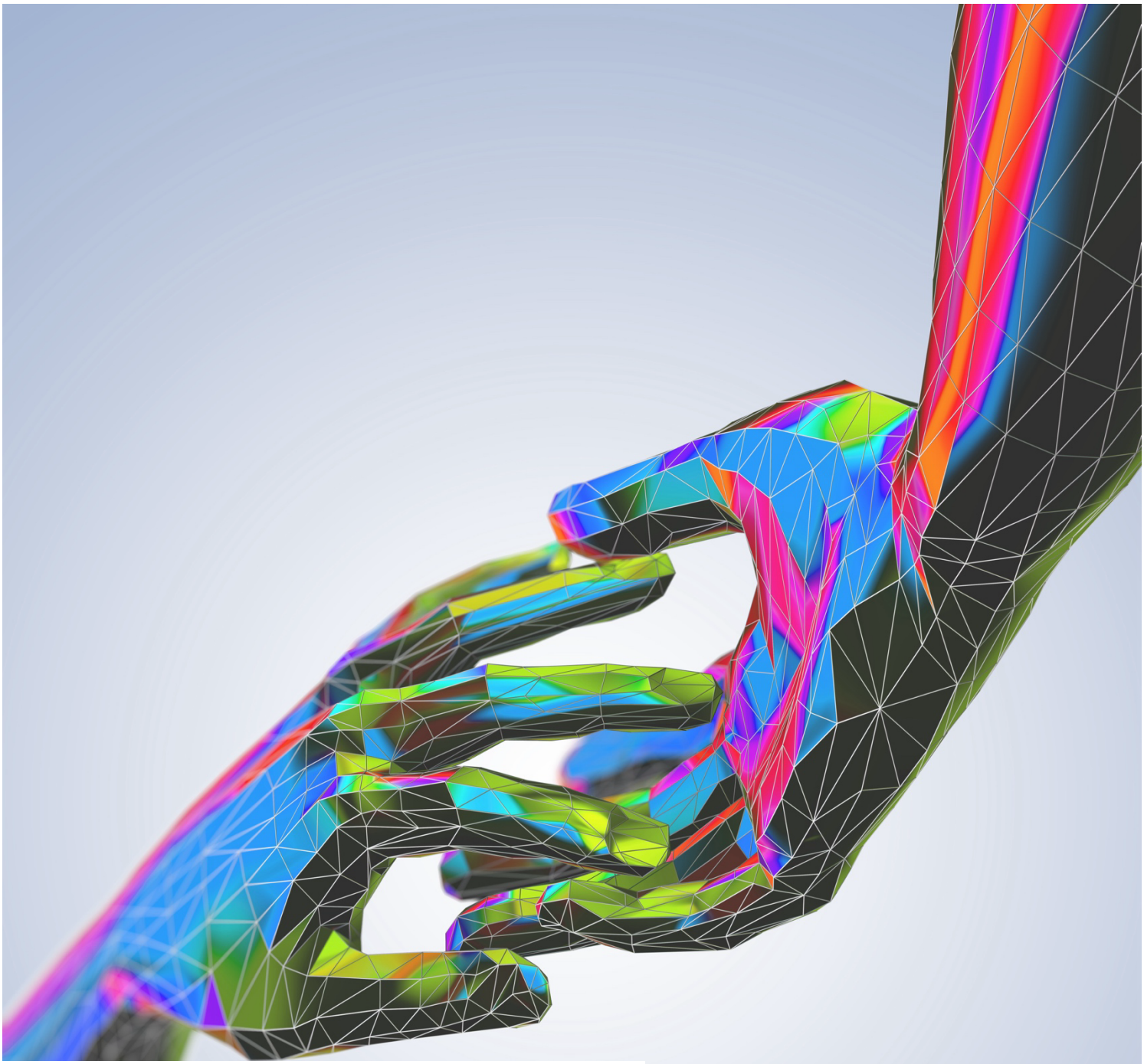
Universität Zürich[UZH]

Digital Society Initiative



Pilot Study: Digital Trust

Felix Gille, Markos Mpadanes, Federica Zavattaro

Imprint
© 26 November 2024
University of Zurich

Design and infographic
iStockphoto LP

Address
Universität of Zurich
Digital Society Initiative
Rämistrasse 69
8001 Zurich

Website
https://www.dsi.uzh.ch/en.html

Project category	Independent research project
Document	Research report
Project lead	Dr Felix Gille, Digital Society Initiative, University of Zurich
Researchers	Markos Mpadanes and Federica Zavattaro, Digital Society Initiative, University of Zurich
Funding	Swiss Academy of Engineering Sciences (SATW)

Funding statement:
This research project was initiated and financially supported by the Swiss Academy of Engineering Sciences (SATW). The research activities and the formulation of results were conducted independently of SATW.

Outside of this work, Dr Felix Gille receives funding from Novartis AG, Stiftung Sanitas, Digitalisierungsinitiative der Zürcher Hochschulen, and the World Health Organization.

Acknowledgement:
We thank Dr Melanie Knieps, Senior Researcher at the Digital Society Initiative, University of Zurich, and Co-Lead CYREN^{ZH}, as well as Dr Caroline Brall, Researcher and co-manager at Ethics and Policy Lab, University of Bern, for their internal reviews of this report.

About the authors:
Dr Felix Gille has a background in health policy and European public health. For over 10 years, he has been researching public trust in the health system, with a focus on health data sharing and digital health initiatives. Since 2021, Dr Gille has been a postdoctoral fellow at the Digital Society Initiative, University of Zurich. His previous work includes roles at the Swiss Federal Institute of Technology Zurich and the University of Cambridge. He holds a PhD from the London School of Hygiene and Tropical Medicine.

Markos Mpadanes has a background in communication and media research. He is a doctoral candidate at the University of Zurich, where he conducts empirical research in the strategic communication lab. His research interests include corporate activism and the ways in which CEOs and other executives express their opinions on socio-political issues online. Markos Mpadanes holds an MSc in Communication Science (Research Master's) and an MA in Contemporary History from the University of Vienna, Austria.

Federica Zavattaro has a background in health policy and public health. Since 2022, she has been a PhD candidate in Digital and Mobile Health at the Digital Society Initiative, University of Zurich. Her current research focuses on the role of public trust in the European health data-sharing policy process. Her previous work experience includes consulting at Clarivate Analytics in London. She holds an MSc from City University, London.

Table of Contents

Tables

Figures

'Digital Trust is a Team Sport'[1]

A literature review and interview pilot study with industry stakeholders to understand the state of knowledge and perceptions towards digital trust in Switzerland and abroad.

Executive summary (available in German, French and Italian)

In the digital economy, digital trust is a cornerstone for the successful implementation and adoption of digital technologies in the service sector. Many industry stakeholders see digital trust as increasingly central to the digital economy. The World Economic Forum describes digital trust as the expectation that digital technologies, services, and providers will protect stakeholders' interests and uphold societal values. Digital trust is vital to the successful adoption of digital technologies in various sectors, including health, defence, mobility, insurance, education, banking, and consumer markets. General trust is fundamental to social cohesion and economic prosperity, especially as digitalisation and technological complexity grow and make it harder for individuals to understand their digital environment. Digital trust helps reduce this complexity, allowing users to engage with digital services.

Given the growing interest in this area, we conducted a literature and interview study to assess the current knowledge among industry stakeholders about implementing, resourcing, and evaluating measures to promote digital trust in Switzerland and abroad.

We interviewed 16 stakeholders from different industries; these were mostly based in Switzerland but interviewees in Estonia, Germany, the United Kingdom, and the United States were also included. We reviewed 11 scientific publications on the subject. We also included a wide range of grey literature and other publications to develop a broader understanding of trust in the context of the digital economy.

The findings suggest that digital trust is a new concept for most industries, yet it is acknowledged as central to the digital economy. Digital trust is perceived by interviewees as a complex concept that can be promoted by a range of human-focused, regulatory and compliance-centred as well as government-supported activities. There should be a particular focus on building company cultures that promote digital trust, employee training to increase digital literacy, strategies to communicate the risks and benefits of digital services, and high technical standards to enable data security, privacy protection, and data traceability. Strong leadership at the executive level, including in the commitment of resources, is needed to drive change towards a corporate culture that promotes digital trust. As is the case for research on trust more broadly, evaluating and measuring digital trust is challenging. Tailored approaches are needed to build industry capacity and awareness regarding digital trust and the importance of digital hygiene.

Open issues for future research and development include the following:

1. Awareness raising at the executive level on digital trust and digital hygiene in companies
2. Development of evaluation methods for trustworthiness and digital trust
3. Development of tools and methods to support industry in digital trust building
4. Integration of digital trust-building principles in governance and administration
5. Knowledge transfer from global banking services and cyber defence to other sectors.

[1] Quote from Industry Stakeholder Interviewee

„Digitales Vertrauen ist ein Teamsport“[2]

Im Rahmen einer Literaturrecherche und einer Interview-Pilotstudie mit Branchenakteur:innen wurde der Wissensstand und die Wahrnehmung in Bezug auf digitales Vertrauen in der Schweiz und im Ausland ermittelt.

Zusammenfassung

Die erfolgreiche Einführung digitaler Technologien im Dienstleistungssektor basiert auf einem grundlegenden Vertrauen in die digitale Wirtschaft. Folglich stellt digitales Vertrauen für zahlreiche Branchenakteur:innen einen zunehmend zentralen Aspekt der digitalen Wirtschaft dar.

Das Weltwirtschaftsforum definiert digitales Vertrauen als die Erwartung, dass digitale Technologien, Dienstleistungen und Anbietende die Interessen der Akteur:innen schützen und gesellschaftliche Werte wahren. Digitales Vertrauen ist eine wesentliche Voraussetzung für die erfolgreiche Einführung digitaler Technologien in verschiedenen Sektoren, darunter Gesundheit, Verteidigung, Mobilität, Versicherungen, Bildung, Banken und Verbrauchermärkte. Allgemeines Vertrauen ist für den gesellschaftlichen Zusammenhalt und den wirtschaftlichen Wohlstand von grundlegender Wichtigkeit. Insbesondere vor dem Hintergrund der fortschreitenden Digitalisierung und gewachsenen technologischen Anforderungen ist es für Individuen zunehmend schwierig, die eigene digitale Umgebung zu verstehen. Digitales Vertrauen reduziert diese Komplexität und ermöglicht Nutzenden erst die Interaktion mit digitalen Services.

Angesichts des wachsenden Interesses an diesem Bereich haben wir eine Literatur- und Interviewstudie durchgeführt. Ziel war es, den aktuellen Wissensstand der Branchenakteur:innen über die Umsetzung, Finanzierung und Bewertung von Massnahmen zur Förderung des digitalen Vertrauens in der Schweiz und im Ausland zu ermitteln.

Im Rahmen der vorliegenden Studie wurden 16 Interessenvertreter:innen aus verschiedenen Branchen befragt. Die Befragten waren grösstenteils in der Schweiz ansässig, jedoch wurden auch einzelne Personen aus Deutschland, Estland, Großbritannien und den Vereinigten Staaten einbezogen. Zusätzlich wurden elf wissenschaftliche Publikationen sowie eine Vielzahl an nichtwissenschaftlicher Literatur und anderen Publikationen analysiert, um ein umfassenderes Verständnis von Vertrauen im Kontext der digitalen Wirtschaft zu entwickeln.

Die Ergebnisse deuten darauf hin, dass digitales Vertrauen für die meisten Branchen ein neues Konzept ist, dessen Bedeutung für die digitale Wirtschaft jedoch zunehmend anerkannt wird. Die Befragten betrachten digitales Vertrauen als komplexes Konzept, das durch eine Reihe von auf den Menschen ausgerichteten, regulatorischen und auf die Einhaltung von Vorschriften ausgerichteten sowie von der Regierung unterstützten Aktivitäten gefördert werden kann. Besonderes Augenmerk gilt dem Aufbau von Unternehmenskulturen, die digitales Vertrauen fördern, der Schulung von Mitarbeitenden zur Verbesserung der digitalen Kompetenz, der Entwicklung von Strategien zur Kommunikation der Risiken und Vorteile digitaler Dienste sowie der Einhaltung hoher technischer Standards zur Gewährleistung von Datensicherheit, Datenschutz und Datenrückverfolgbarkeit. Es obliegt der Führungsebene, den Wandel hin zu einer Unternehmenskultur voranzutreiben, die von digitalem Vertrauen geprägt ist. Dazu muss sie insbesondere die Bereitstellung von Ressourcen fördern. Um die Kapazitäten und das Bewusstsein der Branche für digitales Vertrauen und die Bedeutung der digitalen Hygiene zu stärken, sind massgeschneiderte Ansätze erforderlich.

Die Bewertung und Messung des digitalen Vertrauens stellen ebenso eine Herausforderung dar, wie sie auch bei der Forschung zum Thema Vertrauen im Allgemeinen beobachtet werden kann. Für die Zukunft werden die folgenden Aspekte als wichtige Forschungsbereiche erwartet:

2 Zitat aus einem Interview mit einem Interessenvertreter der Industrie

1. Sensibilisierung der Führungsebene für digitales Vertrauen und digitale Hygiene im Unternehmen
2. Entwicklung von Bewertungsmethoden für Vertrauenswürdigkeit und digitales Vertrauen
3. Entwicklung von Instrumenten und Methoden zur Unterstützung der Industrie beim Aufbau digitalen Vertrauens
4. Integration von Grundsätzen für den Aufbau digitalen Vertrauens in die Unternehmensführung und -verwaltung
5. Wissenstransfer von globalen Bankdienstleistungen und Cyberabwehr auf andere Sektoren.

‘La confiance numérique est un sport d'équipe’[3]

Une revue de littérature et une étude pilote des entretiens, réalisés avec des acteurs du secteur, pour comprendre l'état des connaissances et des perceptions à l'égard de la confiance numérique en Suisse et à l'étranger.

Résumé

Dans l'économie numérique, la confiance numérique constitue une pierre angulaire pour la mise en œuvre réussie et l'adoption des technologies dans le secteur des services. De nombreux acteurs estiment qu'elle est au cœur de l’économie numérique. Le Forum économique mondial définit la confiance numérique comme l'attente que les technologies, services et fournisseurs numériques protègent les intérêts des parties prenantes tout en défendant les valeurs sociétales. Cette notion est essentielle pour l'adoption des technologies numériques dans divers secteurs tels que la santé, la défense, la mobilité, l'assurance, l'éducation, la banque ou encore les marchés de consommation. La confiance générale est fondamentale pour la cohésion sociale et la prospérité économique, d'autant plus que la numérisation et la complexité technologique augmente et rendent plus difficile pour les individus, la compréhension de leur environnement numérique. En réduisant cette complexité, la confiance numérique facilite l'engagement des utilisateurs dans les services numériques.

Face à l'intérêt croissant de ce sujet, nous avons réalisé une étude bibliographique et mené des entretiens afin d’évaluer l’état actuel des connaissances des acteurs industriels concernant la mise en œuvre, le financement et l’évaluation des mesures visant à promouvoir la confiance numérique en Suisse et à l'étranger.

Ainsi, nous avons interrogé 16 acteurs issus de différents secteurs, principalement basés en Suisse, ainsi qu'en en Estonie, en Allemagne, au Royaume-Uni et aux États-Unis. Parallèlement, 11 publications scientifiques ont été examinées. Nous avons également inclus un large éventail de littérature grise et d'autres publications afin de développer une compréhension plus large de la confiance dans le contexte de l'économie numérique.

Les résultats montrent que la confiance numérique est un concept encore relativement récent pour la majorité des industries. Bien qu’elle soit largement reconnue comme essentielle, sa mise en œuvre est perçue comme un défi complexe. Selon les acteurs, cette confiance peut être renforcée par des initiatives centrées sur l'humain, par des mesures de réglementation et de conformité, ainsi que par des actions soutenues par le gouvernement. Selon eux, il serait essentiel de prêter davantage attention à la création d'une culture d'entreprise favorisant la confiance numérique. Cela passerait notamment par la promotion de la formation des salariés afin de renforcer la démocratisation du digital, le développement de stratégies efficaces pour communiquer les risques et les avantages des services numériques, et la mise en place de normes techniques élevées visant à garantir la sécurité des données, la protection de la vie privée et la traçabilité des informations. Un leadership fort au niveau de la direction, y compris dans l'engagement des ressources, est également indispensable pour impulser ce changement culturel en faveur de la confiance numérique. Cependant, comme pour la recherche sur la confiance en général, évaluer et mesurer la confiance numérique reste un défi de taille. Des approches personnalisées sont nécessaires pour renforcer les compétences et sensibiliser davantage le secteur à l'importance de la confiance numérique et des bonnes pratiques en matière d'hygiène numérique.

Les questions ouvertes pour la recherche et le développement futurs comprennent ce qui suit :

1. Sensibilisation au niveau de la direction sur la confiance numérique et l'hygiène numérique dans les entreprises
2. Développement de méthodes d'évaluation de la fiabilité et de la confiance numérique

[3] Citation d'une personne interrogée dans l'industrie

3. Développement d'outils et de méthodes pour soutenir l'industrie dans la construction de la confiance numérique
4. Intégration des principes de renforcement de la confiance numérique dans la gouvernance et l'administration.
5. Transfert de connaissances des services bancaires mondiaux et de la cyberdéfense vers d'autres secteurs.

«La fiducia digitale è uno sport di squadra»[4]

Un'analisi della letteratura e uno studio pilota con interviste a stakeholder del settore per comprendere il livello di conoscenza e le percezioni circa la fiducia digitale in Svizzera e all'estero.

Riassunto

Nell'economia digitale, la fiducia digitale è una pietra miliare per un'implementazione e adozione di successo delle tecnologie digitali nel settore dei servizi. Molti stakeholder del settore considerano la fiducia digitale sempre più centrale per l'economia digitale. Il World Economic Forum descrive la fiducia digitale come l'aspettativa che tecnologie, servizi e fornitori digitali proteggano gli interessi degli stakeholder e rispettino i valori della società. La fiducia digitale è fondamentale per l'adozione di successo delle tecnologie digitali in vari settori, tra cui sanità, difesa, mobilità, assicurazioni, istruzione, banche e mercati dei consumatori. In generale la fiducia è fondamentale per la coesione sociale e la prosperità economica, soprattutto con l'aumento della digitalizzazione e della complessità tecnologica che rende più difficile per gli individui comprendere il proprio ambiente digitale. La fiducia digitale aiuta a ridurre questa complessità, consentendo agli utenti di interagire con i servizi digitali.

Dato il crescente interesse per questo ambito, abbiamo condotto uno studio basato sulla revisione della letteratura e su interviste per valutare le attuali conoscenze tra gli stakeholder del settore riguardo l'implementazione, le risorse e la valutazione di misure per promuovere la fiducia digitale in Svizzera e all'estero.

Abbiamo intervistato 16 stakeholder di diversi settori, per lo più basati in Svizzera ma anche in Estonia, Germania, Regno Unito e Stati Uniti. Abbiamo fatto una revisione di 11 pubblicazioni scientifiche sull'argomento, includendo un'ampia gamma di letteratura grigia e altre pubblicazioni per comprendere in maniera più ampia la fiducia nel contesto dell'economia digitale.

I risultati suggeriscono che la fiducia digitale è un concetto nuovo per la maggior parte dei settori, ma è riconosciuta come centrale per l'economia digitale. La fiducia digitale è percepita dagli intervistati come un concetto complesso che può essere promosso da una serie di attività incentrate sull'uomo, sulla regolamentazione e sulla conformità, nonché supportate dai governi. Dovrebbe essere posta particolare attenzione alla costituzione di culture aziendali che promuovano la fiducia nel digitale, alla formazione dei dipendenti per aumentare l'alfabetizzazione digitale, alle strategie per comunicare i rischi e i benefici dei servizi digitali e a standard tecnici elevati per garantire la sicurezza dei dati, la protezione della privacy e la tracciabilità dei dati. Una leadership forte a livello esecutivo, inclusa la disponibilità di risorse, è necessaria per guidare il cambiamento verso una cultura aziendale che promuova la fiducia digitale. Come nel caso della ricerca sulla fiducia piu' generica, valutare e misurare la fiducia digitale è una sfida. Sono necessari approcci personalizzati per costruire la capacità e la consapevolezza del settore riguardo la fiducia digitale e l'importanza dell'igiene digitale.

Le questioni aperte per la ricerca e lo sviluppo futuri includono:

1. Sensibilizzazione a livello dirigenziale circa la fiducia digitale e l'igiene digitale nelle aziende
2. Sviluppo di metodi di valutazione dell'affidabilità e della fiducia digitale
3. Sviluppo di strumenti e metodi per supportare l'industria nella creazione di fiducia digitale
4. Integrazione di principi che contribuiscono alla formazione della fiducia digitale nella governance e nell'amministrazione.
5. Trasferimento di conoscenze dai servizi bancari globali e dalla difesa informatica ad altri settori.

[4] Citazione di uno stakeholder del settore intervistato nello studio

Introduction

As the digitalisation and technologisation of society and industry continue, trust will play an increasingly important role. For us humans, driven by digitalisation, our private and professional environments have become increasingly complex and, in many cases, less comprehensible. In the digital economy, digital trust offers a way to reduce this complexity while maintaining our ability to act and navigate our environments (Luhmann, 2009). For example, as users of algorithm-supported services, we are often unable to fully understand how our data are processed, stored, or shared. We use many services, either consciously or unconsciously, trusting that our data will be used and protected in our best interests. In many cases, we weigh the potential benefits against perceived risks when choosing digital services (Swiss Digital Initiative, 2021).

Digital trust is of increasing interest in the digital economy and digital technology industry. Although there is no commonly accepted definition, the World Economic Forum defines the concept as follows:

> 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 (World Economic Forum, 2022, p. 5) .

There is some research on digital trust dating back to 1996, but research efforts gained momentum around 2016, with the most relevant studies appearing in the field of Computer Sciences, followed by Engineering and Business Economics. Notably, and as our study confirmed, the term 'digital trust' was coined more recently, and other terms, such as 'cyber trust', were previously used to refer to similar concepts (Pietrzak and Takala, 2021). For the digital economy, digital trust is essential for the successful implementation and adoption of digital technologies in the service sector (Pietrzak and Takala, 2021; Ryan, 2021; Teigland *et al.*, 2019). Currently, digital trust seems most important in industries that process sensitive data or deal with a high volume of data, including health, defence, mobility, insurance, education, banking, and consumer markets. Trust, in the broader sense, is essential for prosperity, social cohesion and the success of economic systems (Ho, 2023).

Considering the cross-industry interest in digital trust, our study aims to better understand the current state of knowledge regarding the implementation, resource requirements, and evaluation possibilities of trust-promoting measures in the area of digital trust in Switzerland and abroad.

In meeting this aim, the objective of the study is to address the interdependence of business and digital trust in three key areas:

1. digital trust-building measures;
2. resource allocation; and
3. evaluation and measurement.

We conducted a scoping review of relevant literature and interviews with stakeholders from the Swiss and international industry landscape to gain a comprehensive understanding of the subject matter. The methods are outlined on page 24 and following.

Concept: How to describe digital trust

In most industries, the concept of digital trust has emerged only recently. Our interview study shows that outside of global banking and cyber defence, digital trust became an area of interest in the past two to three years. The perceived importance of digital trust for interviewees ranged from being a fundamental issue for their industry to merely a topic for future consideration. Several participants linked digital trust to company culture, with one participant suggesting that there is a need for a paradigm shift towards recognising digital trust as a core business value. The extent to which it is considered relevant to other topics appears to be related to how integral trustworthiness and trust are to a company's core business and its success. Thus, high levels of overall trust in a company appear to influence the perception of its trustworthiness concerning its digital activities. Conversely, if a company is perceived as not being trustworthy in its analogue activities, building digital trust in that company will be challenging, if not impossible. Digital trust was commonly understood by interviewees as a relational concept in the context of data use, where subject A trusts subject B to use their data securely and confidentially, resulting in a beneficial outcome for the trusting party, both parties engaged in the trust relationship, or the industry sector as a whole (beyond a specific service or product) where it relies on similar data-sharing practices. Digital trust drives the use of digital services, encourages engagement, and increases sales. From an entrepreneurial perspective, the need for digital trust can be summarised by its critical role in facilitating seamless 'data flows', which are essential for business operations and growth in the digital economy.

How did interviewees describe digital trust?

Across all interviews, we identified 17 themes portrayed by participants as contributing to digital trust (**Table 1**); the detailed methods are described in the methods section (p. 24). When comparing these 17 themes with existing research on trust outside the digital economy, we found that the themes identified in interviews could be categorised into those unique to digital trust (or trust in the digital context) and those more generally relevant to trust building in a broad economic context. The latter themes are commonly seen in research across a range of trust concepts. The themes presented in Table 1 are not ranked according to relative importance, and we cannot make a claim about how many of the identified characteristics need to be fulfilled to establish trust. This is because the configuration of themes important to trust building is influenced by the context in which trust develops.

In addition to considering what aspects build trust (reflected in the themes identified), it is important to understand the context in which digital trust develops, the network of parties in the trust relationship and those with an external impact on trust building. Therefore, we recommend conducting a conceptual analysis of the context alongside a mapping of the actor network describing the trust relationship. This analysis should address two key questions:

a) Who trusts whom? and
b) Who influences the trust relationship?

The perspective we adopt in the trust analysis shapes the conceptualisation of trust. Are we considering the user perspective, the provider perspective, or that of the state or company? By answering these questions, we can identify the contextual factors influencing the trust relationship and determine the perspective to be taken so as to tailor the trust-building strategy accordingly.

Table 1 *Characteristics contributing to digital trust – Interview results*

Q1: What do you understand by the term digital trust?	
Theme	**Explanation**
Digital-specific trust themes	
Relating to present perceptions	
Data security*	If data are handled securely, digital trust is built.
Data traceability*	If data use is traceable, digital trust is built.
Privacy protection*	If privacy is protected, digital trust is built.
Technical standards*	If technical standards are maintained, digital trust is built.
General trust themes in the economic context	
Relating to past experiences	
Partnership	If trustors and trustees have a long-lasting partnership, digital trust is built.
Positive previous experience	If trustors have positive experiences with digital services, digital trust is built.
Relating to present perceptions	
Accountability	If accountability measures are in place, digital trust is built.
Communication	If data users are informed about data use, digital trust is built.
Competence	If data users are competent, digital trust is built.
Compliance with ethics	If data users comply with ethics, digital trust is built.
Comprehension	If trustors understand how data are used, digital trust is built.
Fairness	If data users are fair, digital trust is built.
General trust in the company	If trustors generally trust a company, digital trust is built.
Responsibility	If data users handle data responsibly, digital trust is built.
State involvement	If the state is involved in digital services, digital trust is built.
Time	If those building trust have time to do so, digital trust is built.
Relating to future anticipations	
Expectations are considered	If trustors' expectations are considered, digital trust is built.

**Themes relating to present perceptions*

Digital-specific trust themes

Data security is linked to digital trust by ensuring that data are protected against unauthorised access and use. A robust cybersecurity infrastructure is essential to protect sensitive data and, in turn, build trust (Kluiters, Srivastava and Tyll, 2023). *Privacy protection* builds digital trust as users are more engaged in technologies when they feel that their privacy is protected. Trust enables users to employ technology without constantly checking whether security and privacy measures are in place (Al-Hujran *et al.*, 2015). Implementing and adhering to *technical standards* can contribute to accountability and transparency, which leads to digital trust (Cao *et al.*, 2016). Similarly, being able to *trace data access and use* contributes to accountability and transparency.

General trust themes in the economic context

The 13 identified themes related to general trust can be clustered into three categories: past experiences, present perceptions, and anticipated outcomes. This categorisation aligns with other conceptualisations of trust, where these three collectively contribute to trust (Gille, 2023). Actors can only build digital trust when they receive information concerning all three timeframes. While most of the 13 themes are common in trust research in economics, three are of particular importance or, compared to existing trust research, somewhat original to this study: communication, general trust in a company, and state involvement.

Communication is fundamental to trust building. Without the exchange of information, trust cannot be built (Illes, Katalin and Mathews, Martin, 2015). *General trust in a company* was also mentioned by interviewees as

critical; it is of little value to invest in building digital trust – understood as user trust in a specific service or data flow – if the company itself is not considered trustworthy or does not have a good reputation. This perspective highlights the need to look beyond the specific context of data flows and consider the company as a whole, if not the entire sector. Other research indicates that users do not always differentiate between similar services or between a digital service and the company offering it. Often, users build trust based on their overall trust in a company or their trust in comparable services, where trust spills over to the new services (Gille, 2023). *Involving the state* in digital services is considered important to building trust as the state typically enjoys high levels of public trust; the rationale is that this trust can be transferred to the digital services offered by the private sector.

Implementation: How to build digital trust and with what resources

Once a comprehensive understanding of digital trust has been established, including the factors that contribute to building digital trust, the next step is trust building and resource allocation for trust building. These resources are time, capital, know-how, an appropriately skilled workforce and others.

What did interviewees say about building digital trust and resources allocation?
Interviewees suggested a wide range of activities that contribute to digital trust building and where resources can be effectively allocated (**Table 2**). Table 2 does not include a ranking of the relative importance of themes. Four key approaches to developing digital trust emerged from the interviews and offer guidance in directing resources:

a) Human-centred approaches
b) Compliance-centred approaches
c) Engineering approaches
d) Government-driven approaches

Table 2 *Activities contributing to digital trust building requiring resource allocation*

How can we build digital trust, and with what resources?
Human-centred approaches
Co-operation with universities to co-develop digital trust-building activities
Corporate culture* promoting digital trust
Customer services as a trustworthy face of the company
Digital hygiene*
Employee training* on trust-building activities
Financial services promoting digital trust
Generate clear added value* of data flow
Governance* promoting digital trust
High company reputation* as a prerequisite for digital trust
Human resources promoting digital trust
Identification of problems* potentially undermining digital trust
Leadership from executive level* to be role models and drive digital trust building
Sales department is the trusted face of the company
Understandable communication strategies
Compliance-centred approaches
Audits to comply with digital trust standards
Labels to certify trustworthiness
Legal advice* to comply with law and regulation
Engineering approaches
Cybersecurity* to protect data
Engineering to construct infrastructures promoting digital trust
Information technology to promote digital trust
Privacy by design to deeply integrate privacy protection into the company
Government-driven approaches
Digital policy to develop a robust digital infrastructure on a national level
E-governance at the state level* to get the public used to digital services
Government provides free-for-service advice to companies about digital trust to build overall capacity
National cybersecurity strategy to protect data within a country

(Interview Q2: How can digital trust be promoted in practice? and Interview Q3: What resources are needed to promote digital trust in practice?)*

Human-centred approaches

Regarding trust as an interhuman relational concept, 14 themes were identified by interviewees as important for digital trust building, focusing on company employees, the company's interaction with its environment, and data providers.

There is a general understanding that leadership is needed at the executive level to a) allocate resources to digital trust and b) drive efforts to build digital trust. Company leaders can act as role models and drive change. Digital trust must be deeply integrated as a core value and as a Key Performance Indicator for successful governance to have meaning in the company. Strong governance efforts are needed to develop a company culture in which digital trust can flourish. Employee training is a vital component in establishing digital trust, especially since human error and low levels of digital literacy can undermine digital trust and damage a company's reputation. High levels of digital hygiene are required (within the company and across society more broadly) to protect data and personal identity (Kioskli *et al.*, 2023). Interviewees suggested that within a company, digital trust building is the responsibility of several organisational units and requires an executive-led team effort. The organisational units that could be considered are customer service, human resources (for coordinating employee training), financial services, sales, legal, IT, and engineering. These units are central to human interaction within a company and between the company and its customers. Tying these areas together, transparent, open, comprehensible, and targeted communication is the cornerstone of digital trust. Internally, an open communication culture is critical to encourage employees to speak up and identify problems. Externally, a company's communication with customers and business partners is key to conveying the direct benefit of data flows and to being transparent about data use and governance.

Compliance-centred approaches

Interviewees discussed three compliance-centred approaches: external and internal auditing, certification processes resulting in labels, and the role of legal services. Auditing reports and labels advance transparency, helping to drive internal change towards more trustworthy behaviour and demonstrating to external stakeholders that the company adheres to certain established standards of trustworthiness. Compliance with laws and regulations is essential for building digital trust, and this is a reminder of the importance of legal advice.

Engineering approaches

A well-engineered information technology infrastructure that incorporates privacy by design and cybersecurity is a critical prerequisite for a company to be considered trustworthy in the digital economy.

Government-driven approaches

Efforts to build digital trust can be supported by a series of government-driven approaches, including a national cybersecurity strategy and digital policies (Information System Authority, 2024). Government-provided free-for-service advice on digital matters can enhance digital literacy and assist companies in strengthening their digital governance. In addition, highly developed e-governance promotes digital literacy at a societal level through the routine use of digital services in various aspects of daily life.

What does the literature say about building digital trust and resources allocation?

In contrast to the interviews, the literature contains very little on resource allocation as a requirement for the introduction, continuation or expansion of digital trust-building measures. The grey literature, within international and comparative occupational field studies, provides little information beyond vague descriptions of current states, assessments, and future prospects. These studies offer recommendations for the promotion and assurance of digital trust, with a particular focus on cyber security. The resources required – such as funding, external consultancy and services – are clear, at least implicitly. Three scientific publications partially address resource allocation in the context of digital trust. One highlights data security as a key

customer concern and urges companies to invest in tools that give customers control over their data and implement strong security and privacy procedures, maintaining transparency throughout (Jacobson, 2018). Another emphasises the need for companies to reorganise their security approach by establishing security teams, managing IT risks, and defining security projects (Asia Insurance Review, 2010). Lastly, a study on non-market strategies in the sharing economy argues that trust building requires essential firm-level resources to engage stakeholders, resolve issues, and enhance credibility (Ko *et al.*, 2022).

The most frequently discussed topics relate to the implementation of digital trust strategies; this was featured in eight out of 11 articles. These studies advance theoretical models to enhance and understand mechanisms of trust. The grey literature also emphasises trust building, with numerous organisations offering materials, including whitepapers, brochures, case studies, and reports that address the significance and need for action to ensure digital trust. Below are two case studies illustrating how the concept of digital trust is framed in the literature on banking and cyber defence, two leading industries in the area of digital trust.

Case: Banking and digital trust

Digital trust plays a central role in the adoption and success of digital banking services. Understanding the link between trust and online banking is essential for sustained customer relations, the adoption of new services and the sustainability of online banking. In online banking, digital trust is mainly associated with customers' perceptions and experiences of system security and reliability. Where customer trust in digital banking services is high, the perceived risk associated with online transactions drops, increasing the likelihood that they will use those services (Bashir and Madhavaiah, 2015; Saif *et al.*, 2022). The relationship between perceptions of data security and the trustworthiness of online banking services is particularly important in societies in which there are relatively high levels of concern about data security and privacy protection. Integrating robust data security measures and easy-to-understand communication about how these measures work can build trust among users (Kaur *et al.*, 2021).

Customer education initiatives can increase digital trust among customers by enhancing their digital literacy and their understanding of online banking services. Engaging customers through live demonstrations and addressing their concerns about online banking can foster trust (Febriyanti *et al.*, 2023). In addition, the shift from face-to-face to online engagement requires a shift from trust in individual banking professionals to trust in the overall banking system, where the trusted face of the bank, the banker, moves into the background. This shift makes the quality of online services even more important (Mbama *et al.*, 2018; Melnyk, 2024). In conclusion, the success of online banking depends on digital trust, a complex concept that relies on data security, reliability, communication, customer literacy and service quality.

Case: Cyber defence and digital trust

Cyber defence comprises strategies and measures to protect digital systems from cyber threats. As these evolve in complexity and frequency, robust cyber defence mechanisms become essential to maintaining and enhancing digital trust among users, organisations, and governments. Therefore, cyber defence and the ability to effectively recover from cyber-attacks are closely linked to digital trust. For example, a zero-trust strategy that requires constant verification can support digital trust by being proactive in the face of evolving threats (Wylde, 2021). Industry stakeholders sharing knowledge and lessons learned about cyber threats and countermeasures can help ensure more robust defence systems, enhancing overall digital trust (Rantos *et al*., 2020).

In conclusion, as these threats continue to evolve, organisations need comprehensive cyber defence strategies that protect against attacks and actively build user trust. A combination of advanced technologies, proactive defence measures, and collaboration and sharing of threat intelligence supports the creation and maintenance of digital trust.

Evaluation: How to evaluate digital trust

Evaluation of digital trust building activities and the measurement of levels of trust are important to:

a) understand if digital trust-building activities such as robust cyber security structures positively influence levels of digital trust;
b) understand if resources invested in digital trust building lead to a benefit as part of economic evaluation;
c) adjust digital trust building activities, data flow processes and overall governance structures where necessary; and
d) to understand levels of digital trust.

What did interviewees say about digital trust evaluation methods?

The evaluation of the effectiveness of digital trust-building efforts can rely on a portfolio of methods, indicating that a combination of approaches is necessary (**Table 3**).

Table 3 *Digital trust evaluation*

How can activities that promote digital trust be evaluated?
Absence of negative media coverage
Comparative analysis
Demonstrable practical relevance
Employee performance assessment
Increase in sales
Monitoring of key performance indicators (KPIs)
Observable benefits
Qualitative research approaches
Trust Stress Tests

Evaluating digital trust (aside from observing increases in sales, the absence of negative media coverage, and the general recognition of its benefits by external parties) requires that companies take deliberate action and allocate the necessary resources. However, with the exception of stress tests, all methods can be integrated into ongoing performance evaluation. One interviewee suggested trust stress tests should be developed to assess the robustness of a company or specific service in withstanding hostile activities, whether internal or external, that could undermine digital trust. More conventional methods include comparative studies of different digital services evaluating their performance in terms of their ability to build and maintain digital trust. Anchoring digital trust in key performance indicators (KPIs) can facilitate comparison and help companies determine whether digital trust has been effectively developed. One interviewee suggested using KPIs to link digital trust to the performance assessment of the executive board. Central to all evaluation methods is their relevance to the process of developing digital trust and their capacity to drive change where needed.

What does the literature say about methods to evaluate digital trust?

The literature suggests a divergence in how evaluation is understood in the context of digital trust. The scientific literature focuses on developing instruments to measure digital trust at the micro level, such as frameworks for workplace assessment. The grey literature adopts a macro perspective, examining digital trust across entire industries and providing practical insights into governance, cyber security, and organisational strategies. Communication is recognised as a key component in evaluating digital trust – since transparent communication helps identify issues that may undermine trust, and the right narratives are essential for building it. However, no definitive evaluation instruments were identified in the literature review.

One of the 11 scientific publications on digital trust in the business sector explicitly addressed its measurement (Launer, Çetin and Paliszkiewicz, 2022). The authors developed a 50-item questionnaire, validated with a global

sample of 5,575 employees from various countries and industries, identifying three key dimensions of digital trust in the workplace: technology (employee confidence in the reliability of workplace technologies), people (trust in colleagues, managers, support staff, and external stakeholders), and processes (effectiveness of mechanisms for data collection, processing, and protection).

We identified four major international comparative field studies on the evaluation of digital trust in the grey literature, indicating that organisations are increasingly relying on surveys and reports to assess and address digital trust challenges. In their 2024 *Global Digital Trust Insights Report*, PwC reveals that top executives plan to adopt generative AI tools for cyber defence despite perceiving them as a significant threat. PwC recommends implementing robust regulatory and governance mechanisms supported by their 'C-suite playbook' (PwC, 2024). Similarly, DigiCert's 2024 *State of Digital Trust Report* reveals that executives often overestimate their organisations' security levels. DigiCert proposes a four-step approach to strengthen digital trust: assess the current situation, define policies, centralise key infrastructure management, and set priorities (DigiCert, 2024). According to the Information Systems Audit and Control Association (ISACA, 2024), 80% of respondents view digital trust as essential for digital transformation, with its importance expected to grow over the next five years. However, only 20% plan to increase their budget for digital trust initiatives. While 27% report revenue benefits, there are other advantages identified, including an enhanced reputation (71%), more reliable decision-making (60%), and a reduction in privacy breaches (60%). Despite 94% of respondents recognising the importance of measuring digital trust, only 23% assess the maturity of their trust processes, even though it could cultivate consumer loyalty. Tufts University's Digital Intelligence Index evaluates digital trust using 197 indicators covering attitudes, behaviour, environment, and experience and has been applied to assess digital trust across 90 economies during the COVID-19 pandemic (Chakravorti *et al.*, 2020).

Support: How to support industry

Digital trust is a complex and relatively new concept for many industry sectors. Building digital trust requires a holistic approach that focuses on human factors while also considering technical and regulatory issues and broader industry, state and social considerations. Clear leadership at the executive level, along with a resource commitment, is essential to implementing activities that increase digital trust.

What did interviewees say about needed support industries in digital trust building?

Given the novelty and complexity of the topic, interviewees expressed a clear consensus on the need for support to actively build digital trust where appropriate and identified three types of support as useful:

a) General awareness campaigns
b) Generic support that is useful across contexts
c) Support tailored to specific needs

Table 4 *Industry support options*

What kind of support would be helpful in your working environment to promote digital trust?
General awareness campaign
Awareness campaigns in industry sector
Generic support across different contexts
Checklist for professionals
Qualitative and quantitative studies for decision-makers
Understanding best practice examples from abroad
Tailored support to specific needs
Active promotion of digital trust by decision-makers
Counselling services

General awareness campaign

Alongside the shifts that companies in the digital economy must make to integrate digital trust as a core value, engaging in broader awareness-raising efforts offers multiple benefits. Raising awareness of digital services among employees and in society more broadly advances digital skills, literacy, and hygiene, enabling users to make informed decisions about data sharing and use while developing the ability to assess the trustworthiness of data flows. Awareness raising can be facilitated by communication strategies and included in employee training and governance structures.

Generic support across different contexts

Checklists that convey the key conditions for digital trust can assist those in charge of implementing measures to build digital trust. A checklist with guiding questions can further support critical reflection on the topic and the development of tailored solutions within the specific company context. Comparative studies and best practice examples can complement these checklists by conveying the benefits and drawbacks of various measures to build digital trust.

Tailored support to specific needs

Combining internal and external support for digital trust building requires actively promoting digital trust by company decision-makers alongside external counselling services that provide tailored support to meet the company's needs.

Next steps: Recommendations for future research and development

We identified five major avenues for future research during the literature review and interview study:

1. Knowledge transfer from global banking services and cyber defence to other industry sectors
2. Evaluation methods for trustworthiness and digital trust
3. Awareness raising among the executive level and digital hygiene
4. Development of industry support tools and methods to build digital trust
5. Integration of digital trust building principles in governance and administration

Future research should contribute to a deeper understanding of what digital trust is, how it can be promoted and safeguarded, and how it can be transformed from an abstract concept into an actionable target value. *Appendix 3* provides a more elaborated research proposal aiming to make the five research avenues actionable.

Knowledge transfer from Global Banking Services and Cyber defence to other industry sectors
The interviews revealed varying levels of knowledge and experience regarding digital trust across industry sectors. The results indicate that industries such as a) global banking services, including credit card companies, and b) cyber (military) defence and intelligence services contain deep and comprehensive knowledge of what constitutes digital trust as well as how it can be promoted and safeguarded. This suggests that future research should explore ways to make this knowledge accessible and transferable to other sectors. Evidence-based conceptualisations are crucial for developing methods to promote, measure and effectively communicate about digital trust, as well as for evaluating the success of efforts to build it. Without a clear understanding of these aspects, building digital trust is hardly possible.

Evaluation methods for trustworthiness and digital trust
Mirroring the complexity and context specificity of digital trust, evaluation methods are not yet fully developed. Currently, evaluation relies on standard approaches such as market research and observation of sales figures that may or may not be associated with levels of digital trust. Also, 'the absence of negative media coverage' is an insufficient basis for determining the effectiveness of trust-building efforts. New methods need to be developed to enable a comprehensive evaluation of digital trust-building activities.

Awareness raising at the executive level and digital hygiene among employees
In the public context, a lack of digital literacy can increase distrust, while positive experiences with digital services, combined with improved digital literacy, ensure these services are better understood. Raising awareness among company executives and across society is an essential part of promoting digital trust in specific settings. Within companies, executives should receive targeted training on digital trust to build capacity; concurrent initiatives can raise employee awareness and increase their knowledge and ability to make informed decisions about whether to engage with digital services and how to navigate the digital sphere. Internal and external digital hygiene is crucial for companies to maintain the security and integrity of their digital services.

Development of industry support tools and methods to build digital trust
A range of support tools – such as checklists, self-assessment tools, and frameworks – need to be developed to help industry actors build digital trust. Support tools must be adaptable to specific contexts and useful across sectors.

Integration of digital trust-building principles in governance and administration
Digital trust-building activities should become integral to the core governance structures and corporate culture of companies and industry sectors. Only if digital trust is recognised as a meaningful performance indicator

linked to the success of a company will employees collectively act and build public trust. If digital trust remains a ‘nice-to-have’, trust-building efforts will be less effective.

Conclusion

The significance of digital trust in the digital economy and technology industry cannot be overstated: it plays a crucial role in ensuring users are willing to engage with digital services, share data, and establish long-term relationships with companies. As our study demonstrates, while knowledge about the concept of digital trust is still emerging across industries, its importance is universally recognised. Digital trust develops from the expectation that digital technologies, services, and providers will safeguard stakeholders’ interests and uphold societal values relevant to the society in which they operate.

Our research, involving a literature review and interviews with stakeholders from Switzerland and beyond, reveals that digital trust is perceived as a multi-faceted and complex construct promoted through a combination of human-centred, regulatory, compliance, and state-supported activities. However, building and maintaining digital trust requires strong leadership and commitment at the executive level, including the allocation of adequate resources and a corporate culture that prioritises trust.

Despite the recognised need for digital trust, its evaluation and measurability remain challenging. Our findings suggest that tailored approaches are necessary to effectively build digital trust across industries. Future research should focus on increasing awareness among executives, embedding the principles of digital trust building within corporate governance, and developing robust methods to evaluate digital trust. Knowledge from sectors with developed digital trust practices, such as global banking services and cyber defence, could be shared to provide insights to other industries, as outlined in Appendix 3.

As digitalisation continues and technological complexity grows, fostering digital trust will be vital for social cohesion and economic prosperity. A concerted effort to develop and implement trust-promoting measures will help ensure that digital environments are secure, reliable, and aligned with societal values, ultimately enhancing stakeholder confidence and engagement.

Study Methods

We developed a comprehensive research methodology to meet the study's objectives. This comprised a scoping review of scientific publications and grey literature on digital trust (Work Package 1 – WP1), as well as interviews with stakeholders from various industries (Work Package 2 - WP2).

WP1: State of knowledge in the literature regarding digital trust

We conducted a scoping review of 1) scientific publications and 2) grey literature to develop a sense of the current state of knowledge regarding the implementation, resource requirements and options to evaluate trust-promoting measures in the area of digital trust and business.

Research question: *What is the current state of knowledge regarding the implementation, resource requirements and evaluation options for trust-promoting measures in the area of digital trust and business?*

Methods:

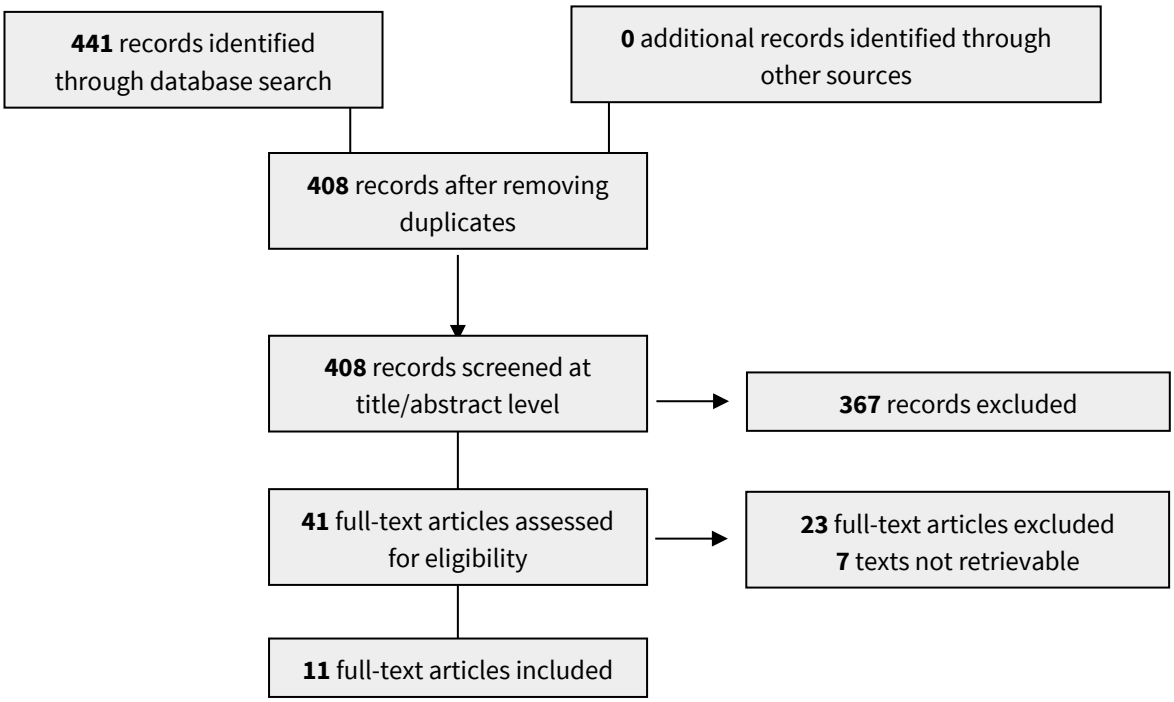
1) Scoping review of scientific publications

We developed a comprehensive strategy to search the Scopus, EBSCO, ACM, SSNR, PubMed, Lexcampus, and HeinOnline databases, which cover publications from the disciplines of medicine and public health, communication, computer science, law, and business. This approach aimed to develop a comprehensive view of the literature on 'digital trust' from a range of disciplines. We used the following search string, adjusted for each database:

> *"Digital Trust" AND ((evaluation OR assessment OR measurement OR analysis) OR (implementation OR adoption OR apply OR application OR implement OR intervention) OR (resources OR support OR programs OR services)) AND (LIMIT-TO (EXACTKEYWORD, "Digital Trust")) AND (LIMIT-TO (LANGUAGE , "English"))*

Our database search yielded 408 articles, which were screened by MM and FZ at the title and abstract levels. Of these, 367 articles were excluded, and 41 full-text articles were assessed for eligibility. The inclusion criteria were that the title or abstract mentioned the term 'digital trust' and referenced at least one of the following areas: implementation, resource allocation, and evaluation. This screening resulted in 11 full-text articles being included in the study as relevant (**Figure 1**; list of references for reviewed scientific papers in **Appendix 1**).

Figure 1 *Scoping review – study selection flowchart*



2) Scoping review of grey literature

We conducted a scoping review of grey literature by searching for references to the dimensions of implementation, resource allocation, and evaluation of digital trust on company webpages and in reports (grey literature listed in **Appendix 2**). The target companies were identified during stakeholder interviews and the scoping review of scientific publications. The organisations included are the following:

- *Cyber security and digital trust solutions*: Verisign, Appviewx, Luxtrust, DigiCert, Keyfactor, Safelayer Secure, Communications, Trustgrid, Jumio, Subex
- *Trust management, governance, and digital identity*: Intertrust, GLEIF (Global Legal Entity Identifier Foundation), Digital Trust Foundation, Swiss Digital Initiative (Digital Trust Label), SBP Digital Trust Consulting, Endera
- *Digital transformation, technology, and consulting*: IBM, PwC, Deloitte
- *E-signature and secure document management*: Docusign, Signzy Technology, Privy
- *Banking and financial services*: American Bankers Association, Mastercard
- *Industry governance and professional organisations*: ISACA
- *Cyber security risk management*: Motifworks

WP2: Current state of knowledge among key stakeholders in industry, society, politics and research regarding digital trust

From June to July 2024, FG conducted 30-minute online interviews in German and English with 16 key stakeholders to explore 1) whether there is a common understanding of the concept of 'digital trust'; 2) how digital trust can be promoted; 3) the resources needed to promote digital trust in practice; 4) modalities to evaluate digital trust; and 5) the support needed to promote digital trust.

Participants came from diverse sectors, including academia, pharmaceuticals, fintech, cyber defence, infrastructure, insurance, medicine, certification, and software companies, as well as government departments across Switzerland, Estonia, Germany, the United Kingdom, and the United States.

The online interviews were conducted on Zoom (version 5.17.11), audio-recorded and then transcribed by the same platform. Transcripts were then anonymised by FZ and uploaded to MaxQDA24, a software for qualitative research. FG coded the transcripts using reflexive thematic analysis to identify emerging themes. FZ reviewed the codes and reached an agreement with FG on the emerging themes identified to ensure the quality of the analysis. The study was conducted in compliance with the Declaration of Helsinki, and participants' consent was obtained in writing.

Study limitations

The scoping review of scientific studies and the grey literature focused on mapping the breadth of available literature rather than conducting an in-depth critical analysis. This may have resulted in an incomplete assessment of the quality of the studies included. Additionally, grey literature lacks the rigorous peer-review process typical of scientific publications, which may affect the reliability and validity of their findings. By contrast, interview studies provide rich, detailed insights into participants' experiences and perceptions of the researched topic, making them invaluable for understanding complex and emerging phenomena. However, the generalisability of interview studies is often limited due to their small sample size since qualitative research prioritises depth and context over statistical representation (Tong *et al.*, 2007). Interview studies thus offer valuable context-specific insights, which may not be universally applicable. During the study, we were aware of potential biases and made efforts to mitigate them, as explained in **Table 5**.

Table 5 *Bias mitigation*

Biases	**Explanation**	**Mitigation**
Interview Study		
Confirmation bias	Moderator focuses on interview answers supporting their own opinions.	We employed neutral and open-ended questions and structured questioning techniques. Coding frameworks were applied to ensure responses were analysed objectively. Interviews were pilot tested to identify and rectify any questions or moderation techniques that might inadvertently lead participants towards particular responses.
Interpretation bias	Researcher misinterprets results based on their own views.	We involved a second researcher to independently review the data, reducing the influence of individual perspectives. Regular discussions among researchers allowed cross-checking of interpretations and ensured that multiple viewpoints were considered.
Moderator bias	Moderator influences participants' opinions.	We used neutral, open-ended questions to avoid leading participants towards specific answers and maintained a non-judgemental tone throughout the discussions. We also pilot tested the interview to identify any biases in questioning or moderation techniques and made adjustments as needed.
Sampling bias and selection bias	Participants do not represent the broader society and are chosen to favour opinions.	Participants were purposively sampled to ensure diverse perspectives from industries in Switzerland and abroad on digital trust, ensuring a balanced representation of key sectors rather than favouring specific opinions.
Social desirability bias	Participants say what is socially acceptable and not their own views.	We assured participants that their responses would remain confidential and anonymous, creating a safe environment for them to express their opinions without fear of judgment. We also used neutral, non-leading questions to avoid steering participants towards answers they might perceive as more socially acceptable. Moderators also maintained a non-judgemental and neutral tone throughout the discussions, encouraging honesty.

Technical bias	Technology affects participants' answers.	We ensured that all participants had access to reliable and familiar technology during the interviews, minimising the potential impacts of technological difficulties on their responses. Participants were provided with clear instructions and support before the sessions to ensure they were comfortable with the digital tools being used. Additionally, the moderation process remained flexible, allowing for breaks or adjustments if technical issues arose, ensuring that participants were not rushed or influenced by technological interruptions.

References

Al-Hujran, Omar *et al.* (2015) 'The Imperative of Influencing Citizen Attitude Toward E-Government Adoption and Use', *Computers in Human Behavior*, 53, pp. 189–203. https://doi.org/10.1016/j.chb.2015.06.025.

Asia Insurance Review (2010) Technical Feature - IT in Insurance : Using Digital Trust Tto Create Industry Value. https://www.asiainsurancereview.com/Magazine/ReadMagazineArticle?aid=8132.

Bashir, I. and Madhavaiah, C. (2015) 'Consumer Attitude and Behavioural Intention Towards Internet Banking Adoption in India', *Journal of Indian Business Research*, 7(1), pp. 67–102. https://doi.org/10.1108/JIBR-02-2014-0013.

Cao, Q. H., Khan, I, Farahbakhsh, R, Madhusudan, G, Lee, G.M. and Crespi, N (2016) 'A Trust Model for Data Sharing in Smart Cities', in *2016 IEEE International Conference on Communications (ICC)*. *ICC 2016 - 2016 IEEE International Conference on Communication*s, Kuala Lumpur, Malaysia: IEEE, pp. 1–7. https://doi.org/10.1109/ICC.2016.7510834.

Chakravorti, Bhaskar, et al. (2020) Digital in The Time Of Covid - Trust in the Digital Economy and Its Evolution Across 90 Economies as the Planet Paused for a Pandemic. https://digitalplanet.tufts.edu/wp-content/uploads/2022/09/digital-intelligence-index.pdf

DigiCert (2024) *State of Digital Trust Report 2024*. https://www.digicert.com/campaigns/digital-trust-survey.

Febriyanti, Riska. *et al.* (2023) 'Predicting the Effect of Digitalization and Brand Trust on Customers' Saving Intention of Islamic Banking', *Asian Journal of Economics, Business and Accounting*, 23(20), pp. 78–91. https://doi.org/10.9734/ajeba/2023/v23i201093.

Gille, F. (2023) What is Public Trust in The Health System?: Insights into Health Data Use. Policy Press. https://doi.org/10.51952/9781447367352.

Illes, Katalin and Mathews, Martin (2015) Leadership, Trust and Communication: Building Trust in Companies Through Effective Leadership Communication. https://westminsterresearch.westminster.ac.uk/download/7a79d9b5cda6987091b70feaad66f167ae97c4a31b775c1ea26b3b9fadc91ba6/637036/Trustreport-1.pdf.

Information System Authority (2024) Cyber Security in Estonia 2024. https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf.

ISACA (2024) 'New ISACA Research: Many Organizations Believe Digital Trust Will Become More Important, Yet Budget, Strategy, Skills Lagging'. https://www.isaca.org/about-us/newsroom/press-releases/2024/many-organizations-believe-digital-trust-will-become-important-yet-budget-strategy-skills-lagging.

Jacobson, T. (2018) 'How to Build Digital Trust' https://www.destinationcrm.com/Articles/Columns-Departments/The-Tipping-Point/How-to-Build-Digital-Trust-125436.aspx.

Kaur, Simran Jit, *et al.* (2021) 'Adoption of Digital Banking Channels in an Emerging Economy: Exploring the Role of In-Branch Efforts', *Journal of Financial Services Marketing*, 26(2), pp. 107–121. https://doi.org/10.1057/s41264-020-00082-w.

Kioskli, Kitty. *et al.* (2023) 'The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0', *Applied Sciences*, 13(6), p. 3410. https://doi.org/10.3390/app13063410.

Kluiters, L., Srivastava, M. and Tyll, L. (2023) 'The Impact of Digital Trust on Firm Value and Governance: An Empirical Investigation of US Firms', *Society and Business Review*, 18(1), pp. 71–103. https://doi.org/10.1108/SBR-07-2021-0119.

Ko, Guihan*, et al.* (2022) 'Non-Market Strategies and Building Digital Trust in Sharing Economy Platforms', *Journal of International Management*, 28(1), p. 100909. https://doi.org/10.1016/j.intman.2021.100909.

Launer, M., Çetin, F. and Paliszkiewicz, J. (2022) 'Digital Trust in The Workplace: Testing a New Instrument on a Multicultural Sample', *Forum Scientiae Oeconomia*, (10), pp. 30–47. https://doi.org/10.23762/FSO_VOL10_NO1_2.

Luhmann, N. (2009) Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität. 4. Aufl., *UTB für Wissenschaft Soziologie fachübergreifend*. 4. Aufl. Lucius&Lucius.

Mbama, Cajetan Ikechukwu, *et al*. (2018) 'Digital Banking, Customer Experience and Financial Performance: UK Bank Managers' Perceptions', *Journal of Research in Interactive Marketing*, 12(4), pp. 432–451. https://doi.org/10.1108/JRIM-01-2018-0026.

Melnyk, V. (2024) 'Transforming the Nature of Trust Between Banks and Young Clients: From Traditional to Digital Banking', *Qualitative Research in Financial Markets*, 16(4), pp. 618–635. https://doi.org/10.1108/QRFM-08-2022-0129.

Pietrzak, P. and Takala, J. (2021) 'Digital Trust – A Systematic Literature Review', *Forum Scientiae Oeconomia*, (3), pp. 59–71. https://doi.org/10.23762/FSO_VOL9_NO3_4.

PwC (2024) Global Digital Trust Insights 2024, Genai for Cyber Defence is on the Rise. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.

Rantos K, Spyros A, Papanikolaou A, Kritsas A, Ilioudis C, Katos V.. (2020) 'Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem', *Computers*, 9(1), p. 18. https://doi.org/10.3390/computers9010018.

Saif, Mashaal A. M., Nazimah Hussin, Maizaitulaidawati Md Husin, Ayed Alwadain, and Ayon Chakraborty (2022) 'Determinants of the Intention to Adopt Digital-Only Banks in Malaysia: The Extension of Environmental Concern', *Sustainability*, 14(17), p. 11043. https://doi.org/10.3390/su141711043.

Swiss Digital Initiative (2021) Digital Trust From The Customer's Perspective. https://digitaltrust-label.swiss/wp-content/uploads/2021/11/booklet-digital-trust.pdf.

World Economic Forum (2022) Earning Digital Trust: Decision-Making for Trustworthy Technologies. Geneva. https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

Wylde, A. (2021) 'Zero Trust: Never Trust, Always Verify', in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. Dublin, Ireland: IEEE, pp. 1–4. https://doi.org/10.1109/CyberSA52016.2021.9478244.

Appendix 1: List of reviewed paper

Asia Insurance Review. (2010). Using digital trust to create industry value. *Technical Feature—IT in Insurance*. https://www.asiainsurancereview.com/Magazine/ReadMagazineArticle?aid=8132

Asprion, P., Grieder, H., Grimmberg, F., and Moriggl, P. (2023). Building digital trust to protect whistleblowers—A blockchain-based reporting channel. *Proceedings of the 56th Hawaii international conference on system sciences*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2023.528

Jacobson, T. (2018, 1 June). How to build digital trust. *Customer Relationship Management*. https://www.destinationcrm.com/Articles/Columns-Departments/The-Tipping-Point/How-to-Build-Digital-Trust-125436.aspx

Ko, G., Amankwah-Amoah, J., Appiah, G., and Larimo, J. (2022). Non-market strategies and building digital trust in sharing economy platforms. *Journal of International Management*, *28*(1), 100909. https://doi.org/10.1016/j.intman.2021.100909

Launer, M., Çetin, F., and Paliszkiewicz, J. (2022). Digital trust in the workplace: Testing a new instrument on a multicultural sample. *Forum Scientiae Oeconomia*, *10*, 30–47. https://doi.org/10.23762/FSO_VOL10_NO1_2

Mazzella, F., Sundararajan, A., Butt d'Espous, V., and Möhlmann, M. (2016). How digital trust powers the sharing economy: The digitization of trust. *IESE Insight*, *30*, 24–31. https://doi.org/10.15581/002.ART-2887

Mo, Z., Liu, Y., Lu, C., and Yu, J. (2023). Influences of industrial internet platform firms' ESG performance and digital leadership on user firms' innovation performance: The mediating role of inter-firm trust. *Journal of Digital Economy*, *2*, 204–220. https://doi.org/10.1016/j.jdec.2024.01.002

Montezuma, L. A., Schmidt, C., and Loke, Q. L. (2019). The digital trust deficit and principles on how to restore digital trust. *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, *3*(8), 13–16.

Moulaei, K., and Bahaadinbeigy, K. (2023). Challenges and opportunities of digital trust in the healthcare industry. *Frontiers in Health Informatics*, *12*, 140. https://doi.org/10.30699/fhi.v12i0.437

Rane, T., and Huang, J. (2023). Blockchain-based digital trust mechanism: A use case of cloud manufacturing of LDS syringes for COVID-19 vaccination. *Journal of Integrated Design and Process Science*, *26*(2), 103–129. https://doi.org/10.3233/JID-210021

Seleznyov, A., Ahmed, M. O., and Hailes, S. (2004). Co-operation in the digital age—Engendering trust in electronic environments. *BT Technology Journal*, *22*(3).

Appendix 2: List of grey literature

Chakravorti, B., Chaturvedi, R.S., *et al.* (2020) *Digital in the time of COVID – Trust in the digital economy and its evolution across 90 economies as the planet paused for a pandemic*. https://digitalplanet.tufts.edu/wp-content/uploads/2022/09/digital-intelligence-index.pdf.

digicert. (2024). *2024 State of digital trust report* (pp. 1–24). https://www.digicert.com/content/dam/digicert/pdfs/report/2024-state-of-digital-trust-survey-report-en.pdf

ISACA. (2024). *State of digital trust 2024* (pp. 1–25). https://www.isaca.org/resources/reports/state-of-digital-trust-2024

PwC. (2024). *The C-suite playbook: Putting security at the epicenter of innovation. Findings from the 2024 Global Digital Trust Insights* (pp. 1–20). https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights/pwc-2024-global-digital-trust-insights-main-report.pdf

Appendix 3: Future research and development avenues

An overview of possible avenues for research and development on the needs identified in the pilot study. Fundamental to all research will be a comprehensive understanding of what digital trust is in the context of interest, as insufficient conceptual research undermines attempts to build and evaluate digital trust.

A.3.1.: Knowledge transfer from (Global) Banking Services and Cyber defence to other industry sectors

(Global) banking and military cyber defence, including intelligence services, appear to have considerable digital-trust know-how. Transferring this to other industries is a valuable and economically efficient way to inform cross-industry activities and build digital trust. Building on existing and practice-proven experiences and knowledge avoids unnecessary duplication of effort. We suggest the following approach to facilitate the knowledge transfer.

Research Questions

R1: What are the core principles for building and maintaining digital trust in the banking and cyber defence industries?
R2: How can these principles be translated to other industries?
R3: What are the challenges and opportunities for cross-industry transfer of these best practices?

Objectives

O1: Identify the key principles of digital trust in banking and cyber defence (e.g., data privacy, security protocols, compliance).
O2: Analyse successful frameworks used in these industries (e.g., cybersecurity frameworks, regulatory compliance) to build and maintain digital trust.
O3: Explore the challenges faced by these industries in building digital trust.
O4: Develop a transfer model that applies the various insights to other sectors.

Methodology

Primary Research

Conduct interviews and surveys with industry experts from banking and cyber defence. Review industry reports, case studies, and academic papers on digital trust and government regulation.

Framework Development

Develop a conceptual digital trust framework and identify key elements that can be adapted to other industries.

Gap Analysis

Compare current practices in other industries (e.g., retail, logistics, healthcare) with those in banking and cyber defence, and identify gaps in technology, policy, and processes that hinder efforts to build digital trust.

Knowledge Transfer Mechanisms

Workshops & Seminars

Organize cross-industry workshops involving stakeholders from banking and cyber defence. Develop industry-specific training materials on adopting digital trust strategies in other sectors.

Cross-industry Collaboration

Foster collaboration between the banking and cyber defence sectors and sectors such as healthcare, retail, and logistics to create a shared knowledge base (e.g., creating a consortium for digital trust).

Tailored Frameworks

Design industry-specific digital trust toolkits based on the banking and cyber defence models. Provide adaptation guidelines for smaller organizations in less regulated sectors.

Expected Outcomes

1. *Framework*: A customizable digital trust framework for industries like healthcare, retail, and logistics.
2. *Best Practice Guidelines*: Guidelines for adopting key elements from the banking and cyber defence sectors, such as identity management systems and incident response planning.

A.3.2.: Evaluation methods for digital trust

Evaluation of digital trust and user perceptions of a company's trustworthiness is important to understand a) levels of trust and b) the extent to which resources allocated to trust building are effective. Economic evaluation is often neglected in trust building but remains an important step in the evaluation process.

Research Question

R1: What evaluation methods for trustworthiness and digital trust work in practice?

Objectives

O1: Develop a conceptual understanding of digital trust.
O2: Develop evaluation methods
O3: Pilot-test the evaluation methods in practice
O4: Refine the evaluation methods based on the results of O3.

Methodology

Primary Research

Conduct a mixed-methods study following existing evaluation and measurement-development methodologies.

Framework Development

Develop a conceptual digital trust framework as the basis for evaluation and measurement.

Expected Outcomes

1. *Framework*: A digital trust framework for the development of evaluation methods
2. *Evaluation methods* for digital trust.

A.3.3.: Awareness raising among the executive level and digital hygiene

Our findings suggest that, for most of the industry executives interviewed, digital trust is a topic that appeared on their agenda in the course of the last two to three years. Given the importance of digital trust (and the closely linked digital hygiene) in most industries, awareness raising is a valuable way to promote the topic and offer guidance where needed. Utilising the SATW networks, it is worth considering awareness initiatives in different formats. The interviewees mentioned two formats as being particularly useful: a) general awareness campaign and b) efforts tailored support to specific needs. Both should reach executives and convey necessary information about digital trust and digital hygiene.

Research Question

R1: How can awareness of digital trust and digital hygiene be raised at the executive level?

Objectives

O1: Develop a conceptual understanding of digital trust.
O2: Develop awareness-raising strategies targeting executives.
O3: Roll out awareness-raising initiatives.
O4: Evaluate the success of awareness-raising initiatives.

Methodology

Primary Research
Develop an awareness-raising strategy, including implementation and evaluation.

Framework Development
Develop a conceptual digital trust framework as the basis for awareness raising.

Expected Outcomes

1. *Strategy to raise awareness* about digital trust and digital hygiene.
2. *Roll out* of awareness-raising initiative.
3. *Evaluation* of awareness-raising initiative.
4. *Increased awareness* among executives about digital trust and digital hygiene.

A.3.4.: Development of industry support tools and methods to build digital trust
Executives and those in charge of building digital trust will need guidance, ranging from generic information and tools such as checklists to tailored consultancy solutions.

Research Question
R1: What tools and methods can aid executives in the development of digital trust in practice?

Objectives
O1: Develop a conceptual understanding of digital trust.
O2: Review existing methods in other trust research that are potentially transferable to the digital trust domain.
O3: Develop digital trust-building methodologies.
O4: Pilot test trust-building methodologies in practice.
O5: Refine the evaluation methods based on the results of O4.

Methodology

Primary Research
Conduct a study to review existing tools and co-develop tools with industry partners.

Framework Development
Develop a conceptual digital trust framework as the basis for support tools and methods.

Expected Outcomes

1. *Actionable tools and methods* to build digital trust in practice.

A.3.5.: Integration of trust building principles in governance and administration
Connected to A.3.4. (development of industry support tools and methods to build digital trust), trust-building principles should be integrated into corporate governance and administration. The process of integration into existing governance structures or the integration of trust building principles during the process of designing new governance structures should be supported with tailored guidance.

Research Question
R1: How can trust building principles be integrated into governance and administration?

Objectives
O1: Develop a conceptual understanding of digital trust.
O2: Integrate trust building principles in governance and administration.
O3: Evaluate the integration.

Methodology

Primary Research
Conduct a case-study project with industry partners.

Framework Development
Develop a conceptual digital trust framework to integrate digital trust-building principles in governance and administration.

Expected Outcomes
1. *Framework*: A digital trust framework for the integration of digital trust-building principles in governance and administration.

Appendix 4: Digital Trust Q&A

Person

- *Why is digital trust needed?*

As society and industry continue to digitalise and adopt new technologies, trust has become increasingly critical. The growing complexity of our personal and professional environments, driven by digitalisation, often makes it hard for individuals to understand these developments. We need mechanisms to manage this complexity and maintain our capacity to act effectively within it. Digital trust is one such mechanism for navigating the digital economy. It is fundamental to the successful implementation and widespread adoption of digital technologies, particularly within the service sector. Digital trust drives the use of digital services, encourages engagement, and increases sales.

- *Who trusts whom in a digital trust relationship?*

In the context of data use, digital trust is a relational concept: Party A places trust in Party B to handle their data securely and confidentially, with the expectation of a beneficial outcome for either the trusting party, both parties or even the broader sector. Given that digital trust is situation specific, it is essential to analyse its context and the network of actors influencing the trust relationship. This requires asking two key questions: a) Who trusts whom? and b) Who influences the trust relationship? The perspective adopted in the trust analysis significantly shapes how the concept is understood. Are we considering the perspective of users, providers, or that of the state or company? Answering these questions can help companies identify the contextual factors that influence the trust relationship, allowing trust-building strategies to be tailored accordingly.

- *What promotes trust in the digital space? What influence does transparency have?*

Interviews with key stakeholders revealed four main factors promoting digital trust: data security, privacy protection, adherence to technical standards, and traceability. Data security builds trust by ensuring data are protected from unauthorised access, while privacy protection promotes user engagement by safeguarding personal information. Trust allows users to engage with technology without constant concern over security and privacy. The implementation of technical standards and the ability to trace the use of data enhance accountability and transparency, further supporting trust. Interviewees also highlighted compliance-centred approaches, such as auditing and certification processes, which increase transparency and thereby contribute to overall trust.

- *What influence does people's digital competence have on their perception of digital trust?*

Low levels of digital literacy and human error can undermine digital trust and harm a company's reputation, making employee training crucial. High standards of digital hygiene in companies and society are essential for safeguarding data and personal identity. Free, government-provided digital advice services can improve digital literacy and support companies in strengthening their digital governance. Additionally, well-developed e-governance systems promote digital literacy at a societal level by encouraging the routine use of digital services in everyday life. That said, higher levels of digital literacy also contribute to the ability to critically assess digital services and to build 'healthy levels of mistrust'.

Organisation

- *What digital trust governance frameworks already exist? What makes them different, and what do they have in common?*

Publications frequently discuss the implementation of digital trust strategies, with eight out of 11 articles addressing this topic. Many of these studies propose theoretical models to enhance and understand trust mechanisms. Similarly, the grey literature places significant emphasis on trust building, with numerous organisational materials, such as whitepapers, brochures, case studies, and reports, underscoring the importance of digital trust and the need for concrete action. The frameworks identified were primarily presented in the context of digital trust evaluation. The scientific literature tends to focus on instruments for measuring digital trust at the micro level, such as workplace assessment frameworks. By contrast, the grey literature takes a macro perspective, examining digital trust across industries and offering practical insights into governance, cybersecurity, and organisational strategies. However, the present study did not identify any concrete or widely accepted digital trust governance frameworks.

- *How can these be implemented, and what skills are needed?*

Interviewees emphasised that building digital trust requires a coordinated effort across several organisational units led by executive management. Key departments involved include customer service, human resources, financial services, sales, legal, IT, and engineering, areas considered pivotal for internal and external human interactions. Transparent, open, and targeted communication ties these units together as the foundation of digital trust. Internally, cultivating a culture of open communication is essential to encourage employees to raise issues and identify problems. Externally, clear communication with customers and business partners is critical to demonstrating the benefits of data usage and ensuring transparency in data governance.

- *For which companies/organisations/projects/use cases are investments in digital trust particularly important?*

Investments in digital trust are critical across industries, especially in sectors that handle sensitive or high-volume data flows. Key sectors include healthcare, defence, mobility, insurance, education, banking, and consumer markets. As artificial intelligence becomes increasingly integrated into business operations, digital trust will play an even more central role. Artificial intelligence brings new digital risks, making it essential for boards of directors and leadership teams to align their digital trust strategies with broader digital transformation and other key initiatives.

- *How is financing for implementation typically organised?*

Our research does not provide specific insights into how financing for digital trust-building initiatives is typically organised. However, based on interviews with key stakeholders, we have identified several areas where budgetary resources could be effectively allocated. These include human- and compliance-centred approaches, engineering-based strategies, and government-driven initiatives. While the literature makes clear that resources such as time, capital, expertise, and workforce are essential for building and sustaining digital trust, the precise mechanisms for financing these efforts remain underexplored.

- *Is there any relevant financial experience in this area? When is investing in digital trust 'worth it' from an economic point of view?*

According to ISACA's January 2024 global *State of Digital Trust* survey of approximately 137,000 individuals in various sectors, including banking, finance, consulting, and government, 27% of respondents indicated that high levels of digital trust could lead to increased revenues, suggesting that prioritising digital trust within organisations can yield financial benefits. Other advantages identified include enhanced reputation (71%), more reliable decision-making (60%), and a reduction in privacy breaches (60%). Despite 94% of respondents recognising the importance of measuring digital trust, only 23% of organisations actually measured their digital trust maturity. However, 68% agreed that assessing the maturity of their organisation's digital trust practices was highly important. A cost–benefit analysis could support investment in digital trust initiatives, given the significant potential for increased profits and operational efficiencies.

Technologies

- *What technological solutions already exist that promote digital trust? How are these implemented? To what extent are they already being evaluated? Where does cybersecurity play a role, and what is that role?*

The study shows that well-engineered IT infrastructures that incorporate privacy by design and robust cybersecurity measures are crucial for fostering trust in the digital economy. This aligns with the four trust-building themes identified by interviewees, namely: data security (which requires a strong cybersecurity infrastructure to protect sensitive data and build trust), privacy protection, adherence to technical standards and traceability of data access (which strengthens accountability and transparency).

In terms of evaluation methods, interviewees proposed the development of 'trust stress tests' to assess the resilience of companies or services against hostile activities – whether internal or external – that could undermine digital trust. More conventional approaches include comparative studies evaluating the performance of different digital services in building and maintaining trust. Anchoring digital trust in KPIs was also recommended to facilitate comparison and assess whether digital trust has been effectively developed. One suggestion was to link digital trust to the performance assessments of executive boards via KPIs. Central to all evaluation methods is their relevance to the process of developing digital trust and their capacity to drive change where needed. The literature reveals a divergence in approaches to evaluating digital trust. While

scientific studies focus on developing instruments to measure digital trust at the micro level, for example, in workplace assessment frameworks, the grey literature adopts a macro-level perspective, examining trust across entire industries and offering practical insights into governance, cybersecurity, and organisational strategies. Communication is consistently recognised as key in the evaluation of trust: transparent communication helps identify issues that may erode trust, and the right narratives are essential for building it. However, no definitive evaluation instruments were identified in the literature review.