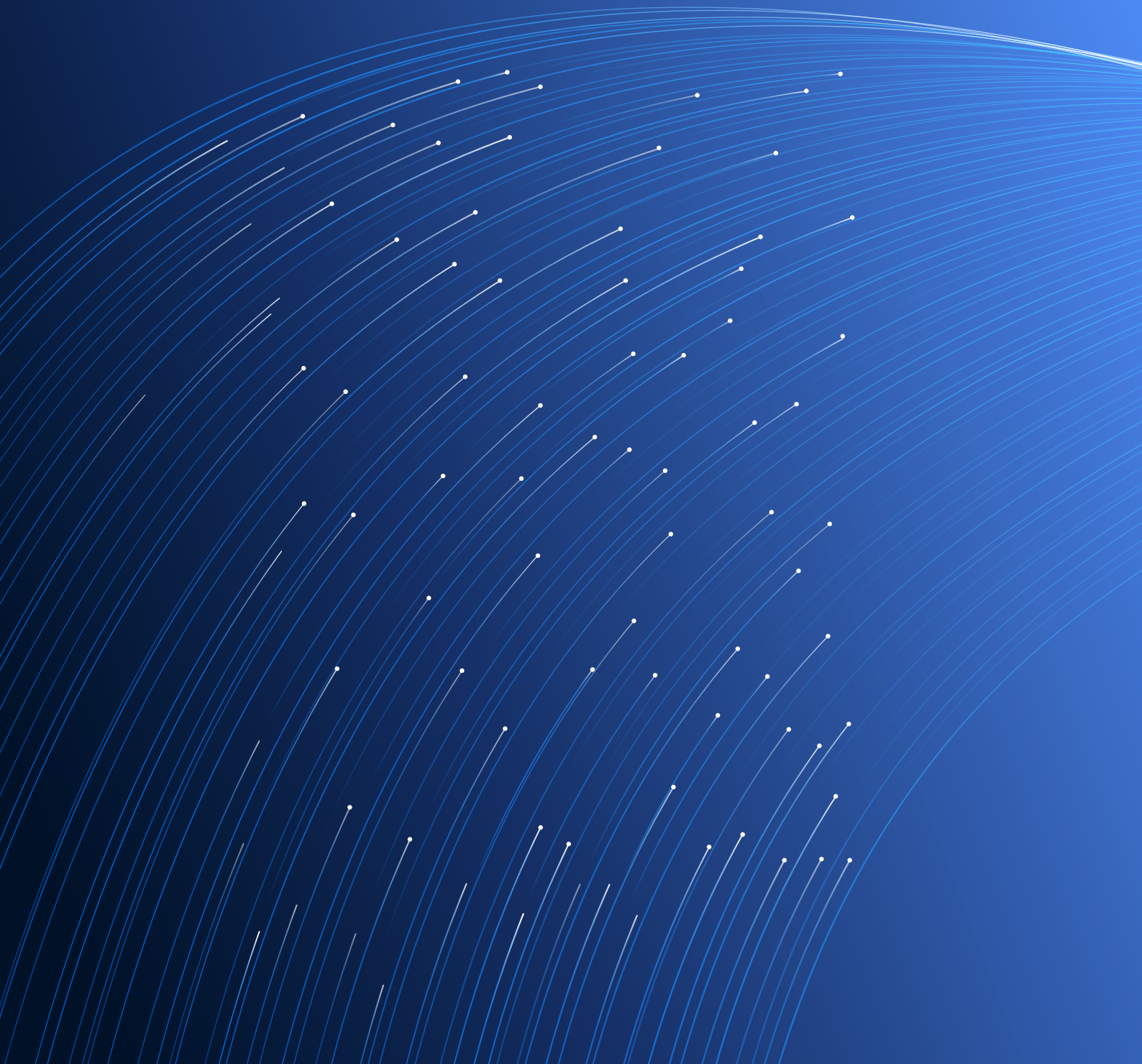
In collaboration
with Accenture

WORLD ECONOMIC FORUM

Measuring Digital Trust: Supporting Decision-Making for Trustworthy Technologies

WHITE PAPER

OCTOBER 2023



Images: Getty Images

Contents

Foreword

Being able to measure digital trust can aid leaders when making decisions regarding trustworthy technologies.

Daniel Dobrygowski
Head, Governance and Trust,
World Economic Forum

David Treat
Senior Managing Director,
Lead, Metaverse Continuum
Business Group, Accenture

A fundamental organizational objective is to have fruitful, long-standing relationships with consumers, clients, employees and partners. In due course, relationship capital can be accrued, which promotes constructive relationships. Translating these concepts to the digital realm is not necessarily straightforward, especially when considering emerging technologies associated with the Fourth Industrial Revolution. How, for example, does an organization successfully translate or build relationships in the Metaverse's immersive environments?[1] How does an organization explore the use of generative artificial intelligence in a trustworthy and responsible manner?[2] There is a need, therefore, for the World Economic Forum's Digital Trust initiative to define general-purpose thought leadership to support leaders in addressing such questions in a trustworthy manner as they seek to develop relationship capital.

Launched in 2021, the Digital Trust initiative set out to establish a global consensus among key stakeholders regarding what digital trust means and what measurable steps can be taken to improve the trustworthiness of digital technologies. This white paper builds upon the Forum's 2022 insight report, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*,[3] which defined digital trust and provided a decision-making framework and a roadmap to help organizations establish a digital trust programme. With digital trust defined as individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values,[4] leaders across sectors and industries have the opportunity and responsibility to make decisions regarding trustworthy technologies that meet and exceed this expectation.

To further support the decision-making process, this report defines how leaders can measure digital trust. It uses the Forum's digital trust framework to point leaders in the right direction and outlines the relevant considerations to aid them when making decisions regarding trustworthy technologies.

Executive summary

This paper defines measures for leaders to be able to evaluate an organization's progress towards digital trust goals and the maturity of digital trust dimensions.

The World Economic Forum's Digital Trust initiative was launched to establish a global consensus among key stakeholders regarding what digital trust means and what measurable steps can be taken to improve the trustworthiness of digital technologies. Subsequently, digital trust has been defined as individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.[5]

The Forum's digital trust framework is a tool to guide leaders as they make decisions and navigate how to earn digital trust.[6] This tool can help them as they seek to measure their organization's progress towards digital trust goals and assess the maturity of digital trust dimensions. Measures towards digital trust goals are intended to examine the extent to which an organization's relationship with an actor (whether an individual or an organization) is strong and resilient in accordance with the digital trust framework's goals: security and reliability; accountability and oversight; and inclusive, ethical and responsible use. These measures are subjective, retrospective and based on external perceptions and behaviour associated with an organization's digital products or services.

When measuring the maturity of an organization's digital trust dimensions, the aim is to evaluate the extent to which the organization has proper governance in place to fulfil an individual or organization's expectations in accordance with the digital trust framework's dimensions of decision-making: cybersecurity; safety; transparency; interoperability; auditability; redressability; fairness; and privacy. In contrast to progress towards the digital trust goal measures, the maturity of digital trust dimension measures examine the internal objectives and capabilities of an organization's digital trust programme. These measures are objective and prospective.

This white paper and its measures are primarily meant for organizational leaders, but could also be useful for regulators, investors, watchdogs and the like. The measures summarized in the paper could spur the subsequent creation of digital trust maturity models, benchmarking or certification. To that end, the Forum and the International Organization for Standardization (ISO) are engaged in further developing measures to support digital trust, as discussed in this paper.

While such measures are not necessarily a cure-all and are not without limitations, they are an important next step for leaders on their journey to earning digital trust. And to aid them in this endeavour, the Digital Trust Initiative's website[7] provides supplemental materials that can support leaders as they translate the measures highlighted in this report for their own organization.

Introduction

The Forum's digital trust framework aims to guide organizational leaders as they determine how best to earn digital trust.

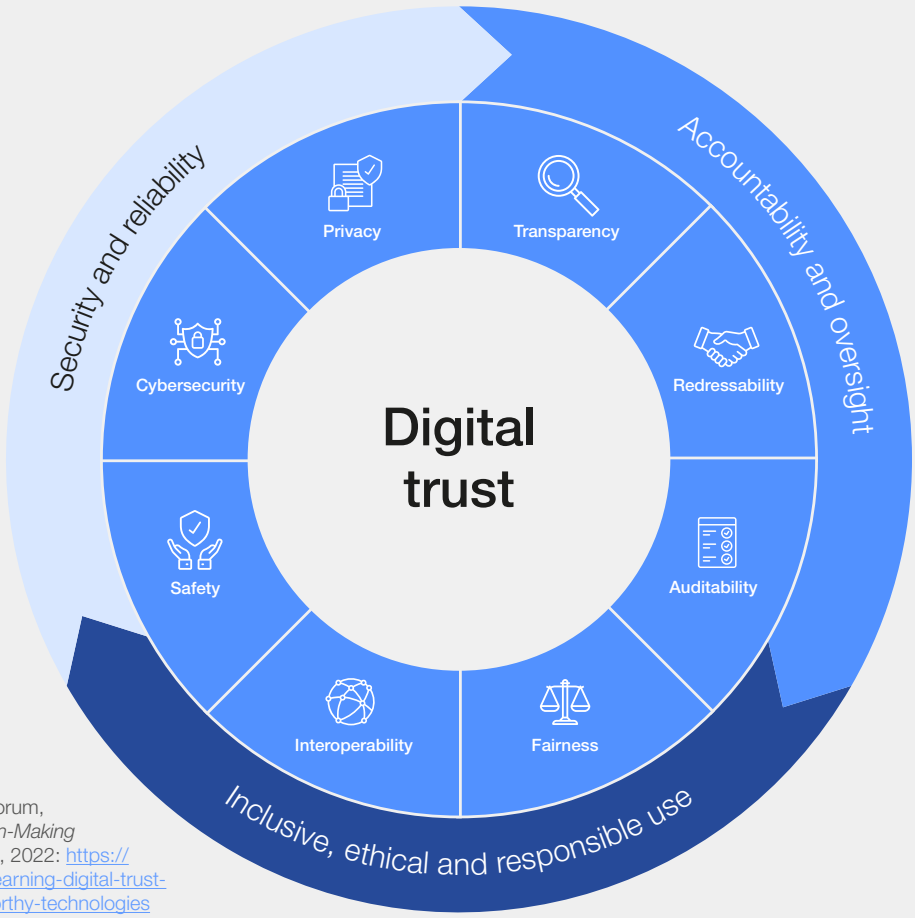
Broadly, measures are discrete values that enable comparisons to be drawn.[8] In an organizational setting – where leaders across sectors and industries are responsible for the decisions that develop trustworthy technologies – measures can both inform decision-making and act as indicators of the success of decision-making.

The World Economic Forum defines digital trust as "individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values".[9]

To that end, the Forum's digital trust framework (see Figure 1), with its goals and dimensions of digital trust decision-making, serves as a tool to guide organizational leaders exploring how best to earn digital trust.[10] Digital trust goals are considerations that motivate or can be achieved by actions or decisions (i.e. dimensions).[11] Digital trust dimensions are the aspects of digital trust over which organizational decision-makers, such as CEOs and senior executives, have control and which, if applied to a given technology with a human-centric approach, will promote digital trustworthiness.[12]

> **Digital trust is individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.**

FIGURE 1 **Digital trust framework**



Source: World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies

This white paper's contribution is to propose universally applicable measures – discrete values that enable comparison— that are in accordance with the Forum's digital trust framework. What follows are summaries of objects of study to measure both an organization's progress towards digital trust goals (i.e. the extent to which an organization's relationship with an actor – whether an individual or an organization – is strong and resilient) and the maturity of digital trust dimensions (i.e. the extent to which an organization has the proper governance in place to fulfil an individual or organization's expectations). The former measures are subjective, retrospective and based on external perceptions and behaviour associated with an organization's digital products or services; in contrast, the latter measures are objective and prospective as they examine the internal objectives and capabilities of an organization's digital trust programme.

Leaders are encouraged to monitor these measures to allow comparisons to be drawn – say, given an organization's industry, ecosystem or geography – and enable subsequent decision-making – regarding investment allocation, for example. Ongoing monitoring that seeks continuous improvement can inform long-standing, trusted relationships, whether in a business-to-consumer, business-to-business or even a business-to-business-to-consumer context.[13] In addition to organizational leaders, these measures could be useful to regulators, investors, watchdogs and others. Table 1 describes the measures summarized in this report.

TABLE 1 **Summary of measures**

	Progress towards digital trust goals	Maturity of digital trust dimensions
Summary	The extent to which an organization's relationship with an actor (whether an individual or an organization) is strong and resilient	The extent to which an organization has the proper governance in place to fulfil an individual or organization's expectations
Focus area	Organization's digital products or services	Organization's digital trust programme
Object of study	Perceptions and behaviour associated with an organization's digital products or services	Objectives and capabilities of an organization's digital trust programme
Relation to framework	Digital trust goals (i.e. security and reliability; accountability and oversight; inclusive, ethical and responsible use)	Digital trust dimensions (i.e. cybersecurity; safety; transparency; interoperability; auditability; redressability; fairness; privacy)
Qualities	Subjective, retrospective	Objective, prospective

The effort that defined the measures outlined in this paper was inspired by the Forum's previous work on defining Stakeholder Capitalism Metrics.[14,15] The following tenets specifically informed the measures reported below:

Well-established and verifiable

- The measures were sourced from an interdisciplinary set of digital trust leaders and experts from across industries (including leading technology innovators), governments, regulators and academic institutions, as well as citizen and consumer advocates, who drew on their expertise in privacy, cybersecurity, technology ethics, law and a variety of other fields to define the measures presented in this report
- The measures were selected for:
  - Universality across industries and business models
  - Feasibility to be monitored and reported
  - Capability of verification and assurance while also being understandable for a range of stakeholders (e.g. leaders, consumers, regulators, investors) according to their needs and levels of expertise
- Notably, the measures are not intended to replace relevant sector-specific or company-specific indicators

Complementary and Illustrative

- Measures are considered beyond regulatory requirements, which can vary according to jurisdiction. The universally relevant measures summarized below are:
  - Indicative of best practices
  - Not intended to act as an exhaustive list
- The examples, while broadly applicable, may be defined uniquely according to sector and industry and thus leaders are encouraged to build upon them in ways that are most suitable for their organization

Programmatic and mature

- Measures evaluate an organization's digital trust programme, which governs its digital products

or services. The measures highlighted in this report are intended to gauge the maturity of an organization's digital trust programme, including its established objectives and capabilities, and the external interpretation of an organization's digital trust efforts. Generally, the measures seek to indicate the quality of a digital trust programme, in either absolute or relative terms, as appropriate, thanks to underlying data that is ideally collected in an ongoing manner

– For additional details on how to establish a Digital Trust programme, please see this Initiative's *Pre-Implementation Briefing Paper*[16]

Existing measures can provide a useful foundation for measures associated with progress towards digital trust goals and the maturity of digital trust dimensions. Generally, surveys have shown that investment in the dimensions of digital trust (e.g. privacy or cybersecurity) have translated into better consumer perception in the market.[17] Specifically, many organizations use existing measures to evaluate an individual's perception of an organization (e.g. net promoter score) and an individual's behaviour (e.g. impressions and clicks) as they interact with an organization's digital products or services. Additionally, the publication of research and rankings performed by research firms (e.g. Gartner, or Edelman) in relation to digital trust could also be useful to leaders as they assess market dynamics more broadly (e.g. emerging technology adoption, corporate citizenship, and cybersecurity scorecards). Examining such measures in relation to the goals of digital trust as defined in the World Economic Forum's framework (e.g. security and reliability; accountability and oversight; and inclusive, ethical and responsible use) can help an organization understand how these factors are externally interpreted. Therefore, such measures could be repurposed to indicate the amount of trust an individual or organization has in an organization, with improvements in such measures serving as indicators of increased trust.

As for the maturity of digital trust dimensions, there are existing measures associated with these topics, many of which are reported below. However, such measures are not necessarily typically evaluated in relation to each other. When seeking to earn digital trust and promote digital trustworthiness, leaders are encouraged to take a comprehensive approach to the study of the goals and dimensions of digital trust decision-making.

Before summarizing the relevant measures, it is worthwhile noting existing efforts. The Swiss Digital Initiative's Digital Trust Label for consumers denotes the trustworthiness of a digital service in clear, plain, non-technical, easily understandable language that is matched with a visual indicator of certification.[18] For professionals, ISACA has broadened its professional credential offering to include considerations of digital trust, informed by insights from its research on the topic.[19] These developments are significant steps forward in promoting digital trust.

The following sections highlight universally relevant measures. The measures summarized in this report are not a complete model, but instead lay the foundation for future work that will continue to define the necessary building blocks to help support leaders as they seek to earn digital trust. The examples given below, while believed to be broadly applicable, may be adjusted or augmented according to the sector and industry. Leaders are encouraged to build upon these examples in ways that are most suitable for their organization. Supplemental materials that can aid leaders as they translate the measures highlighted in this report for their own organization can be found on the Digital Trust Initiative's website.[20]

1 Measuring progress towards digital trust goals

These measures are subjective and retrospective, and assess the strength and resilience of an organization's relationship with an actor in line with the digital trust framework's goals.

When calibrating an organization's progress towards digital trust goals, measures examine the extent to which an organization's relationship with an actor (whether an individual or an organization) is strong and resilient in accordance with the digital trust framework's goals: security and reliability; accountability and oversight; and inclusive, ethical and responsible use. When a relationship is called into question, leaders face a *moment of truth*, an opportunity to strengthen their relationship or a situation where they may fail to do so; the measures aid decision-makers to focus on dimensions that can repair breaches of trust. These measures are subjective and retrospective. They are indicative of a relationship and can be evaluated according to the perceptions as well as the behaviour of individuals, such as customers, employees and other stakeholders. While this paper is primarily focused on consumer trust of an organization, trust in an employee-to-organization or organization-to-organization context could potentially leverage similar concepts.

As summarized in Table 2, perception measures that could be collected by survey assess the following concepts: satisfaction; feedback; confidence; loyalty; enthusiasm; and comprehension of data flow. The last concept seeks to address the risk of mistrust if a user trusts but does not fully understand the data flows associated with an organization's products or services. Behavioural measures that could be collected during use of an organization's digital products or service could assess: adoption; engagement; retention; and promotion. In particular, engagement behaviour could include examining a user's activity regarding privacy settings and actioning opportunities for redress, as privacy and redress are key dimensions of an organization's digital trustworthiness. Examining such measures in relation to the goals of digital trust as defined in the Forum's framework (i.e. security and reliability; accountability and oversight; and inclusive, ethical and responsible use) can help an organization understand how such factors, promoted by the organization's digital trust efforts, are externally interpreted. Therefore, such measures could be repurposed to indicate the amount of trust an individual or organization has towards an organization, and improvements in such measures would serve as indicators of increased trust.

TABLE 2 **Progress towards digital trust goal measures**

Progress towards digital trust goals The extent to which an organization's relationship with an actor (whether an individual or an organization) is strong and resilient.	
Perception measures:	**Behavioural measures:**
Satisfaction	Adoption
Feedback	Engagement (e.g. user setting and support activity)
Confidence	Retention
Loyalty	Promotion
Enthusiasm	
Comprehension of data flow	

2 Measuring the maturity of digital trust dimensions

These measures are objective and prospective, and evaluate an organization's governance in line with the digital trust framework's decision-making dimensions.

When measuring the maturity of an organization's digital trust programmes, the aim is to evaluate the extent to which the organization has the proper governance in place to fulfil an individual or organization's expectations in accordance with the digital trust framework's dimensions of decision-making: cybersecurity; safety; transparency; interoperability; auditability; redressability; fairness; and privacy. These measures are objective, prospective and based on the internal objectives and capabilities of an organization's digital trust programme. They indicate the relevant characteristics that suggest another party can be trusted.

The following subsections define suggested measures according to the dimensions of the Forum's digital trust framework (listed in the same order as the Digital Trust initiative's insight report; this order is not meant to suggest an order of importance). Within each dimension, the relevant programmatic objectives are illustrated with a sampling of pertinent capabilities. Furthermore, these governance mechanisms can be measured in terms of their effectiveness. However, such effectiveness measures would be unique according to the organization's sector and industry and thus leaders are encouraged to build upon these best practices in ways that are most suited to their organization.

2.1 Cybersecurity

Cybersecurity focuses on the security of digital systems – including the underlying data, technologies and processes. Effective cybersecurity mitigates the risk of unauthorized access and damage to digital processes and systems, ensuring resiliency. It also ensures the confidentiality, integrity and availability of data and systems.[21] As summarized in Table 3, measures conveying the governance of cybersecurity, as encapsulated in an organization's cybersecurity programme, are widely understood to address two objectives: 1) incident prevention; and 2) incident response. Programmatic cybersecurity capabilities in support of a prevention objective include the security of accounts, devices, networks, infrastructure, data and software, while capabilities regarding the incident response objective include planning, detection, recovery and investigations.

TABLE 3 **Measures of a programme's cybersecurity maturity**

Cybersecurity Cybersecurity focuses on the security of digital systems – including the underlying data, technologies and processes. Effective cybersecurity mitigates the risk of unauthorized access and damage to digital processes and systems, ensuring resiliency. It also ensures the confidentiality, integrity and availability of data and systems.[22]	
Objective: Incident prevention	**Objective: Incident response**
Capability:	**Capability:**
Account security	Incident response planning
Infrastructure and device security	Predefined goals for recovery point objective (RPO) and recovery time objective (RTO)
Network and data security	Detection and analysis
Application and software security	Containment, eradication and recovery
	Investigation and forensics

2.2 Safety

Safety encompasses efforts to prevent harm (e.g. emotional, physical or psychological) to people or society from technology uses and data processing.[23] Similar to cybersecurity, the safety objectives of a digital trust programme would include incident prevention efforts as well as incident response objectives, as outlined in Table 4.

For preventative objectives, the corresponding capabilities could include: safety training; new product or service assessments; quality-control procedures; user guidelines; and threat modelling and mitigation – all of which contribute to identifying and minimizing the likelihood and impact of safety threats. Notably, in a business-to-business context, such due diligence could include considering who could have access to the product or service, how it could be abused and what controls are in place to mitigate the risk of abuse. And for safety incident response objectives, capabilities could also include incident response planning and corrective actions to ensure that those harmed are made whole. Please note that measures associated with externally reported trust and safety issues (e.g. consumer or user reported issues) will be documented below in the redressability subsection. More information on digital safety can be found on the World Economic Forum's Global Coalition for Digital Safety website, which includes global principles and a risk assessment framework.[24]

TABLE 4 | **Measures of a programme's safety maturity**

Safety Safety encompasses efforts to prevent harm (e.g. emotional, physical or psychological) to people or society from technology uses and data processing.[25]	
Objective: Incident prevention	**Objective: Incident response**
Capability:	**Capability:**
Safety training (e.g. escalation routes, evacuation exercise)	Incident response planning
New product or service assessment	Corrective action
Quality control	
User guidelines	
Threat modelling and mitigation	

2.3 Transparency

Transparency requires honesty and clarity around digital operations and uses. Enabling visibility into an organization's digital processes reduces the information asymmetry between an organization and its stakeholders while signalling to individuals that the organization intends not only to act in the individual's interests but also to make those actions known and understandable to those inside and outside of the organization.[26] While transparency, in the form of product labelling or other reporting requirements, is often well-defined in regulations governing jurisdictions and industries, when seeking to earn digital trust, organizational leaders' objective should be to go beyond such requirements and take a proactive approach to transparency. This could include communicating relevant information about vendors or third parties and associated data flows.

With that in mind, the programmatic transparency objectives of a digital trust programme could include: 1) appropriate disclosure; and 2) informative disclosure, as seen in Table 5. Regarding the former, defining a process that governs where, when and to whom to disclose additional information, as well as the level of detail provided, will help to ensure that additional transparency supports the other dimensions of digital trust. For example, contributing code to the open-source community is a way to demonstrate transparency as well as interoperability and earn digital trust (a topic discussed further in the interoperability subsection that follows), while on the other hand, inappropriate additional disclosure could undermine cybersecurity and safety efforts to protect users from harm. With regard to capabilities to ensure that additional disclosure is indeed informative, such capabilities could entail translating content for specific audiences, creating engaging content and giving consumers the information and the ability to submit questions and provide feedback (which is related to the digital trust dimension of redressability discussed below).

TABLE 5 | **Measures of a programme's transparency maturity**

Transparency Transparency requires honesty and clarity around digital operations and uses. Enabling visibility into an organization's digital processes reduces the information asymmetry between an organization and its stakeholders while signalling to individuals that the organization intends not only to act in the individual's interests but also to make those actions known and understandable to those inside and outside of the organization.[27]	
Objective: Appropriate disclosure	**Objective: Informative disclosure**
Capability:	**Capability:**
Decision-making process to determine any additional disclosure beyond requirements (e.g. legal and compliance) regarding where, when and to whom, and the level of detail provided	Translation of content according to audience (e.g. consumer FAQ, developer blog post)
	Engaging presentation
	Ability to submit questions upon reading the disclosure and provide feedback

2.4 Interoperability

Interoperability is the ability of information systems to connect and exchange information for mutual use without undue burden or restriction.[28] A digital trust programme's interoperability objectives will focus on technical interoperability (e.g. data interoperability and platform interoperability) and community participation and engagement, as summarized in Table 6. Notably, data interoperability enables individual data portability, which allows data access requests to be fulfilled. And for community participation and engagement, the organization's ecosystem efforts with respect to standards, open-source code and application programming interfaces (APIs) could be evaluated. Such interoperability efforts, namely open-source software, have been found not only to be cost-saving but also to enable faster development speed.[29]

TABLE 6 **Measures of a programme's interoperability maturity**

Interoperability Interoperability is the ability of information systems to connect and exchange information for mutual use without undue burden or restriction.[30]	
Objective: Technical interoperability	**Objective: Community participation and engagement**
Capability:	**Capability:**
Data interoperability, including individual data portability	Participation in standard-setting
Platform interoperability	Use of standards in technology design, governance process, etc.
	Open-source contributions and use
	Developer relations
	Exposure of and usage of APIs

2.5 Auditability

Auditability is the ability of both an organization and third parties to review and confirm the activities and results of technology, data processing and governance processes. Auditability serves as a check on an organization's commitments and signals its intent to follow through on those commitments.[31] As seen in Table 7, a digital trust programme's auditability objectives seek to ensure that all internal as well as independent, external audit procedures are sound and therefore assess: 1) the process; and 2) the remediation. Regarding the audit's process objectives, planning and scoping of the subject of the audit need to be appropriate to ensure the audit is targeting the most high-risk areas. And with respect to the remediation objectives, defining the accountability structure – such as roles and responsibilities, timeline and milestones as well as functionality for monitoring and ongoing improvement – can support efforts to have an audit remediated in a timely manner while seeking to have minimal repeat audit findings.

TABLE 7 | **Measures of a programme's auditability maturity**

Auditability Auditability is the ability of both an organization and third parties to review and confirm the activities and results of technology, data processing and governance processes. Auditability serves as a check on an organization's commitments and signals its intent to follow through on those commitments.[32]	
Objective: Effective process	**Objective: Effective remediation**
Capability:	**Capability:**
Planning: scheduling, setting roles/responsibilities	Assigning roles and responsibilities
Scoping of the audit subject so as to target the most high-risk areas	Timeline and milestones
	Monitoring
	Ongoing improvement

2.6 Redressability

Redressability represents the possibility of obtaining recourse where individuals, groups or entities have been negatively affected by technological processes, systems or data uses. With the understanding that unintentional errors or unexpected factors can cause unanticipated harms, trustworthy organizations have robust methods for redress when recourse is sought and mechanisms in place to make individuals whole when they have been harmed.[33] As seen in Table 8, the objectives of a digital trust programme in terms of redressability include both providing user-friendly support and incorporating user feedback. Regarding user-friendly support, capabilities could include self-service, multiple modes of support and predefined escalation paths. And with respect to user feedback, capabilities could include having a process in place to review support ticket themes (i.e. identify which issues are recurring), organizational personnel designated as user advocates in relevant product or service design meetings, and regular improvements made in response to support tickets. By measuring both user-friendly support and incorporation of user feedback, an organization endeavouring to earn digital trust will seek to ensure there is a consistent ebb and flow between these two objectives.

TABLE 8 | **Measures of a programme's redressability maturity**

Redressability Redressability represents the possibility of obtaining recourse where individuals, groups or entities have been negatively affected by technological processes, systems or data uses. With the understanding that unintentional errors or unexpected factors can cause unanticipated harms, trustworthy organizations have robust methods for redress when recourse is sought and mechanisms in place to make individuals whole when they have been harmed.[34]	
Objective: User-friendly support	**Objective: Incorporation of user feedback**
Capability:	**Capability:**
Self-service	Review process of support ticket themes (i.e. identify recurring issues)
Multiple modes of support functionality (e.g. phone, chat, email)	User advocates in relevant product or service design meetings
Predefined escalation paths	Regular improvements made in response to support tickets

2.7 Fairness

Fairness requires that an organization is aware of the potential for technology and data processing to have a disparate impact and that it aims to achieve just and equitable outcomes for all stakeholders, given the relevant circumstances and expectations.[35] As such, programmatic fairness objectives could include both procedural and outcome fairness considerations, as seen

in Table 9. Procedural fairness objectives would govern the fairness of a digital product or service as a whole, and could include capabilities such as new digital products or service assessments, periodic reviews of digital products or services and documentation of corresponding fairness decisions. Notably, such assessments and reviews are encouraged to assess the context in which a digital product or service exists, as fairness considerations are sensitive to context and it is therefore important to understand how a digital product or service is one piece of a larger puzzle. Outcome fairness objectives would include evaluations of new features prior to deployment, bias assessment of a dataset or model, and documentation of corresponding fairness decisions.

TABLE 9 **Measures of a programme's fairness maturity**

Fairness Fairness requires that an organization is aware of the potential for technology and data processing to have a disparate impact and that it aims to achieve just and equitable outcomes for all stakeholders, given the relevant circumstances and expectations.[36]	
Objective: Process fairness	**Objective: Outcome fairness**
Capability:	**Capability:**
New digital products or service assessments (e.g. inclusivity and accessibility, contextual considerations)	Evaluations of new features prior to deployment
Periodic reviews of digital products or services	Bias assessment (e.g. equality, equity) of a dataset or model
Documentation of corresponding fairness decisions	Documentation of corresponding fairness decisions

2.8 Privacy

Privacy, for individuals, is the expectation of control over or confidentiality of their personal or personally identifiable information. For organizations, privacy is the meeting of this expectation through the design and manifestation of data processing that facilitates individual autonomy through notice and control over the collection, use and sharing of personal information.[37] As seen in Table 10, programmatic privacy objectives could seek to support users as well as organizational personnel. User functionality could include frequently asked questions (FAQs) associated with privacy policies, an engaging consent process, optionality in user settings and management of intellectual property in addition to personal data. Organizational personnel support capabilities could include privacy impact assessments (which could include considerations of contextual privacy expectations), privacy by design assessments and escalation procedures.

TABLE 10 **Measures of a programme's privacy maturity**

Privacy Privacy, for individuals, is the expectation of control over or confidentiality of their personal or personally identifiable information. For organizations, privacy is the meeting of this expectation through the design and manifestation of data processing that facilitates individual autonomy through notice and control over the collection, use and sharing of personal information.[38]	
Objective: User functionality	**Objective: Organizational functionality**
Capability:	**Capability:**
FAQs associated with privacy policies	Privacy impact assessments, including considerations of contextual privacy expectations
Engaging consent process	Privacy by design assessments
Optionality in user settings, including data access requests	Escalation procedures
Management not only of personal data but also intellectual property	

Conclusion

The measures summarized in this paper are primarily meant for organizational leaders as they take a comprehensive approach to earning digital trust.

Leaders are encouraged to use the methodologies outlined above, which highlight the relevant objects of study, to measure an organization's progress towards digital trust goals and the maturity of digital trust dimensions, according to the World Economic Forum's digital trust framework. By assessing these measures on an ongoing basis as part of a continuous improvement process inherent to an organization's digital trust programme, leaders can understand how their programmatic decisions contribute to earning digital trust and maintaining long-standing relationships.

The measures summarized in this white paper could spur further development in the field, to potentially inform maturity models, benchmarking or certification. To that end, the Forum and ISO are engaged in further establishing measures to support digital trust, as discussed in this paper. While such measures are not a cure-all and are not without limitations – including concerns about mistrust and how perception can differ from reality – this paper defines an important next step for leaders as they seek to earn digital trust and fulfil the old adage that what gets measured gets managed.

Further information can be found on the Digital Trust Initiative's website, which provides supplemental materials that can aid leaders as they translate the measures highlighted in this paper to their own organizations.[39]

Contributors

Lead Author

Amanda Stanhaus
Project Fellow, Digital Trust Initiative, World Economic Forum; Responsible Metaverse Manager, Metaverse Continuum Business Group, Accenture

World Economic Forum

Daniel Dobrygowski
Head, Governance and Trust

Cathy Li
Head, AI, Data and Metaverse; Member of the Executive Committee

Hesham Zafar
Lead, Digital Trust Initiative

Digital Trust Initiative Project Advisers

Sean Joyce
Global Cybersecurity and Privacy Leader, US Cyber, Risk and Regulatory Leader, PwC

David Treat
Senior Managing Director, Lead, Metaverse Continuum Business Group, Accenture

Akhilesh Tuteja
Global Cyber Security Practice Leader, KPMG

Digital Trust Initiative Fellows

Margarita Gorospe
Project Fellow, Digital Trust Initiative, World Economic Forum; Associate, PwC

Helena Kotschenreuther
Project Fellow, Digital Trust Initiative, World Economic Forum; Cyber Strategy and Risk, KPMG

Jake Meek
Project Fellow, Digital Trust Initiative, World Economic Forum; Director, PwC

Augustinus Mohn
Project Fellow, Digital Trust Initiative; Cyber Strategy and Risk, KPMG

Toby Spry
Executive Fellow, Digital Trust Initiative, World Economic Forum; Principal, Data Risk and Privacy, PwC

Kathryn White
Executive Fellow, Digital Trust Initiative, World Economic Forum; Responsible Metaverse Lead, Metaverse Continuum Business Group, Accenture

Annemarie Zielstra
Executive Fellow, Digital Trust Initiative, World Economic Forum; Partner, Cybersecurity, KPMG

Digital Trust Initiative Community

This report would not have been possible without the support of the Forum's broader digital trust community.[40]

Acknowledgements

The initiative team would like to especially thank the following key contributors for their generosity in the form of time, attention, and insights throughout 2023 that made this report possible: Chloe Autio (The Cantellus Group), Jenny Brinkley (Amazon), Ravi Shankar Chaturvedi (Tufts University), Natasha Crampton (Microsoft), Jill Crisman (Underwriters Laboratories), Kaje De Leon (Coca-Cola), Nicolas Fischbach (Google), Francisco Fraga (McKesson), Liz Grennan (McKinsey), Vera Heitmann (IKEA), Kai Hermsen (Twinds), Randy Herold (ManpowerGroup), Desiree Lee (Armis), Rachel Matthews (Callsign), Jutta Juliane Meier (Identity Valley), Iwona Muchin (Ageas), Philipp Raether (Allianz), Karen Silverman (The Cantellus Group), Lynn Simons (Salesforce), Jacob Springer (Abbott), Sridhar Sriram (Microsoft), Alissa Starzak (Cloudflare), Cyrus R. Vance Jr (Baker McKenzie), Nicolas Zahn (Swiss Digital Initiative), Shahar Ziv (PayPal).

An additional thank you to the following individuals for their contributions to this effort, including in the forms of subject matter expertise and diligent review: Emily Bayley (World Economic Forum), Stella Ljung (Accenture), Chris McClean (Avanade), Maeve Miller (Accenture), Cassidy Novello (Accenture), Lara Pesce Ares (Accenture) and Anna Schilling (Accenture).

Production

Laurence Denmark
Creative Director, Studio Miko

George Messer
Designer, Studio Miko

Ali Moore
Editor, Astra Content

Endnotes

1. World Economic Forum, *Metaverse Privacy and Safety*, July 2023: https://www3.weforum.org/docs/WEF_Metaverse_Privacy_and_Safety_2023.pdf.
2. World Economic Forum, *The Presidio Recommendations on Responsible Generative AI*, June 2023: https://www3.weforum.org/docs/WEF_Presidio_Recommendations_on_Responsible_Generative_AI_2023.pdf.
3. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, November 2022: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
4. Ibid.
5. Ibid.
6. Ibid.
7. World Economic Forum, "Digital Trust Initiative": https://initiatives.weforum.org/digital-trust/about.
8. International Bureau of Weights and Measures' Joint Committee for Guides in Metrology, *International Vocabulary of Metrology – Basic and General Concepts and Associated Terms (VIM)*, 3rd edition, 2006: https://www.nist.gov/system/files/documents/pml/div688/grp40/International-Vocabulary-of-Metrology.pdf.
9. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, November 2022: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
10. Ibid.
11. Ibid.
12. Ibid.
13. Tripathi, Nitisha, Jose Pablo Ampudia, Emmy Peng, Shuqi Ding and Jian Gu, *Incentivizing Trustworthy Technologies*, 2023: https://www.sipa.columbia.edu/sites/default/files/2023-05/For_Publication_SAP_Daniel%20Dobrygowski%281%29.pdf.
14. World Economic Forum, *Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation*, September 2020: https://www3.weforum.org/docs/WEF_IBC_Measuring_Stakeholder_Capitalism_Report_2020.pdf.
15. Please note, the measures documented in this report are not necessarily related to these ESG metrics.
16. World Economic Forum, *World Economic Forum Digital Trust Initiative*, June 2023: https://media.licdn.com/dms/document/media/D561FAQGQ-MOe9-Jo5Q/feedshare-document-pdf-analyzed/0/1689789112216?e=1690416000&v=beta&t=lH_frX-bvlV43nAp5XglXA8VXbD6Q2j4ojBM7FUHBW0.
17. Sabin, Sam, "Finance, Retail Sectors Reap Data Privacy Wins in Harris Poll", Axios, 26 May 2023: https://www.axios.com/2023/05/26/data-privacy-harris-poll-chase-apple.
18. Swiss Digital Initiative, "A Commitment to Digital Responsibility": https://www.swiss-digital-initiative.org/digital-trust-label/.
19. ISACA, "In Pursuit of Digital Trust", 2023: https://www.isaca.org/digital-trust.
20. World Economic Forum, "Digital Trust Initiative": https://initiatives.weforum.org/digital-trust/about.
21. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, November 2022: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
22. Ibid.
23. Ibid.
24. World Economic Forum, "A Global Coalition for Digital Safety": https://initiatives.weforum.org/global-coalition-for-digital-safety/home.
25. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, November 2022: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
26. Ibid.
27. Ibid.
28. Ibid.
29. The Linux Foundation, "The Value of Open Source Software Is More than Cost Savings", 7 March 2023: https://www.linuxfoundation.org/blog/the-value-of-open-source-software-is-more-than-cost-savings.
30. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, November 2022: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
31. Ibid.
32. Ibid.
33. Ibid.
34. Ibid.
35. Ibid.
36. Ibid.
37. Ibid.
38. Ibid.
39. World Economic Forum, "Digital Trust Initiative": https://initiatives.weforum.org/digital-trust/about.
40. World Economic Forum, "The Digital Trust Community": https://initiatives.weforum.org/digital-trust/community.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org

START YOUR FINANCE

起点财经，网罗天下报告