World Economic Forum Digital Trust Initiative

IMPLEMENTATION WORKSTREAM
PRE-IMPLEMENTATION BRIEFING PAPER

JUNE 2023

Images: Getty Images

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Introduction

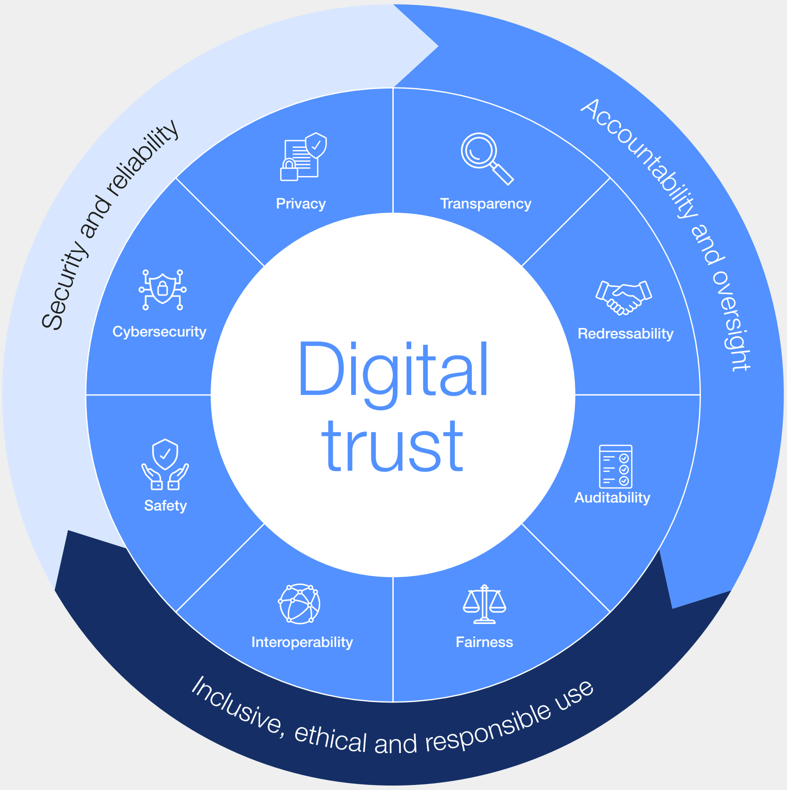
Taking digital trust from conceptual to operational – demonstrating a commitment to responsible digital practices.

Embedded, ubiquitous and continually evolving – digital technologies underpin nearly every aspect of modern society. By designing and deploying these capabilities, organizations play an outsized role in how commerce, communications and social connection take place in today's world.[1] For many across the globe, this trend is not an optimistic one.[2] The erosion of trust in society combined with the pace of innovation perpetuates feelings of distance between end-user and provider.[3] This trust gap feels inescapable. How is it possible to reverse this trend and promote a society underpinned by **trusted** technology and innovation?

The World Economic Forum brought together over 60 specialists and leaders across privacy, cybersecurity, data ethics, law and other disciplines to define a path forward for trust in the digital age.[4] This effort – organized as the World Economic Forum Digital Trust Initiative – draws upon the experience of its contributors to design a global framework for digital trust comprised of eight operating dimensions in service to three overarching goals – security and reliability, accountability and oversight, and inclusive, ethical and responsible use.[5]

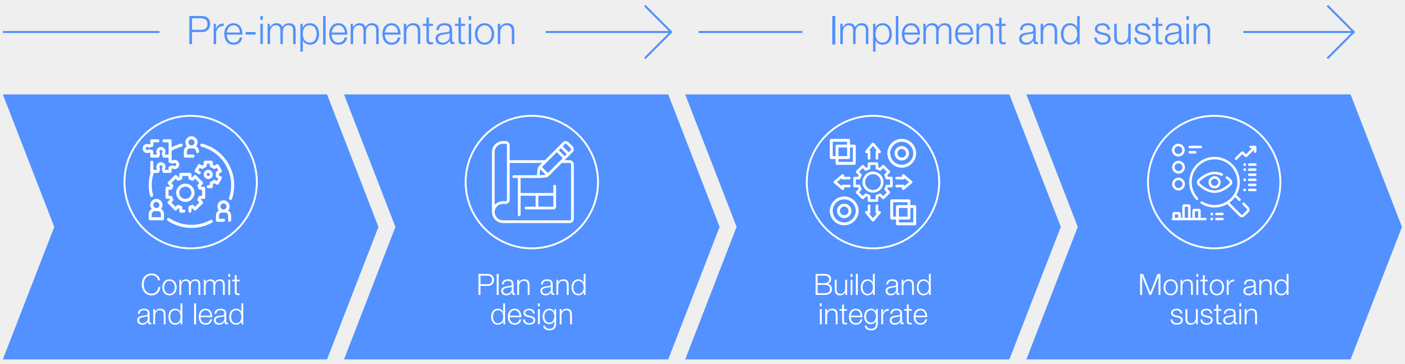
With the framework completed, the Forum turned its attention to the steps necessary to implement digital trust within organizational strategies, operating models and frontline capabilities. The initiative is now defining a roadmap to advance digital trust from conceptual to operational.

FIGURE 1 **Digital trust framework**



Source: World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 9.

FIGURE 2 | **The digital trust roadmap**



Source: World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 31.

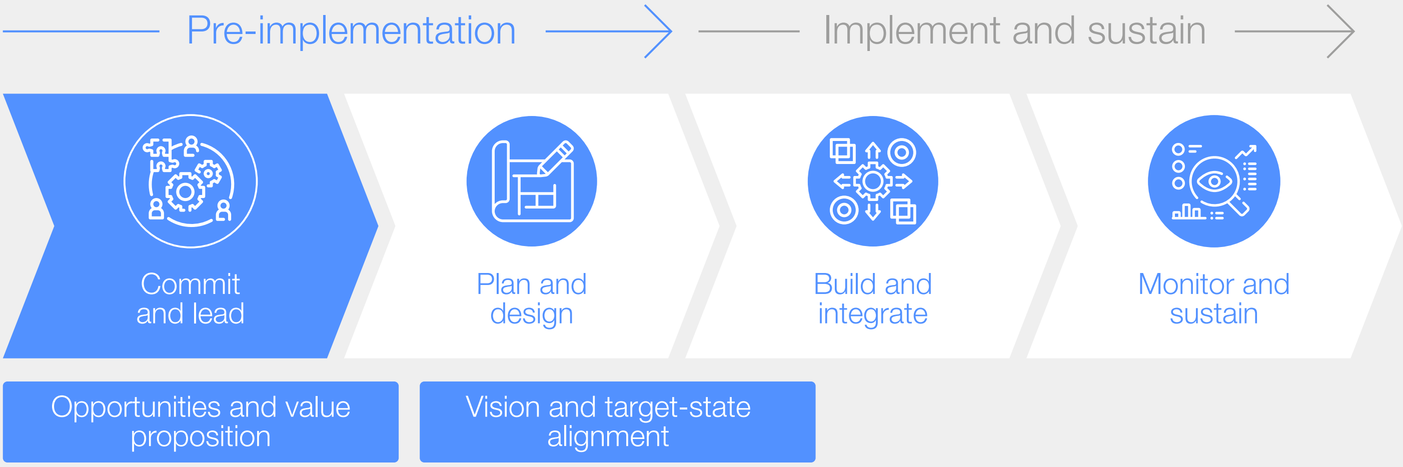
This briefing paper provides an overview and perspective on the pre-implementation steps for the digital trust programme and the foundational journey to establish that programme and culture. A future report will cover the implementation and sustainment phases for digital trust. This paper details how to frame digital trust within the unique context of an organization, how to chart a vision and target-state, and describes the due diligence and planning that can help drive leadership buy-in and successful implementation efforts.

1 Commit and lead

Starting the digital trust journey with a compelling vision that resonates with stakeholders across the organization.

Recent years have provided opportunities for organizations to take on large-scale initiatives under the banner of digital trust. Evolving global regulatory frameworks around data protection, cybersecurity, privacy and safety encourage collaboration across stakeholder groups to meet compliance objectives through incentives and severe penalties.[6] The structures and relationships established for regulatory readiness may prove helpful for organizations pursuing a digital trust strategy. Amid competing interests between stakeholder groups, regulatory requirements often serve as the common driver for decision-making. In contrast, digital trust implementation does not currently benefit from a baseline regulatory mandate. Instead, digital trust compels organizations to think beyond compliance and undertake a values-sensitive approach to decision-making. This translation layer between abstract and concrete – values to action – is a key objective of the pre-implementation phases of work for an organization's digital trust programme. This pre-work anchors a compelling vision for digital trust, aligns stakeholders and secures the necessary leadership buy-in.

FIGURE 3 **Commit and lead phases**



1.1 Opportunities and value proposition

The shortest route to a compelling business case for digital trust is identifying and qualifying the potential benefits of digital trust adoption.[7] Framing digital trust to unlock value for the organization in addition to serving the public good resonates well with senior leadership and can align interests across diverse stakeholder groups. The value proposition of digital trust is likely unique to each organization – a function of many factors that add texture to a digital trust implementation plan. The below questions are provided as suggestions to help contextualize digital trust value within a specific organization; they should be tailored to each organization's unique needs and values.

TABLE 1 Guiding questions

Organizational values and commitments	– What are the organization's stated core values? – What commitments relevant to digital trust have been made to the public or to regulators? – What objectives have been identified as part of an environmental, social and governance (ESG) campaign?
Industry, sector and competitive considerations	– How does the industry or sector influence expectations for digital trust? – What perceptions exist about the organization's trustworthiness? – How regulated is the industry? What is the competitive environment? – Who is the audience or audiences for trust-building efforts? – What is the elasticity of consumer buying or loyalty choices if a more trustworthy option were to exist?
Existing functions and capabilities	– How mature are the digital trust functions within the organization? – How effective are cross-functional decision-making and collaboration efforts? – How confident is the organization in its data collection and use practices? – What risk tolerances have been defined, and are these consistent throughout the organization? – How are users informed about the decisions made by the organizations upon their data?
Data volume and sensitivity	– What personal data is collected – what sensitivity and volume? – Are vulnerable populations represented or implicated in the data? – Are impactful decisions being made using automated decision-making?
Digital strategy and innovation	– What are the ambitions for the organization's business or digital strategy? – What opportunities are being explored in the market, and how might they impact data processing, risk management and trust? – How new and novel are the technologies or services being considered? – How vulnerable is the digital strategy to changes in regulation, industry standards or consumer consent?

With these factors in mind, organizations can begin to qualify the potential value of a digital trust strategy.[8] The scope and extent of the potential benefits will be unique to each organization and may include:

Benefits to the business

- **Demonstrable commitment to organizational values:** Many efforts to drive trust are incomplete or unable to connect to clear goals and actions in external messaging. Advancing a digital trust strategy internally can help strengthen the punch of external messaging – with actions demonstrating commitment where words fall short.

- **Competitive advantage:** Digital trust is one of the many factors consumers evaluate as they make buying and loyalty choices.[9] Prioritizing privacy, security, reliability and safety resonates with consumers and may introduce new challenges to competitors who may be less prepared to respond with similar commitments.[10]

- **Virtuous circles:** Trustworthiness in an organization's digital technology and services gives users the confidence to engage more enthusiastically. This confidence can help drive stronger adoption, improved loyalty and increased lifetime value of data.[11] For organizations sensitive to the consent preferences of its user base, digital trust drives down consent acquisition costs and makes preferences "stickier".

- **Confidence to pursue innovation and new opportunities:** As digital trust strengthens command over data operations and risk management within companies, they can be better positioned to explore new revenue streams. Reticence risk tied to potential user blowback or regulatory scrutiny can stifle exploration and expansion.[12] Digital trust cuts through reticence by giving leadership better data on risks and trade-offs to drive confident decision-making.

Benefits to society

- **Protecting health and safety:** Digital technologies serve a key role in critical infrastructure, health systems and (increasingly) life-impacting decision-making.[13] The care taken to design and deploy technology responsibly can translate to care taken for individual lives and well-being.

- **Promoting interconnectivity:** Digital platforms and infrastructures help to knit society (and societies) together in common discourse and connectivity. Prioritizing access, inclusivity and reliability via a digital trust strategy can drive significant benefits and extend the promise of technology to members of society.

- **Stable societies and strong institutions:** Digital trust is an effort shared by organizations, governments and society.[14] Safe and trustworthy digital products and services facilitate the growth and development of society, and strong, reliable institutions that society can trust with their data facilitate collaboration for the betterment of society.[15]

Benefits to risk mitigation

- **Better command over data collection and use:** Confidence in risk mitigation is powered by data awareness inside the organization. Many organizations struggle with the cross-functional coordination required to obtain resilient data inventories. Digital trust provides the strategic backstop that can drive the necessary coordination.[16]

- **Better able to anticipate and mitigate harms, including intangible harms:** Research on potential harms – tangible and intangible – has grown significantly in recent years. Digital trust provides the values-based direction for mature risk mitigation activities to think beyond compliance or tangible risks (e.g. identity theft).[17]

- **Elevating regulatory perceptions:** Digital trust commitments can elevate regulators' perceptions and provide mitigating factors to future inquiries or investigations.[18]

Benefits to operational efficiency

- **Improved decision-making and coordination:** Anchoring on shared objectives as part of a digital trust strategy can make it easier for diverse business and functional units to evaluate options and align on key decisions (e.g. risk profile, trade-offs and opportunities).

- **Streamlined, not siloed processes:** Digital trust opens opportunities to harmonize day-to-day operations that would otherwise be performed several times over in different digital trust dimensions. For example, instead of separate approvals processes and assessments for new initiatives, digital trust may open opportunities to harmonize a single process with various stakeholders working together.

- **Resilience to better navigate change:** Recent data protection and privacy regulations have disrupted operations several times over, especially with the need for inventories and current-state discovery efforts. Digital trust can drive more sustainable data awareness practices that make navigating change less disruptive.[19]

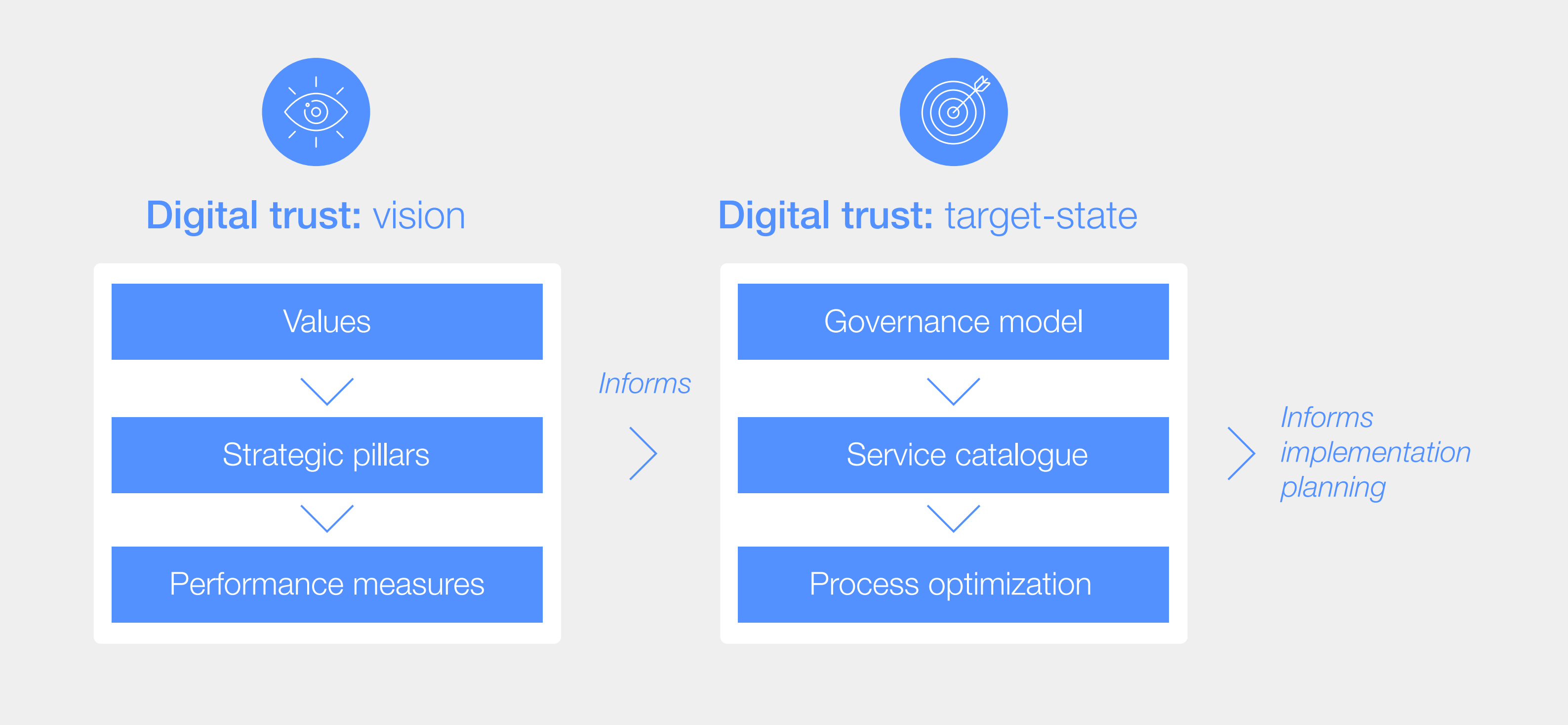
2

Vision and target state alignment

Establishing digital trust with a clear vision, defined governance, developed capabilities and a compelling business case.

Having assessed the role and value of digital trust to the organization, pre-implementation work continues with the crafting of a vision and target state for digital trust. This phase of work is where digital trust is "made real" for each organization – capturing the attention of stakeholders and leaders necessary to endorse implementation.

FIGURE 4 **Vision and target state**



Anchoring a vision for digital trust

Developing a vision for digital trust is the process of translating **values** into **strategic pillars** – and strategic pillars into measurable **performance metrics.**[20] This is a critical step to move from abstract values to measurable outcomes. The middle layer – strategic pillars – are ambitious, qualitative goals to be achieved in service to digital trust commitments. These pillars may be taken directly from the "objectives" defined by the Forum's digital trust framework or synthesized from the initial objectives-setting effort unique to the organization. Each strategic pillar is assigned quantitative performance measures that evidence progress towards objectives. This is more than an academic exercise – the strategic pillars and performance measures are the foundation for decision-making, providing disparate stakeholders with common ground and shared objectives. As organizations move through the initial implementation of the digital trust strategy and into maintenance, these strategic pillars and performance measures may be reviewed and modified on a regular basis.

Defining a target state digital trust programme

The design of the **governance model** is a critical early decision for digital trust.[21] For some organizations, digital trust is most effectively

> The eight dimensions of digital trust, as defined by the World Economic Forum digital trust initiative, provide a helpful framework for "operationalizing" digital trust.

positioned as a standalone vertical with an executive leader driving alignment and decision-making. For others, digital trust will cut across siloed business and functional units horizontally, serving as connective "scaffolding" driving coordination. Decisions in this horizontal model may be escalated to an accountable senior executive or to a steering committee comprised of leadership from each digital trust function. In both models, digital trust governance should have the authority and acumen to reach across functions and into key business areas impacted by digital trust (e.g. product design, marketing, brand and risk management).

The eight dimensions of digital trust, as defined by the World Economic Forum digital trust initiative, provide a helpful framework for "operationalizing" digital trust. Cybersecurity, privacy, transparency, redressability, auditability, fairness, interoperability and safety are elements that can be distilled into a service catalogue of capabilities that comprise digital trust operations.[22] The service catalogue for each dimension should include existing and desired capabilities by function, focusing on the activities that can better achieve the defined performance metrics. This pre-work may include evaluating similar day-to-day operations within siloed dimensions (e.g. assessments, training). The service catalogue might also identify where technology or **process optimization** can be used to better achieve performance metrics.

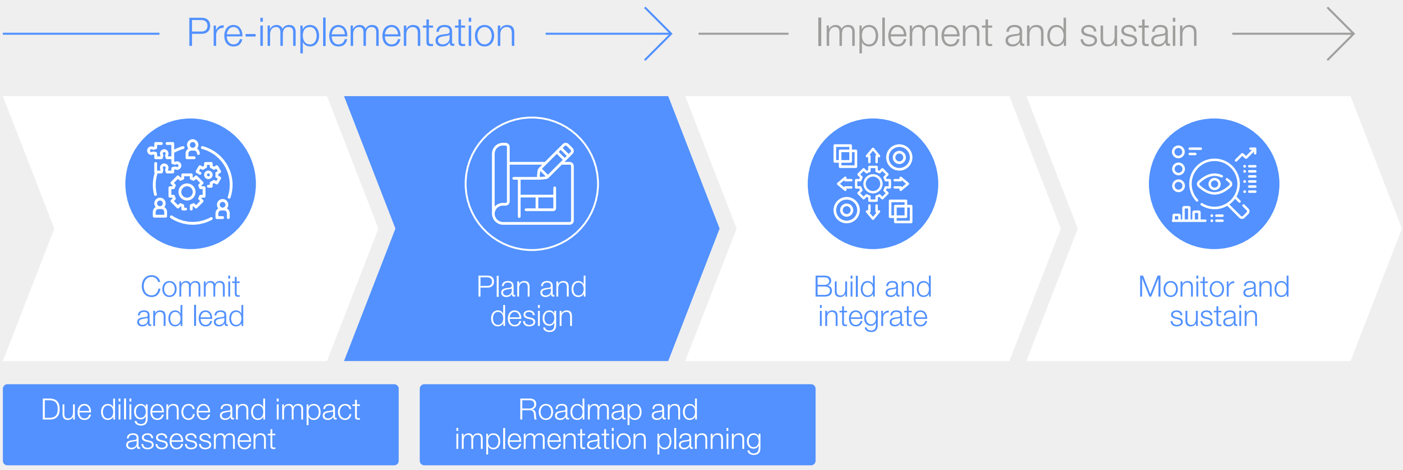
The groundwork is completed – benefits defined, vision and target-state outlined. Next comes the consolidation of these elements into a compelling business case that secures support and funding for the due diligence phase of this work.

3 Plan and design

Charting a path for digital trust implementation informed by current capabilities and potential challenges.

By this stage, the promise of a digital trust strategy resonates with leadership, and the question transitions from "What does this mean to our organization?" to "What does it take to get there?" To address these questions, the next steps in pre-implementation include the necessary due diligence and current-state assessment work and determining the extent digital trust drives positive or negative impacts on the business. Following this, the organization has the necessary raw material to package an implementation plan, a roadmap and the complete business case.

FIGURE 5 **Plan and design phases**



3.1 Due diligence and impact assessment

The current-state due diligence is the process through which these gaps are interrogated and resolution steps are identified.

A current-state assessment for digital trust can provide an honest appraisal of where the organization stands in pursuit of a defined target-state.[23] For example, one or more dimensions of digital trust may have significant gaps to close as part of the implementation efforts. Conversely, some organizations will have mature capabilities but poor connectivity across siloes that need attention and development. Still, others may see digital trust as a means of achieving maturity across all dimensions. The current-state due diligence is the process through which these gaps are interrogated and resolution steps are identified. To promote alignment at this stage, recruiting stakeholders representing each digital trust dimension may be beneficial. Working in concert, this diligence effort may include the following:

- **Documenting current-state capabilities:** The digital trust service catalogue developed in the prior phase can serve as a blueprint for the current-state assessment, outlining the specific capabilities that comprise (or will comprise) each dimension. Through stakeholder interviews and document reviews (e.g. playbooks, process flows, technology requirements), one can achieve a stronger understanding of each dimension day-to-day.

- **Assessing capabilities against digital trust objectives**: Current-state capabilities are evaluated against the defined digital trust strategic pillars and performance measures to derive recommendations for enhancement. Where capabilities do not exist, recommend the development of new operations.

- **Evaluating governance structures:** The above steps are repeated with an eye towards existing governance structures or escalation paths that can bring disparate stakeholder groups together for information sharing, decision-making and collaboration. This assessment evaluates whether existing structures could be modified to serve digital trust objectives or if new operating structures might be recommended.

- **Socializing with key stakeholders:** The above recommendations are packaged for stakeholder review and feedback.

- **Assessing business impact:** Not all enhancements to day-to-day operations are equal. Care should be taken to evaluate the recommendations' near-term and long-term implications to estimate the potential impact on business operations. This work includes evaluating in-flight initiatives that digital trust efforts may impact.

3.2 Implementation planning

Depending on the size and complexity of the organization, it may be appropriate to formalize project-specific governance and digital trust workstreams. These workstreams compartmentalize the work (e.g. dimension by dimension) and help raise issues and blockers to project leadership in an organized fashion. With this model in hand, the work can begin to translate current state recommendations into discrete project milestones – reflecting the incremental progress made in standing up new or enhanced capabilities or governance structures. Each workstream might have its own prioritized roadmap, reflecting the phasing of the work and any dependencies relating one milestone to another.[24] While extending the overall implementation timeline, segmenting the work into discrete phases may improve deployment for a project with so many impacted processes and stakeholders.

The development of a prioritized roadmap, segmented by workstreams, serves as the backbone for resource and funding estimates. With the line of sight on the people, capabilities and technologies necessary for the implementation, organizations can formalize a final estimate for the time and resourcing of the work. With the business case, the project plan and the strategic vision – the organization can secure the necessary buy-in and funding to launch the implementation phase.

Conclusion

Digital trust is as much a cultural transformation for organizations as an operational transformation.

Taking on the journey of digital trust reflects a significant commitment to a new era of innovation. The lofty ideals of the digital trust community signal a future where technology aligns with the interests of individuals and society. The pre-implementation steps outlined in this briefing paper are meant to bring action to digital trust commitments. This action can energize a community of values-driven organizations working to share lessons learned and insights from their digital trust efforts. Working together, it will be possible to accelerate the journey of digital trust and build a more trusted future.

Contributors

The Digital Trust Initiative is a multistakeholder collaboration led by the World Economic Forum with contributions by the entire digital trust community.

Lead authors

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

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

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

Digital Trust Initiative Fellows

Helena Kotschenreuther
Digital Trust Project Fellow; Cyber Strategy and Risk, KPMG

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

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

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

Kathryn White
Platform Fellow, Digital Trust, World Economic Forum; Associate Director, Metaverse Continuum Business Group, Accenture

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

The initiative team would like to especially thank the following members of the Digital Trust Initiative's measurement workstream 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), Yasodara Cordova (unico IDtech), Jill Crisman (UL Research Institutes), Kaje De Leon (Coca-Cola), Nicolas Fischbach (Google), Francisco Fraga (McKesson), Liz Grennan (McKinsey & Co.), 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), Jacob Springer (Abbott), Sridhar Sriram (Microsoft), Alissa Starzak (Cloudflare), Courtney Stout (Coca-Cola), Nicolas Zahn (Swiss Digital Initiative Foundation).

Production

Studio Miko

Laurence Denmark
Creative Director

Martha Howlett
Editor

Oliver Turner
Designer

Endnotes

1. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, pp. 29 and 46, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
2. “Losing digital trust will harm technological innovation: Here’s how to earn it again”, *World Economic Forum*, 8 December 2022, https://www.weforum.org/agenda/2022/12/losing-digital-trust-will-harm-technological-innovation/.
3. Edelman, *Edelman 2023 Trust Barometer Global Report*, 2023, p.23, https://www.edelman.com/sites/g/files/aatuss191/files/2023-03/2023%20Edelman%20Trust%20Barometer%20Global%20Report%20FINAL.pdf.
4. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 4, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
5. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 9, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
6. Duball, Joseph, “2023 brings US state privacy law preparedness into focus”, *IAPP*, 4 January 2023, https://iapp.org/news/a/2023-brings-us-state-privacy-law-preparedness-into-focus/.
7. Wakely, Jane, “How to harness the power of 1 billion people to accelerate sustainable change”, *World Economic Forum*, 17 January 2023, https://www.weforum.org/agenda/2023/01/consumers-sustainable-change-davos2023/.
8. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 9, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
9. Hojjati, Avesta, “Digital Trust now critical for maintaining customer loyalty”, *iWire*, 18 January 2023, https://itwire.com/guest-articles/guest-opinion/digital-trust-now-critical-for-maintaining-customer-loyalty.html.
10. “The surprisingly competitive advantage of digital trust”, *Tarsus Distribution*, 23 February 2023, https://tarsusdistribution.co.za/the-surprisingly-competitive-advantage-of-digital-trust.
11. World Economic Forum, *Good Data: Sharing Data and Fostering Public Trust and Willingness*, 2021, pp. 4 and 10, https://www3.weforum.org/docs/WEF_Good_Data_Sharing_Data_and_Fostering_2021.pdf.
12. Dobrygowski, Daniel, “Losing digital trust will harm technological innovation: Here’s how to earn it again”, *World Economic Forum*, 8 December 2022, https://www.weforum.org/agenda/2022/12/losing-digital-trust-will-harm-technological-innovation/.
13. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, pp. 11 and 22, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
14. Chakaravorti, Bhaskar, Ajay Bhalla and Ravi Shankar Chaturvedi, “How Digital Trust Varies Around the World”, *Harvard Business Review*, 25 February 2021, https://hbr.org/2021/02/how-digital-trust-varies-around-the-world.
15. Edelman, *Edelman 2023 Trust Barometer Global Report*, 2023, p.29, https://www.edelman.com/sites/g/files/aatuss191/files/2023-03/2023%20Edelman%20Trust%20Barometer%20Global%20Report%20FINAL.pdf.
16. “Building digital trust: Trust in data”, *PwC*, n.d., https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/digital-trust-leadership-operations-partnership/trust-in-data.html.
17. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 10, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
18. “FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet”, *The White House*, 28 April 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/.
19. “Achieving Organizational Resilience Through Digital Trust”, *Forbes*, 19 September 2022, https://www.forbes.com/sites/forbestechcouncil/2022/09/19/achieving-organizational-resilience-through-digital-trust/?sh=158e8be911e2.
20. Davis, Justin, “It’s Time To Set Performance Standards For Digital Trust And Safety”, *Forbes*, 3 May 2021, https://www.forbes.com/sites/forbestechcouncil/2021/05/03/its-time-to-set-performance-standards-for-digital-trust-and-safety/?sh=33a2edc34f8c.
21. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 32, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
22. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 8, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
23. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 32, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
24. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, p. 31, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.

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