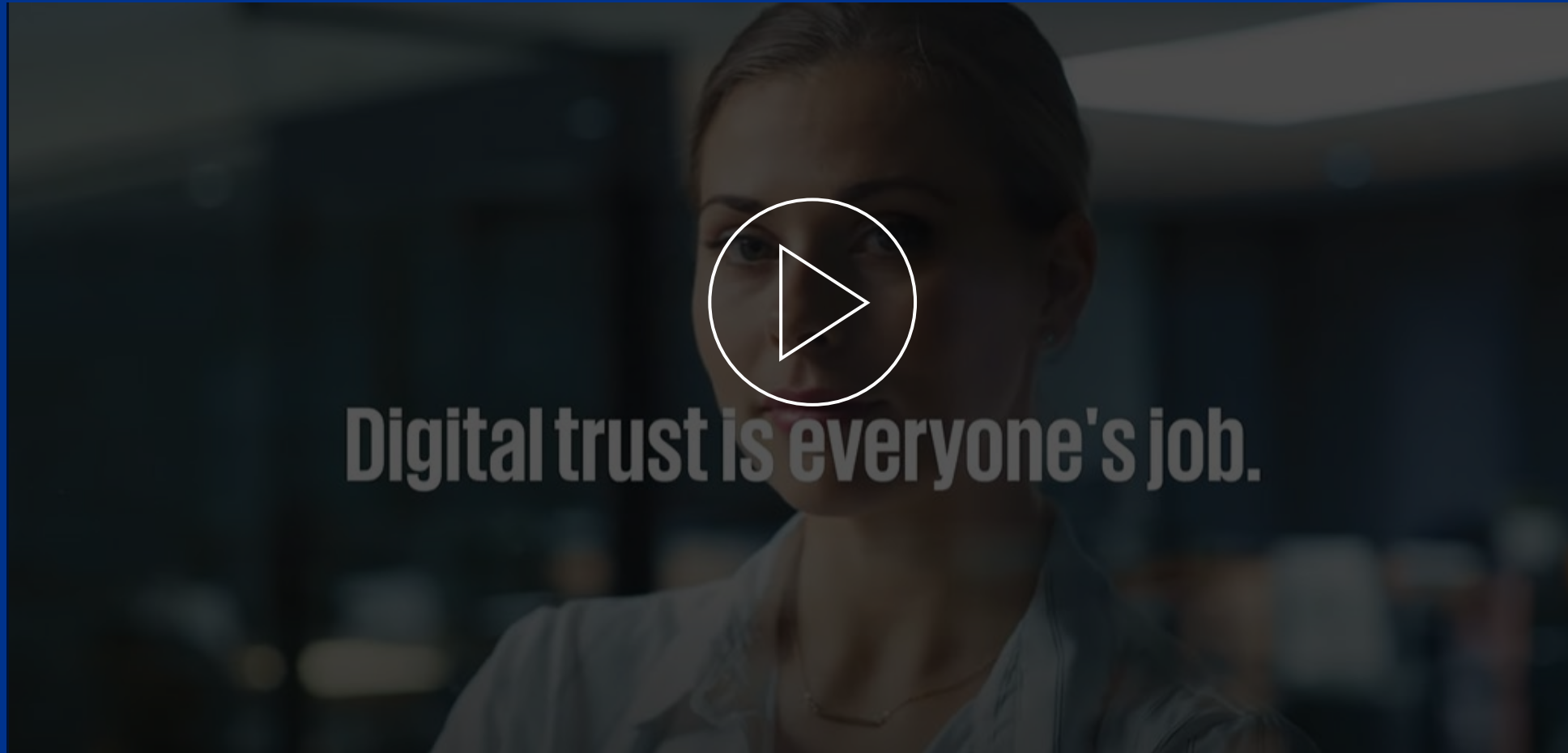
For a detailed overview of recent trends in digital trust, visit our Trusted Imperative website [here](#).



Discover more technology risk insights by visiting our Modern Technology Risk: Centers of Excellence [here](#).



Building digital trust in your organization



Contact us



Beth McKenney

Principal, Technology Risk
KPMG LLP



Lena Buglak

Director, Technology Risk
KPMG LLP



Emily Frolick

Partner, US Trusted Imperative Leader
KPMG LLP



Robert Pizzuto

Director, Technology Risk
KPMG LLP





Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us:



kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS001115-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.