

Towards a Comprehensive Evaluation of Trust Frameworks for Data Spaces

Evaluation Methodology and Criteria

Title: Towards a Comprehensive Evaluation of Trust Frameworks for Data Spaces
Authors: Dr. B. (Bernadette) Farias Lóscio, P. (Pim) Mulder. MSc (TNO)
Date: July 2025
pages: 36 (excl. front and back page)
annexes:

Management Summary

As data spaces become central to Europe's Data Strategy, the ability to credibly share data between organizations is paramount. However, a key challenge is the lack of a common language for standardized guidelines to evaluate the effectiveness and completeness of existing trust frameworks. This ambiguity makes it difficult for organizations to select the optimal solution to foster a truly trustworthy environment.

This report introduces a future-proof model to systematically assess trust frameworks within a data sharing environment. This enables data space stakeholders to identify strengths and weaknesses in the creation of trust frameworks within a data sharing environment. As a result, we have created a model that exposes the dynamics of trust. It relies on the data sharing trust triangle and data sharing trust concerns.

The data sharing trust triangle describes the three pillars that build trust. This model is the foundation for a practical assessment method. It is an intuitive model that dissects the complex concept of trust into three essential, interdependent components. To remain future proof, this model provides a holistic view, rather than purely technical checks. The pillars are:

- *Empathy*: This pillar ensures the participants, and the trust framework operate in a manner that is fair, transparent, and accountable to all stakeholders. It relates to clear governance, equitable rules, effective dispute resolution, and demonstrable respect for data sovereignty and privacy.
- *Dependability*: This pillar addresses the reliability of the technical system itself. It covers the performance, availability, security, and resilience of the data space's underlying infrastructure and services.
- *Integrity*: This pillar focuses on the trustworthiness and quality of the data involved. It ensures data is authentic, accurate, and comes from verified sources, and that its provenance can be traced.

What makes this model novel is its inclusion of the "Empathy" dimension and its recognition that the operational aspects of the trust framework itself can either increase or decrease trust.

These driving factors are combined with the data sharing concerns – the barriers, such as distrust in data quality and compliance, that hinder stakeholders from sharing data. These concerns were systematically collected through an ad-hoc literature review.

The combination of the driving factors and concerns were then translated into practical first-person "user stories", each describing a participant's expectation for a trustworthy data transaction. Finally, each user story was used to derive a detailed list of concrete, verifiable requirements. While these requirements reflect currently available technology, the framework is designed for evolution, with provisions for adopting state-of-the-art technologies as they emerge. This two-step process ensures that every requirement is traceably linked back to a specific stakeholder concern.

As a result, organizations can use this methodology to make informed decisions when establishing a data space or to make targeted improvements to enhance partner confidence. A key aspect of this is the ability to assess a framework's design for interoperability, allowing organizations to select and combine frameworks to support larger data ecosystems. Similarly, trust framework operators can strategically position themselves based on our model.

Table of Contents

Management Summary	3
Table of Contents	4
1 Introduction.....	5
2 Trust and trust frameworks for data spaces.....	7
2.1 Layers of trust within a data space	8
2.2 Data sharing trust triangle.....	8
2.3 Data sharing concerns	10
3 Trusted data transactions: user stories.....	12
3.1 Pre-transfer phase	12
3.2 Discovery & Negotiation.....	12
3.3 Data transfer & Usage	13
3.4 Post-transfer phase.....	13
4 Operational concerns of trust frameworks	15
4.1 Adaptivity.....	15
4.2 Technological Assurance.....	15
4.3 Availability & Transparency.....	15
4.4 Extraterritoriality	16
4.5 Reliability (of Operator/Business)	16
4.6 Continuity	16
4.7 Sector Specific	17
5 A method for assessing trust frameworks.....	18
5.1 Dependability Requirements.....	19
5.2 Integrity Requirements.....	19
5.3 Empathy Requirements	20
5.4 Operational Requirements	20
6 Conclusion.....	22
References	23
Appendix A - Requirements for assessing trust frameworks	24
A.1 Capability requirements	24
A.2 Operational requirements	27
Appendix B – Guiding questions for the requirements evaluation	30
Appendix C – Research Method	36
Colofon	37

1 Introduction

Recent advancements in the data spaces landscape have transitioned from theoretical frameworks to practical, market-ready solutions, fostering global adoption and cross-sector innovation. The introduction of the Data Spaces Support Centre (DSSC) Blueprint and Toolbox¹ has significantly accelerated the deployment and operationalization of data spaces across various industries. Additionally, the development of standards and protocols are making data sharing more secure, scalable, and accessible, positioning data spaces as a cornerstone for trustworthy data ecosystems in Europe and beyond (Gieß et al., 2024).

Despite significant advancements in the data spaces landscape, sharing data between unknown partners still presents various challenges. One of the most critical issues is the establishment and maintenance of trust among parties. For example, data consumers may have concerns about data quality and provenance. Meanwhile, data providers want to ensure their data is used according to pre-defined access and usage policies. To bridge these concerns, a trust framework may be established to outline the agreements for data sharing.

According to (Temoshok & Abruzzi, 2018), a trust framework is “a generic term used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements”.

On one hand, although trust frameworks for data spaces are an important subject, there is a lack of guidelines to assist their assessment helping the identification of their strengths, but also possible gaps and points for improvements. These assessments become even more challenging due to the lack of a common understanding of the fundamentals of trust and trust frameworks for data spaces. On the other hand, there is a demand from data sharing initiatives on assistance for selecting trust frameworks that best suit their needs.

This report introduces a method to systematically assess trust frameworks within a data sharing environment. The proposed method relies on the data sharing trust triangle and data sharing trust concerns. The data sharing trust triangle describes the three pillars, also named driving factors, to build trust among the data space’s participants: dependability, integrity and empathy. Empathy relates to clear governance, equitable rules, effective dispute resolution, and demonstrable respect for transparency, data sovereignty and privacy. Dependability covers the performance, availability, security, and resilience of the data space’s underlying infrastructure and services. Integrity focuses on the trustworthiness and quality of the data being shared. It ensures data is authentic, accurate, and comes from verified sources, and that its provenance can be traced.

These driving factors are combined with the data sharing concerns – the barriers, such as distrust in data quality, compliance and interoperability, that hinder stakeholders from sharing data. These concerns, systematically collected through an ad-hoc literature review, reflect general issues raised by data space participants when sharing data. The relevance of each concern may vary accordingly to the domain. For example, in the health domain the quality of the data may be crucial as well as the confidentiality of sensitive data. We do not claim that the set of data sharing concerns is complete, but at least it reflects crucial data sharing concerns.

The combination of the driving factors and concerns were then translated into practical first-person “user stories”, each describing a participant’s expectation for a trustworthy transaction. Finally, each user story was used to derive a detailed list of concrete, verifiable requirements. While these requirements reflect currently available technology, the evaluation method is designed for evolution, with provisions for adopting state-of-the-art technologies as they emerge. This two-step process ensures that every requirement is traceably linked back to a specific stakeholder concern.

The requirements are the core components of the method. The evaluation’s result will show which requirements are met by the trust framework. This result can be helpful for both data space initiatives

¹ <https://dssc.eu/>

and trust framework developers. The method is flexible and when needed the proposed set of data sharing concerns and their corresponding requirements can be adjusted according to the requirements of a specific domain or data sharing initiative. The main characteristics of the proposed method are summarized in Table 1.1.

Table 1.1: Main characteristics of the trust framework evaluation method

Characteristic	Description
Motivation	The lack of guidelines and methods to assist trust frameworks assessment to identify their strengths, but also possible gaps and points for improvements.
Supporting definitions	A Trust Framework is the collection of artifacts that together promote trust through the reinforcement of the driving factors (Dependability, Integrity and Empathy) and the mitigation of data sharing concerns.
Goal & scope	Assessment of trust frameworks used to establish and maintain trust among participants of a data space.
Main audience	Data Space initiatives seeking to identify trust frameworks that best support their objectives, as well as trust framework developers aiming to assess the strengths and areas for improvement in their solutions.
Components	Trust framework requirements, Data sharing concerns, Trust framework operational concerns, Data sharing trust triangle
Supporting artifacts	Evaluation plan and data collection instrument (ex: survey).
Number of requirements	37 capability requirements and 27 operational requirements
Input	Trust framework documentation and other sources of information about the trust framework (ex: expert's knowledge).
Output	Report with evaluation results.

The remainder of this report is organized as follows. Section 2 presents definitions and concepts, including: definitions of trust and trust frameworks for data spaces, the layers of trust within a data space, the three key driving factors of trust that compose the Trust Triangle for Data Sharing, and the concerns of participants when sharing data in a data space. Section 3 presents a scenario describing the main steps of executing a trusted data transaction in a data space and a set of user stories extracted from this scenario. Section 4 focuses on the operational concerns of trust frameworks, i.e., concerns related to its own operationalization and reliability. Section 5 details the method for evaluating trust frameworks. Section 6 presents some conclusions.

2 Trust and trust frameworks for data spaces

Trust is a complex and multifaceted concept that spans multiple disciplines, including among others Sociology, Economics, Psychology and Computer Science (Rouhani & Deters, 2021), (Lim & Thing, 2024). Trust encompasses aspects of ethics, emotions and values.

Several definitions shed light on what trust means:

- (Cho et al., 2015) provides a summary of trust definitions stating that trust is “the willingness of the trustor (evaluator) to take a risk-based on a subjective belief that a trustee (evaluatee) will exhibit reliable behaviour to maximize the trustor’s interest under uncertainty (e.g., ambiguity due to conflicting evidence and/or ignorance caused by complete lack of evidence) of a given situation based on the cognitive assessment of past experience with the trustee”.
- (Mayer, Davis, & Schoorman, 1995) defines trust as: “...the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor—irrespective of the ability to monitor or control that other party.”.

To establish and maintain trust among parties, principles, protocols, and standards can be employed to ensure consistent and transparent trust practices. This can be done through a trust framework, which helps ensure that trust practices are consistent and clear. Van der Peet et al. (2024) explain that these frameworks show how different organizations and sectors aim to build trust and work together smoothly. A trust framework may be domain-specific²³, such as the one presented in (Brewer et al., 2021). Alternatively, more generic trust frameworks are also available, like those provided by iSHARE⁴ and Gaia-X⁵. While building a trust framework from scratch requires significant investments of time and money, using an existing framework can be a more efficient choice.

According to Joosten, “trust frameworks are meta-level mechanisms that establish principles, protocols, or standards designed to help parties achieve and maintain trust.” These frameworks often include key features such as i) Identity verification systems: Ensuring people or entities are who they say they are; ii) Standardized evaluation metrics: Providing objective ways to measure performance; and iii) Audit and compliance mechanisms: Monitoring adherence to agreed-upon standards.

According to (Temoshok & Abruzzi, 2018), a trust framework is “a generic term used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements”. Trust frameworks are used in various domains, such as cybersecurity, digital identity systems, and inter-organizational collaborations. In the context of data spaces, a trust framework is specifically used to foster confidence among all participants. Generally, these frameworks are supported by various elements, including formal documents, technical specifications, industry standards, communication protocols, and software components.

According to the DSSC⁶, a trust framework is “a composition of policies, rules, standards, and procedures designed for trust decisions in data spaces based on assurances. Trust framework is part of the data space governance framework”. In this work, we are aligned with the definitions previously presented.

² <https://medmij.nl/en/home/>

³ <https://directtrust.org/what-we-do/trust-framework>

⁴ <https://framework.ishare.eu/>

⁵ <https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/>

⁶ <https://dssc.eu/space/BVE2/1071252161/Alphabetical+List+of+All+Defined+Terms+in+Blueprint+v2.0>

2.1 Layers of trust within a data space

Trust is the cornerstone upon which successful data ecosystems are built. Without it, participants are unlikely to share valuable or sensitive data, thereby limiting the potential for innovation and value creation. Data spaces are often explicitly defined as "trusted" environments, and data owners require "specific and precise guarantees" regarding data protection and prevention of misuse before engaging in sharing activities. Indeed, the promise of technologies like Artificial Intelligence (AI) cannot be fully realized without access to "reliable and consent-based data," which necessitates a trusted framework for sharing.

Furthermore, trust mechanisms are essential for mitigating the inherent risks associated with data sharing, including data breaches, unauthorized use, and the erosion of data sovereignty. The historical breakdown of trust in existing data paradigms, often characterized by opaque data practices and a lack of user control, has been a significant driver for the development of data spaces that prioritize sovereign control and transparent governance.

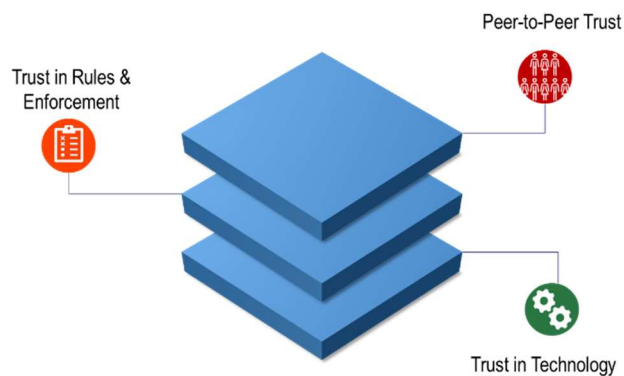


Figure 2.1: Layers of trust within a data space

It is important to recognize that trust in data spaces is not a monolithic or static attribute. Instead, it is dynamic and evolving confidence built and potentially eroded through ongoing interactions and experiences even outside data spaces themselves. This confidence operates at multiple levels as illustrated in Figure 2.1: between individual participants (peer-to-peer trust), between participants and the data space infrastructure (trust in technology), and between participants and the overarching governance framework (trust in rules and enforcement). The distinction between trust based on organizational policies and trust based on dependable technical guarantees highlights the need to assess and cultivate confidence across these various facets of interaction within the data space. Continuous reinforcement through verifiable mechanisms is therefore paramount.

2.2 Data sharing trust triangle

To systematically analyze and assess trust within data spaces, we focus on three key driving factors: Dependability, Integrity, and Empathy. These are essential factors to be incorporated when sharing data to effectively achieve trust within a data space. Together, these elements compose the Trust Triangle for Data Sharing and foster an environment of trust, ensuring participants that their data is secure, ethically managed, and transparently processed.

Our proposal of a Trust Triangle for Data Sharing, presented in **Figure 2.2**, is inspired by the works of Aristotle⁷ and Frances Frei and Anne Morriss (Frei & Morriss, 2020), which emphasize the importance of credibility, logical reasoning, and emotional connection in building trust in communication and leadership, respectively.

⁷ <https://plato.stanford.edu/entries/aristotle-rhetoric/>

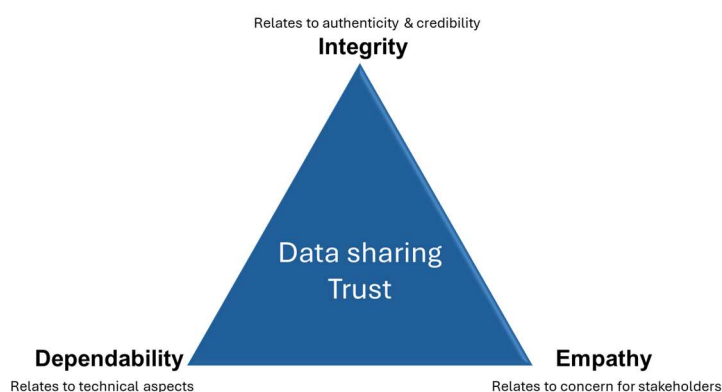


Figure 2.2: Data Sharing Trust Triangle

The Aristotle's rhetorical appeal also known as "Rhetorical Triangle" ⁸ can help us to clearly present our position in a persuasive way. Aristotle identified three methods of persuasion: *ethos*, which is an appeal based on credibility; *pathos*, which is an appeal based on emotions; and *logos*, which is an appeal based on logic.

The Aristotle's rhetorical triangle establishes the foundation for the trust triangle of leadership, proposed by (Frei & Morriss, 2020). Frances Frei and Anne Morriss adapted Aristotle's principles to the context of leadership. The trust triangle of leadership is composed of authenticity (aligning with *ethos*), logic (reflecting *logos*), and empathy (corresponding to *pathos*). In our proposal, **Dependability** corresponds to *logos* in Aristotle's model and **logic** in Frei's framework. **Integrity** aligns with *ethos* in Aristotle's model and **authenticity** in Frei's framework. **Empathy** relates to *pathos* in Aristotle's model and **empathy** in Frei's framework.

In the context of data spaces, **Dependability** (Technical) refers to the capability of the system to deliver its services reliably and securely. It encompasses several attributes, including the availability of the data space infrastructure and its services (e.g., connectors, catalogues, identity management systems), the reliability of data operations such as transfer, storage, and processing, the performance of the system in terms of latency and throughput, the security of the underlying technical infrastructure against unauthorized access and cyber threats, and the maintainability of the system components.

Integrity (Credibility and Authenticity) in data spaces pertains to the trustworthiness of the data itself and the participants involved in data transactions. This includes the accuracy, completeness, consistency, and timeliness of the data (data quality). It also encompasses the authenticity of data sources, the verifiability of data origin (provenance), assurance that data has not been improperly altered, and the verifiable identity of all participants engaging in the data space.

Empathy (in relation to stakeholders) in the context of data spaces refers to the design and operation of the ecosystem in a manner that is fair, transparent, accountable, and responsive to the needs, expectations, and rights of all its stakeholders. This includes the establishment of clear, equitable, and enforceable governance rules, transparent communication of policies and operational procedures, effective mechanisms for stakeholder engagement and feedback, fair dispute resolution processes, and a demonstrable respect for data sovereignty, privacy, and broader ethical considerations.

These three factors are deeply interrelated. For instance, a technically dependable infrastructure is a prerequisite for ensuring data integrity. Similarly, transparent governance and fair processes (empathy) are essential for building participant confidence in the dependability of the system and the integrity of the data shared. While dependability and integrity represent crucial technical and data-centric pillars of trust, empathy—manifesting as fairness, transparency, and robust stakeholder engagement—is increasingly recognized as a vital socio-organizational differentiator.

In complex, federated environments like data spaces, which involve diverse actors with potentially varied interests, such empathetic qualities can significantly influence adoption rates and the long-term sustainability of the ecosystem. Traditional systems often prioritize technical reliability and data accuracy. However, the collaborative nature of data spaces necessitates a stronger focus on these "softer" aspects of trust. The emphasis on "fair conditions and transparent rules" in DSSC

documentation and the embedding of "European values" like openness and data protection in initiatives such as Gaia-X signal this shift. A lack of such empathetic characteristics can breed distrust and hinder participation, even if the underlying technology is sound, as evidenced by public reactions to certain data initiatives.

2.3 Data sharing concerns

Data space participants⁹ may have various concerns when sharing data in a data space, which may delay, reduce or even make data sharing impossible. For example, data consumers may have concerns about the quality of the data they are offered, while data providers have concerns about the sovereignty of their data after exchange. Such concerns may arise from the lack of proper agreements among the data space participants as well as mechanisms to monitor their compliance.

Taking appropriate measures to deal with the stakeholder's concerns is essential for increasing trust and encouraging data sharing. These measures may involve, for example, establishing principles, standards, and agreements, along with mechanisms to monitor their compliance. According to the definitions previously presented, those measures may be implemented by the adoption of a trust framework.

To identify concerns faced by data space participants when sharing data, we performed an ad-hoc literature review. During the literature review, we identified several challenges, barriers and issues hindering data sharing, as the ones presented by (Jussen et al., 2023), (Stein et al., 2022), (Schäfer et al., 2023) and (Puspasari et al., 2021). (Jussen et al., 2023) identified barriers in inter-organizational data sharing, while (Stein et al., 2022) identified requirements and issues towards data sharing in general. (Schäfer et al., 2023) presents an overview of trust challenges and requirements for data sharing. (Puspasari et al., 2021) identified six domains of issues to be considered when sharing data, namely: security, access control, data privacy, confidentiality, integrity, and availability of data, compliance and trust and data audit capabilities.

Other works discussed challenges faced when establishing trust within data sharing scenarios. (Lim & Thing, 2024) present a trust pyramid to examine the causality factors affecting the decision to trust. The trust pyramid is divided into three categories (Foundational, Supplemental, and Innovative) based on their importance and considerations. Within each category, they identify the causality factors that act as key trust elements. (Badirova et al., 2024) discusses some of the main challenges faced while establishing a trust framework for data exchange, such as complex legal, technological, and business issues.

We summarized our findings in the following list of data sharing concerns (see **Table 2.1**). It is important to note that these are **general concerns**, i.e., concerns that may be raised by stakeholders within any data space. While this list is not comprehensive, it provides a significant overview of pertinent trust considerations within data spaces.

Table 2.1: Summary of Data Sharing Concerns

Data Sharing Concern	Description
Accountability	Ensuring that data space participants, are held responsible for their actions and data handling practices.
Compliance	Ensuring that data handling and sharing practices comply with laws, regulations, and industry standards.
Confidentiality	Ensuring the protection of personal or other sensitive information from unauthorized access.
Data quality	Ensuring that the data is of high quality, as poor data quality can lead to incorrect conclusions and decisions. Data quality refers to the condition of data based on factors such as accuracy, completeness, reliability, and relevance.
Identity, Authentication, and Authorization	Ensuring the mitigation of risks of unverified or fraudulent identities, weak authentication mechanisms that can be easily compromised,

⁹ According to the DSSC, a data space participant is a party committed to the governance framework of a particular data space and having a set of rights and obligations stemming from this framework.

	and improper management of access rights, leading to unauthorized data access or actions.
Interoperability	Ensuring the ability of different systems and organizations to work together seamlessly, ensuring that data can be shared and used effectively across various platforms.
Reliability and Availability of Infrastructure/Services	Ensuring the ability to deal with unplanned downtime, unreliable data transfer mechanisms, or data loss due to infrastructure failures.
Scalability & Performance	Ensuring that the system is capable to grow and adapt to increasing data sharing demands while maintaining its functionality and performance.
Security	Stakeholders are concerned about the protection of data from unauthorized access, breaches, and other cyber threats.
Sovereignty	Ensuring maintaining control over their data, ensuring it is stored, processed, and managed within specific geographic or jurisdictional boundaries to comply with local regulations and policies.
Transparency	Ensuring the openness and clarity with which information is shared among participants in a data space, i.e., that all parties have access to relevant information about data handling practices, policies, and procedures.

Data sharing concerns can also be domain specific. For the health domain, for example, ensuring the accuracy of health data is essential. Inaccurate data can lead to incorrect diagnoses or treatments, which can harm patients and reduce trust in the system. Similarly, for the agricultural domain, farmers need to be confident that sharing their data will lead to fair use and tangible benefits, such as improved farming practices, better market access, or enhanced sustainability.

3 Trusted data transactions: user stories

In this section, we present a scenario describing the main steps of executing a trusted data transaction in a data space and a set of user stories extracted from this scenario. The description focusses on the concerns faced by data space participants at different stages of a trusted data transaction. The user stories describe the expectations of the data space participants when joining a data transaction. These expectations reflect what the data space participants must trust in the data sharing process. From the user stories, we identified the requirements for the assessment of trust frameworks, which are presented in Appendix A.

The concept of a trusted data transaction refers to the exchange of data between parties in a manner that ensures the data's integrity, security, and privacy. Data transactions are vital for data spaces as they allow for the efficient and effective exchange of information, which is fundamental for various operations and decision-making processes.

Within any data transaction, there are a lot of moments when trust is required to facilitate the process of sharing, even beyond the transmission procedure itself. In our scenario, a data transaction is divided into three main stages: Discovery & Negotiation, Data Transfer & Use, and Post Transfer Phase. For each one of these stages, we identified two or more user stories, as described below. In general, the user stories have a focus on data space participants. In some cases, the focus is more specific either on the data consumer or on the data provider. Other specific roles, such as data space intermediaries, were not considered in this trusted data transaction scenario. To cover other roles, new scenarios and user stories can be created.

3.1 Pre-transfer phase

Participants in a data ecosystem do not just worry about the data itself. They also have bigger concerns about how well the data space works. For instance, they might question whether the system is truly robust and reliable. Beyond just being "robust," participants might worry whether the data space can consistently deliver the required performance (e.g., speed of data access, query execution times) and whether it can scale effectively to meet increasing demand without degrading service quality.

Table 3.1: Pre-Transfer Phase User Stories

Pre-transfer - User stories
US1. As a Data Space Participant, I want to be assured that the data space system is truly robust and reliable, so that I can trust its foundational stability and continuity for my data operations.
US2. As a Data Space Participant, I want to ensure the data space can consistently deliver required performance (e.g., speed of data access, query execution times) and scale effectively to meet increasing demand without degrading service quality, so that I can rely on its operational efficiency for my critical data activities and future growth.

3.2 Discovery & Negotiation

A data transaction starts when participants explore available data products and services within the data space. This might involve using a data catalogue or other discovery mechanisms. After finding the relevant data product or services, then data consumer and data provider may start the negotiation phase. During the negotiation phase, a business-level negotiation occurs between the data provider and the data consumer. An agreement is also made at the operational level, including technical aspects like data access and transfer protocols.

At this point, the data consumer may have concerns if the data of the provider will genuinely reflect the provider's promise. They may be concerned whether the data comes from truthful measurements and

authoritative sources, and whether its content will match the advertised description. The data consumer may also be concerned that the provider's data will be interoperable with that of others.

Table 3.2: Discover & Negotiation Phase User stories

Discover & Negotiation User stories
US3. As a Data Consumer, I want to verify that the data genuinely reflects the provider's promises and advertised description, originating from truthful measurements and authoritative sources, so that I can trust its content and suitability for my use.
US4. As a Data Consumer, I want to be assured that the provider's data is interoperable with data from other sources or my existing systems, so that I can seamlessly integrate and combine datasets for my applications.

3.3 Data transfer & Usage

Next, the data must travel from provider to consumer. Yet, before doing so, the provider may have concerns whether sharing this information could violate legislation covering competition law, IP rights and data rights, for example. For various reasons, it is likely they want data transactions to comply by default. This would take away these concerns and increase their willingness to share data.

Then, during transmission, many concerns may hinder the transaction. The first relates to the discretion of the content. The consumer and provider are concerned that the channel may not match the confidentiality of the content. If for instance, a broadcast is used for personal data, a large unintended audience may be able to see what they are not allowed to. On the other hand, if a perfectly secure channel is chosen, a large amount of unnecessary overhead is generated.

Besides, the medium may pose a security risk. It may be that the data arrives in an altered way or that the channel is used for unauthorized access or exploitation. The participants are concerned that a malicious third party can gain access to their information systems or that they can manipulate the transaction itself.

When the data is in the hands of the consumer, the provider may be concerned that the consumer extracts value of the data beyond their original intent. The provider has described their intent in the usage restrictions and the access controls. The provider trusts the consumer to not go beyond that.

Table 3.3: Data Transfer & Usage Phase User Stories

Data Transfer & Usage User Stories
US5. As a Data Provider, I want to be assured that data transactions automatically comply with relevant legislation (e.g., competition law, IP rights, data rights, privacy regulations), so that I can share data without fear of legal violations and increase my willingness to participate.
US6. As a Data Space Participant, I want to be assured that the data transfer channel's confidentiality matches the sensitivity of the data being transmitted, so that I can prevent unintended access by unauthorized parties without incurring unnecessary overhead.
US7. As a Data Space Participant, I want to ensure that the data transfer medium is secure against alteration, unauthorized access, or transaction manipulation, so that I can protect my information systems and the integrity of the data exchange
US8. As a Data Provider, I want to be assured that the Data Consumer uses my data strictly within the agreed-upon usage restrictions and access controls, so that I can prevent unauthorized value extraction and protect my data's intended use.

3.4 Post-transfer phase

Data space participants would like to be assured that another party can be held responsible in case the other party fails to achieve a successful transaction. Typically, for this, the parties would address this concern using the judicial system. This enables the parties to make use of a mechanism to resolve disputes and compel compliance. All participants should have openly access to relevant information about data handling practices, policies, and procedures.

Table 3.4: Post-transfer Phase User Stories

Post-transfer User Stories	
US9.	As a Data Space Participant, I want to have a clear mechanism to hold another party responsible and resolve disputes in case of a failed or non-compliant data transaction, so that I can seek redress and ensure accountability.
US10.	As a Data Space Participant, I want to have openly accessible information about other parties' data handling practices, policies, and procedures, so that I can make informed decisions and trust their operational compliance and trustworthiness.

4 Operational concerns of trust frameworks

A trust framework's core purpose is to enable secure and trustworthy data sharing within a data ecosystem. However, for it to truly achieve lasting success and widespread adoption, it must extend beyond just solving specific data-related problems. This means the framework also needs to fulfill crucial operational requirements related to its own functioning and reliability. By meeting these additional needs, the framework ensures its long-term viability. We've grouped these essential requirements into distinct operational aspects, and for each, we'll show the user stories that helped us identify them.

4.1 Adaptivity

This aspect focuses on the trust framework's ability to evolve and self-correct. Participants expect the framework to detect and fix flaws or unexpected issues, like unfair dispute resolutions, ensuring its fairness and effectiveness over time.

User stories

Table 4.1: Adaptivity User Story

Adaptivity User Story
US11. As a Data Space Participant, I want the trust framework to be able to self-correct and adapt to address unfair flaws or unforeseen issues (e.g., in dispute resolution mechanisms), so that I can rely on its long-term fairness and effectiveness.

4.2 Technological Assurance

This category highlights participants' desire for the trust framework to leverage cutting-edge technology (e.g., for data provenance or privacy enhancement). The goal is to provide verifiable guarantees that technologically prevent concerns from materializing, reducing the need for human trust.

Table 4.2: Technological Assurance User Stories

Technological Assurance User Stories
US12. As a Data Space Participant, I want the trust framework to leverage state-of-the-art technologies (e.g., for data provenance, privacy enhancement, usage enforcement), so that it technologically guarantees the mitigation of concerns and replaces human trust wherever possible.
US13. As a Data Space Participant, I want the trust framework to continuously incorporate new technical enablers and evolve its capabilities over time, so that it maximizes guaranteed trust through verifiable technologies and supports a growing number of digital transactions.

4.3 Availability & Transparency

This covers expectations that the trust framework itself is consistently accessible. It also includes the demand for clear and open operations, meaning visibility into its own internal processes, security measures, and the selection of any third-party service providers.

Table 4.3: Availability & Transparency User Stories

Availability & Transparency User Stories
US14. As a Data Space Participant, I want the hosting services and underlying infrastructure supporting the trust framework to demonstrably ensure security and prevent misuse or exfiltration of sensitive information (e.g., through independent certification or software attestation), so that I can trust the integrity and confidentiality of the transmission channel.
US15. As a Data Space Participant, I want the trust framework to ensure transparency in the selection process of any delegated operators (e.g., digital service providers for hosting and deployment), so that I can be assured of a fair and just selection and trust their operational partners.
US16. As a Data Space Participant, I want the trust framework to maintain transparency of its operational procedures, even when delegating tasks to external service providers, so that I can continually understand and trust how my data is handled.

4.4 Extraterritoriality

This aspect addresses concerns about how differing national laws might affect data stored or processed internationally. Participants expect the trust framework to provide clarity and mitigation strategies against the extraterritorial reach of legislation that could undermine data confidentiality or legal protection.

Table 4.4: Extraterritoriality User Story

Extraterritoriality User Story
US17. As a Data Space Participant, I want the trust framework to provide clear guidance and mechanisms to mitigate risks from extraterritorial legislation (e.g., CLOUD Act's reach), so that I can be confident about the confidentiality and legal protection of my data, regardless of where it is stored or processed.

4.5 Reliability (of Operator/Business)

Beyond the technical robustness, this category deals with the trustworthiness and stability of the entity operating the trust framework. Participants need confidence that the business running the framework is reliable and operates from a trustworthy jurisdiction.

Table 4.5: Reliability User Story

Reliability User Story
US18. As a Data Space Participant, I want the trust framework to be operated by a demonstrably trustworthy business entity in a trustworthy jurisdiction, so that I can have confidence in its ongoing integrity and ethical conduct, beyond its technical capabilities.

4.6 Continuity

This aspect concerns the assurance that the trust framework's operations and agreements will persist in the future. Participants want clear plans and support for smooth transitions to new operators, should the current one discontinue services, to safeguard long-term commitments.

Table 4.6: Continuity User Stories

Continuity User Stories
US19. As a Data Space Participant, I want the operator of the trust framework to demonstrate stable positioning and financial certainty, so that I can be assured that trust agreements will be executed reliably in the future and my long-term commitments are secure.
US20. As a Data Space Participant, I want the trust framework to have a clear and supported plan for a smooth transition to a new operator if the current operator discontinues service, so that I can ensure the continuity of trust agreements and data.

4.7 Sector Specific

This reflects the need for a trust framework to be tailored to the unique requirements and growth ambitions of specific communities or industries. Participants expect it to be affordable and to address specialized concerns, like the delegation of trust within a particular sector.

Table 4.7: Sector specific User Stories

Sector specific user stories
US21. As a Data Space Participant (from a specific sector), I want the trust framework to be affordable and address trust concerns specific to my sector (e.g., delegation of trust among known parties), so that it directly supports my community's unique operational and business needs.
US22. As a Data Space Participant, I want the trust framework to align with my community's growth aspirations, including openness to merging with other frameworks and supporting the inclusion of new participants, so that it fosters synergistic expansion and future opportunities within the data ecosystem.

5 A method for assessing trust frameworks

This section details the method¹⁰ for evaluating trust frameworks, which is based on a set of requirements (see Appendix A), a set of data sharing concerns and a set of driving factors influencing trust. To assist with the evaluation, we suggest a set of guiding questions (Appendix B) and, when possible, standards that should be used to implement the requirements. To illustrate how the evaluation method works, consider the relationships presented in **Figure 5.1** and the described below.

- The Trust Framework is the collection of artifacts that together promote trust through the reinforcement of the driving factors and the mitigation of concerns. When the Trust Framework fails to execute their proposal, there is a risk that trust will erode.
- Driving factors comprise the factors with a positive impact, i.e., factors that contribute to enhancing the level of trust and should, therefore, be reinforced by the trust framework.
- Conversely, factors with a negative impact are grouped as Concerns. These factors may hinder trust and therefore should be mitigated by the trust framework.

In a simple way, we could say that the process of building trust among data space participants consists of reinforcing the driving factors and mitigating concerns. The mitigation of one or more data sharing concerns contributes to an increase in one of the driving factors of trust. The intrinsic connection between driving factors and data sharing concerns drives the motivation to implement a trust framework that addresses the requirements for each data sharing concern.

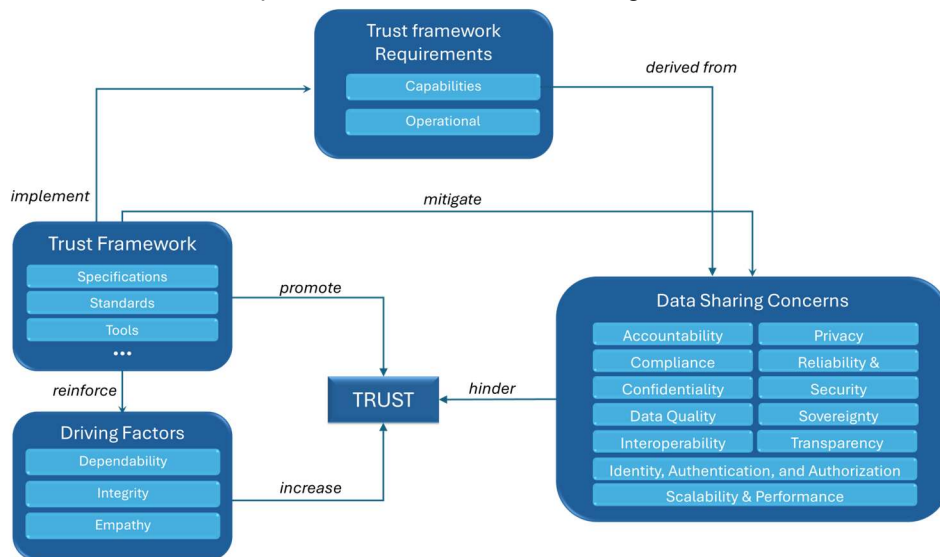


Figure 5.1: Impacting factors of trust within a data space.

The evaluation method can be used by trust framework developers for self-assessment to identify potential gaps in their solutions. It can also highlight their strengths. The results of the self-assessments can be shared with data space stakeholders to help them determine which trust framework best aligns with their objectives. During the assessment, evidence of requirements implementation should be provided through links to relevant documentation or artifacts that clearly demonstrate compliance with the corresponding requirements of the trust framework. When applicable, relevant standards or specifications should also be outlined.

Figure 5.2 illustrates the steps of the evaluation method, which are described in the following.

¹⁰ Appendix C presents the research method employed in developing the proposed assessment approach.

- › Create evaluation plan: this is the foundational step where the purpose and scope of the evaluation are defined. It is important to answer questions, such as: *What do you want to learn from the evaluation? Who needs the evaluation and who will use the results? What specific questions should the evaluation answer?* Based on the answers, the relevant requirements to evaluate the trust framework can be defined.
- › Prepare data collection instrument: at this stage, tools to gather the necessary information based on the evaluation plan must be defined. For example, surveys or interview guides can be developed.
- › Collect data: this is the implementation phase where the actual data is gathered. During this phase, surveys, interviews, focus groups, or observations will be conducted.
- › Prepare evaluation report: the final step involves analyzing the data and presenting the findings.



Figure 5.2: Steps of the evaluation method.

It is important to note that combining the requirements with the data sharing concerns and driving factors provides multiple perspectives for evaluation. In the following, we focus on evaluating the trust framework from the point of view of the driving factors: Dependability, Integrity and Empathy.

5.1 Dependability Requirements

Dependability Requirements evaluate if the trust framework builds trust ensuring the data space demonstrates robust operational resilience, comprehensive disaster recovery, clear communication, verified reliability through audits, standardized performance guarantees (SLAs), proven scalability, and transparent resource management.

Table 5.1: Dependability requirements

Dependability Reliability and Availability of Infrastructure/Services
Operational Resilience Standards
Disaster Recovery & Business Continuity Mandate
Transparency in Operational Status & Incidents
Dependability Scalability & Performance
Service Level Agreement (SLA) Framework for Performance
Scalability Verification and Disclosure
Performance Monitoring & Reporting Standards
Resource Provisioning Transparency
Dependability Reliability and Availability of Infrastructure/Services
Independent Certification/Audit for Reliability

5.2 Integrity Requirements

Integrity Requirements evaluate if the trust framework comprehensively addresses data content integrity, source trustworthiness, system interoperability, legal compliance, and robust data security throughout the data lifecycle within the data space.

Table 5.2: Integrity requirements

Integrity Compliance
Automated Compliance Rule Execution
Legal Framework Integration

Verifiable Policy Enforcement
Integrity Confidentiality
Data Classification & Sensitivity Labeling
Confidentiality Level Specification for Channels
Negotiable Security Controls
Integrity Data Quality
Data Classification & Sensitivity Labeling
Confidentiality Level Specification for Channels
Integrity Identity, Authentication, and Authorization
Credentialing & Identity Verification of Data Sources/Providers
Integrity Interoperability
Standardized Data Description & Metadata
Semantic Interoperability Standards
Technical Interoperability Protocols
Metadata for Interoperability
Integrity Security
Secure Communication Protocol Standards
Data Integrity Assurance Mechanisms
Mutual Authentication Framework
Vulnerability Disclosure & Management Policy

5.3 Empathy Requirements

Empathy Requirements evaluate if the trust framework provides robust control over data usage, clear accountability for participant actions, and transparent mechanisms for building and verifying trust among all stakeholders.

Tabel 5.3: Empathy requirements

Empathy Accountability
Defined Dispute Resolution Process
Clear Liability Framework
Comprehensive Audit Trails
Enforcement & Sanction Mechanisms
Empathy Data Sovereignty
Granular Usage Policy Expression
Verifiable Usage Control & Monitoring
Access Control Management
Post-Usage Reporting & Attestation (Optional but enhances trust)
Empathy Transparency
Standardized Disclosure of Practices
Verifiable Certifications & Badges
Transparency Registry
Reputation & Trust Scoring

5.4 Operational Requirements

The assessment method also encompasses a list of requirements concerning operational concerns about the trust framework, which are presented below.

Table 5.4: Operational Requirements

Adaptability & Technological Assurance
Adaptive Governance Mechanism
Evolution & Update Mechanism
State-of-the-Art Technology Adoption Policy
Technology-Enabled Guarantee Specifications

Continuous Technological Evolution Framework
Future-Proofing & Extensibility Design Principles
Availability & Transparency
Secure Infrastructure Requirements for Trust Framework Services
Confidentiality & Integrity Attestation for Hosting Nodes
Transparent Operator Selection Procedures
Due Diligence Standards for Third-Party Operators
Operational Transparency Standards for Delegated Services
Chain of Trust for Delegated Responsibilities
Extraterritoriality
Cross-Jurisdictional Legal Risk Assessment & Guidance
Legal Framework for Data Sovereignty
Transparency of Jurisdiction for Trust Services
Reliability & Continuity
Operator Trustworthiness Criteria
Jurisdictional Requirements for Operator
Due Diligence & Vetting of Operator
Operator Financial Stability & Transparency
Contingency Planning for Operator Instability
Operator Succession & Transition Protocol
Participant Notification & Engagement in Transition
Sector-specific
Sector-Specific Customization/Extension Mechanisms
Affordability & Cost Model Transparency
Interoperability with Other Trust Frameworks
Scalable Participant Onboarding & Management
Alignment on Growth Strategy

6 Conclusion

This report presented a systematic and adaptable method for assessing trust frameworks within data sharing environments. By grounding the evaluation in the core driving factors of Dependability, Integrity, and Empathy, and addressing the principal concerns that can hinder data sharing, the method ensures a comprehensive and stakeholder-focused assessment. The translation of these factors and concerns into user stories and concrete, traceable requirements provides both data space initiatives and trust framework developers with a clear, actionable means of identifying strengths and potential areas for improvement. The flexibility of the approach allows for adaptation to domain-specific needs, supporting the evolution of technologies and standards over time. Ultimately, this method contributes to strengthening trust among data space participants and advancing the reliable, secure, and effective sharing of data.

References

- Badirova, A., Alangot, B., Dimitrakos, T., & Yahyapour, R. (2024). Towards Robust Trust Frameworks for Data Exchange: A Multidisciplinary Inquiry. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, P-350, 15–26. https://doi.org/10.18420/OID2024_01
- Brewer, S., Pearson, S., Maull, R., Godsiff, P., Frey, J. G., Zisman, A., Parr, G., McMillan, A., Cameron, S., Blackmore, H., Manning, L., & Bidaut, L. (2021). A trust framework for digital food systems. *Nature Food*, 2(8), 543–545. <https://doi.org/10.1038/s43016-021-00346-1>
- Cho, J. H., Chan, K., & Adali, S. (2015). A Survey on Trust Modeling. *ACM Computing Surveys*, 48(2). <https://doi.org/10.1145/2815595>
- Frei, F., & Morriss, A. (2020). Begin with trust. *Harvard Business Review*, 3(June), 112–121. [https://membership.amavic.com.au/files/Begin with trust_HBR_2020.pdf](https://membership.amavic.com.au/files/Begin%20with%20trust_HBR_2020.pdf)
- Gieß, A., Hupperz, M., Schoormann, T., & Möller, F. (2024). *What Does it Take to Connect? Unveiling Characteristics of Data Space Connectors*. <https://doi.org/10.24251/HICSS.2024.511>
- Jussen, I., Schweihoff, J., & Moller, F. (2023, July 25). Tensions in Inter-Organizational Data Sharing: Findings from Literature and Practice. *Proceedings - 2023 IEEE 25th Conference on Business Informatics, CBI 2023*. <https://doi.org/10.1109/CBI58679.2023.10187530>
- Lim, J. W. Z., & Thing, V. L. L. (2024). Building Confidence in a World of Eroding Trust. *Digital Government: Research and Practice*, 5(2). <https://doi.org/10.1145/3653075>
- Roger C. Mayer, James H. Davis, and F. David Schoorman. 1995. An integrative model of organizational trust. *Academy of Management Review* 20, 709–734. <https://doi.org/10.5465/amr.1995.9508080335>
- Puspasari, D., Hadiyanto, A. N., & Setiawan, S. (2021). Inter-Organizational Data Sharing: What Issues Should Be Considered? *Proceedings - 3rd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2021*, 181–186. <https://doi.org/10.1109/ICIMCIS53775.2021.9699333>
- Schäfer, F., Rosen, J., Zimmermann, C., & Wortmann, F. (2023). Unleashing the potential of data ecosystems: Establishing digital trust through trust-enhancing technologies. In *European Conference on Information Systems (ECIS)*. https://aisel.aisnet.org/ecis2023_rp
- Stein, H., Rix, C., Effertz, A., Bergau, S., & Maass, W. (2022). *Data Sharing in the German Food Industry - Empirical Insights* (Vol. 1). <https://aisel.aisnet.org/amcis2022/DataEcoSys/DataEcoSys/1>
- Temoshok, D., & Abruzzi, C. (2018). Developing trust frameworks to support identity federations. *US Department of Commerce, National Institute of Standards and Technology*. <http://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>
- van der Peet, L., Bharosa, N., Dijkhuis, S., & Janssen, M. (2024). *Understanding Trust Frameworks: Goals and Components Identified Through a Case Study* (pp. 223–238). https://doi.org/10.1007/978-3-031-70804-6_15

Appendix A - Requirements for assessing trust frameworks

In this section, we present the requirements that are used in our proposal for assessing trust frameworks for data spaces. We have two types of requirements: capability and operational. While this list may not be exhaustive, it provides a comprehensive set of requirements that can be expanded upon further.

A.1 Capability requirements

In the following, we describe the requirements that capture the main capabilities expected from a trust framework to mitigate the data sharing concerns previously described. The first level of the requirement's number reflects the number of the user story (US) from where it was derived.

Table 0.1: Capability Requirements

US	#req	Name	Description
US1	1	Operational Resilience Standards	The trust framework must define and enforce clear standards for the data space's operational resilience, including minimum acceptable uptime, fault tolerance, and data recovery capabilities.
US1	2	Disaster Recovery & Business Continuity Mandate	The trust framework must require data space operators to implement and regularly test comprehensive disaster recovery and business continuity plans, making key aspects verifiable to participants.
US1	3	Transparency in Operational Status & Incidents	The trust framework must mandate clear and timely communication channels for data space operators to inform participants about system status, planned maintenance, and any unplanned outages or incidents that affect reliability.
US1	4	Independent Certification/Audit for Reliability	The trust framework should define or recognize processes for independent auditing or certification of the data space's operational robustness and reliability (e.g., against ISO 27001 or other relevant operational standards).
US2	1	Service Level Agreement (SLA) Framework for Performance	The trust framework must define a framework for standardizing and enforcing Service Level Agreements (SLAs) regarding key performance indicators (KPIs) such as data access speeds, query response times, and processing throughput.
US2	2	Scalability Verification and Disclosure	The trust framework must require data space operators to demonstrate and transparently disclose their system's scalability capabilities and planned capacity growth to meet increasing participant demands without compromising performance.
US2	3	Performance Monitoring & Reporting Standards	The trust framework must mandate standardized methods for monitoring system performance and require regular, verifiable reporting of actual performance against agreed-upon SLAs and expected benchmarks.
US2	4	Resource Provisioning Transparency	The trust framework should encourage transparency regarding the underlying infrastructure and resource

			provisioning strategies of the data space operator, to build confidence in its ability to sustain performance.
US3	1	Verifiable Data Provenance Standard	The trust framework must define and enforce a standard for capturing, storing, and verifiably asserting the origin, lineage (transformations), and original source of data. This includes specifying mechanisms for attestation (e.g., digital signatures, trusted timestamps).
US3	2	Data Quality Attestation & Disclosure Framework	The trust framework must establish a standardized method for Data Providers to formally attest to and disclose data quality characteristics (e.g., accuracy, completeness, timeliness) and provide evidence for these claims.
US3	3	Standardized Data Description & Metadata	The trust framework must mandate a common semantic model and technical standard for describing data products, including their advertised content, purpose, and relevant context, enabling machine-readability and verifiable consistency.
US3	4	Credentialing & Identity Verification of Data Sources/Providers	The trust framework must offer or integrate with a mechanism to verify the identity and, where relevant, the authority or trustworthiness of original data sources and data providers within the data space.
US4	1	Semantic Interoperability Standards	The trust framework must promote or enforce the use of agreed-upon semantic standards (e.g., ontologies, vocabularies) for data representation, enabling data consumers to understand and integrate data from different providers.
US4	2	Technical Interoperability Protocols	The trust framework must specify or endorse technical protocols and interfaces for data access, transfer, and integration, ensuring compatibility between different participants' systems.
US4	3	Metadata for Interoperability	The trust framework must require the inclusion of interoperability-relevant metadata (e.g., data schema, API specifications, data types, semantic mappings) in data product descriptions.
US5	1	Automated Compliance Rule Execution	The trust framework must define a mechanism for expressing legal and contractual rules in a machine-readable format that can be automatically enforced or checked during data transactions.
US5	2	Legal Framework Integration	The trust framework must provide clear mappings or references to applicable legal frameworks (e.g., GDPR, sector-specific regulations) and offer tools or guidelines for translating legal requirements into enforceable policies.
US5	3	Verifiable Policy Enforcement	The trust framework must enable participants to verify that the policies governing data sharing are being applied correctly and consistently throughout the transaction lifecycle.
US6	1	Data Classification & Sensitivity Labeling	The trust framework must establish a standard for classifying data sensitivity levels and associating these labels with data products.
US6	2	Confidentiality Level Specification for Channels	The trust framework must define standardized confidentiality levels for data transfer channels and provide guidance or mechanisms for matching channel confidentiality to data sensitivity.

US6	3	Negotiable Security Controls	The trust framework should allow for negotiation of security controls (including confidentiality) for data transfer based on data sensitivity and operational context, while adhering to minimum trust levels.
US7	1	Secure Communication Protocol Standards	The trust framework must mandate or recommend specific secure communication protocols (e.g., end-to-end encryption, TLS) for data transfer within the data space.
US7	2	Data Integrity Assurance Mechanisms	The trust framework must specify mechanisms (e.g., cryptographic hashing, digital signatures) to ensure the integrity of data during transit, allowing detection of any unauthorized alteration.
US7	3	Mutual Authentication Framework	The trust framework must provide or integrate with a strong mutual authentication framework for all participants involved in data transfer, ensuring that only verified parties can access or manipulate the data stream.
US7	4	Vulnerability Disclosure & Management Policy	The trust framework should include a policy for responsible disclosure and remediation of security vulnerabilities related to data transfer mechanisms.
US8	1	Granular Usage Policy Expression	The trust framework must define a standard for expressing granular and machine-enforceable usage policies (e.g., "for research only," "no redistribution," "only for a specified duration").
US8	2	Verifiable Usage Control & Monitoring	The trust framework must provide or integrate with mechanisms to verify that data consumers adhere to usage policies, potentially including technical controls (e.g., secure processing environments, verifiable data deletion) and auditable usage logs.
US8	3	Access Control Management	The trust framework must define and enforce clear access control mechanisms, ensuring that data is only accessible to authorized consumers under specified conditions.
US8	4	Post-Usage Reporting & Attestation (Optional but enhances trust)	The trust framework should enable Data Consumers to provide verifiable reports or attestations of their data usage in compliance with policies.
US9	1	Defined Dispute Resolution Process	The trust framework must establish a formal, transparent, and accessible dispute resolution process for addressing grievances related to data transactions or policy non-compliance.
US9	2	Clear Liability Framework	The trust framework must define the responsibilities and liabilities of each participant type for various scenarios (e.g., data quality failures, security breaches, misuse of data).
US9	3	Comprehensive Audit Trails	The trust framework must mandate the creation and secure retention of immutable, verifiable audit trails for all significant data transactions and policy adherence events.
US9	4	Enforcement & Sanction Mechanisms	The trust framework should outline potential consequences or sanctions for non-compliance with its rules and policies, and provide mechanisms for their enforcement.
US10	1	Standardized Disclosure of Practices	The trust framework must define a standard format and minimum requirements for participants to disclose their

			data handling practices, security policies, and operational procedures.
US10	2	Verifiable Certifications & Badges	The trust framework could support a system for participants to obtain and display verifiable certifications (e.g., ISO certifications, compliance badges) demonstrating adherence to specific standards or best practices.
US10	3	Transparency Registry	The trust framework should maintain or integrate with a publicly accessible registry where participants' declared practices, policies, and relevant certifications can be easily discovered and verified.
US10	4	Reputation & Trust Scoring	The trust framework could explore mechanisms for participants to provide feedback or for the system to generate reputation scores based on historical compliance and successful transactions.

A.2 Operational requirements

Besides the requirements presented in the previous section, we identified requirements concerning the quality of the service offered by the trust framework.

Table 0.2: Operational Requirements

US	#req	Name	Description
US11	1	Adaptive Governance Mechanism	The trust framework must include defined processes for adapting its rules, policies, and technical components in response to identified flaws or evolving needs.
US11	2	Evolution & Update Mechanism	The trust framework must have a formal, transparent process for its own evolution, versioning, and updating of standards and protocols.
US12	1	State-of-the-Art Technology Adoption Policy	The trust framework must include a policy for actively evaluating and adopting state-of-the-art technologies that can enhance trust guarantees.
US12	2	Technology-Enabled Guarantee Specifications	The trust framework must specify how technological guarantees are to be implemented and verified within the data space.
US13	1	Continuous Technological Evolution Framework	The trust framework must establish a formal process for continuous research, evaluation, and integration of emerging technical enablers.
US13	2	Future-Proofing & Extensibility Design Principles	The trust framework should be designed with principles of extensibility, allowing for seamless integration of new technologies.
US14	1	Secure Infrastructure Requirements for Trust Framework Services	The trust framework must specify stringent security requirements for the infrastructure hosting its core services and mandate independent security assessments.
US14	2	Confidentiality & Integrity Attestation for Hosting Nodes	The trust framework must define mechanisms to verify that hosting nodes cannot misuse or exfiltrate sensitive information.
US15	1	Transparent Operator Selection Procedures	The trust framework must establish and publish clear, transparent procedures for the selection, evaluation, and onboarding of any delegated operators.

US15	2	Due Diligence Standards for Third-Party Operators	The trust framework must define minimum due diligence standards that its own operator must apply when selecting third-party service providers.
US16	1	Operational Transparency Standards for Delegated Services	The trust framework must mandate continued operational transparency for (delegated) operators.
US16	2	Chain of Trust for Delegated Responsibilities	The trust framework should define how accountability and trust are maintained across a chain of delegated responsibilities.
US17	1	Cross-Jurisdictional Legal Risk Assessment & Guidance	The trust framework must provide clear guidance and tools for assessing and mitigating risks posed by extraterritorial laws.
US17	2	Legal Framework for Data Sovereignty	The trust framework should integrate principles and mechanisms that reinforce data sovereignty and protect against unwarranted foreign legal demands.
US17	3	Transparency of Jurisdiction for Trust Services	The trust framework must clearly disclose the jurisdiction(s) under which its own core services and delegated operations fall.
US18	1	Operator Trustworthiness Criteria	The trust framework must define criteria for assessing the trustworthiness of its operating entity, including financial stability, ethical conduct, and reputation.
US18	2	Jurisdictional Requirements for Operator	The trust framework should specify requirements or recommendations regarding the jurisdiction of its primary operator.
US18	3	Due Diligence & Vetting of Operator	The trust framework should mandate a transparent and verifiable due diligence process for assessing and continually monitoring the trustworthiness of its operator.
US19	1	Operator Financial Stability & Transparency	The trust framework should require its operator to demonstrate and periodically disclose evidence of financial stability and operational certainty.
US19	2	Contingency Planning for Operator Instability	The trust framework should define contingency plans or protocols to address potential instability of the operator.
US20	1	Operator Succession & Transition Protocol	The trust framework must define a clear and robust protocol for the succession of operators, including a transition plan and migration guidelines.
US20	2	Participant Notification & Engagement in Transition	The trust framework must mandate transparent notification and engagement processes with participants during any operator transition.
US21	1	Sector-Specific Customization/Extension Mechanisms	The trust framework should provide mechanisms for sector-specific customization or extension of its rules and policies.
US21	2	Affordability & Cost Model Transparency	The trust framework should define clear and transparent cost models and pricing structures.
US22	1	Interoperability with Other Trust Frameworks	The trust framework should define standards and protocols to facilitate interoperability and potential merging with other trust frameworks.
US22	2	Scalable Participant Onboarding & Management	The trust framework must provide robust and scalable mechanisms for onboarding, identity

			management, and governance of a growing number of participants.
US22	3	Alignment on Growth Strategy	The trust framework should demonstrate a clear strategy for growth and evolution that aligns with the broader aspirations of the data ecosystem community.

Appendix B – Guiding questions for the requirements evaluation

In this section, we present the requirements classified by the corresponding driving factor and data sharing concern. For each one of them, we present one or more questions that could be used to assist the requirements evaluation. When possible, we also present a standard that could be used for the requirement's implementation.

Table 0.1: Dependability Requirements (1)

Dependability Reliability and Availability of Infrastructure/Services	
Operational Resilience Standards	Are explicit standards documented for minimum uptime (e.g., 99.9%), fault tolerance, and data recovery capabilities (RTOs/RPOs) for all critical services?
Disaster Recovery & Business Continuity Mandate	Does the framework mandate that data space operators implement and regularly test comprehensive Disaster Recovery (DR) and Business Continuity Plans (BCP)?
	Possible Standards: ISO 22301 (Business Continuity Management Systems)
	Are key aspects of DR/BCP (e.g., test results, RTO/RPO adherence) verifiable by participants or through audits?
Transparency in Operational Status & Incidents	Are automated, verifiable, and secure (e.g., off-site, immutable) backup procedures mandated for all critical data and configurations?
	Does the framework mandate clear and timely communication channels (e.g., status page, email alerts, APIs) for operational information?
	Are standards in place for informing participants about system status, planned maintenance (with advance notice), and unplanned outages/incidents?
	Are specific timeliness requirements defined for initial notifications and subsequent updates during incidents?
	Are operators required to have and follow clear communication playbooks for various incident types and severity levels?

Table 0.2: Dependability Requirements (2)

Dependability Scalability & Performance	
Service Level Agreement (SLA) Framework for Performance	Does the framework define a clear framework for standardizing and enforcing Service Level Agreements (SLAs) for key performance indicators (KPIs)?
	Are specific KPIs (e.g., data access speeds, query response times, processing throughput) defined within the SLA framework?
Scalability Verification and Disclosure	Does the framework require operators to demonstrate and transparently disclose their system's scalability capabilities and planned capacity growth?
Performance Monitoring &	Does the framework mandate standardized methods for continuous monitoring of system performance against SLAs and benchmarks?

Reporting Standards	Does the framework mandate periodic (e.g., annual) independent audits of key operational resilience and performance aspects for data space operators?
	Does the framework require regular, verifiable reporting of actual performance against agreed-upon SLAs and expected benchmarks?
	Possible standards: W3C Verifiable Credentials
Resource Provisioning Transparency	Does the framework encourage or mandate transparency regarding the underlying infrastructure and resource provisioning strategies of the data space operator?

Table 0.3: Dependability Requirements (3)

Dependability Reliability and Availability of Infrastructure/Services	
Independent Certification/Audit for Reliability	Does the framework define or recognize processes for independent auditing or certification of the data space's operational robustness and reliability?
	Are operators required to make relevant audit findings or certifications verifiable or accessible to participants (e.g., via published reports or attestations)?

Table 0.4: Integrity Requirements (1)

Integrity Compliance	
Automated Compliance Rule Execution	Does the framework define a mechanism for expressing legal and contractual rules in a machine-readable format for automatic enforcement or checking? Possible standards: ODRL (Open Digital Rights Language)
Legal Framework Integration	Does the framework provide clear mappings/references to applicable legal frameworks (e.g., GDPR) and offer tools/guidelines for translating legal requirements into policies?
Verifiable Policy Enforcement	Does the framework enable participants to verify that policies governing data sharing are applied correctly and consistently throughout transactions?

Table 0.5: Integrity Requirements (2)

Integrity Confidentiality	
Data Classification & Sensitivity Labeling	Does the framework establish a standard for classifying data sensitivity levels and associating these labels with data products?
Confidentiality Level Specification for Channels	Does the framework define standardized confidentiality levels for data transfer channels and guide matching channel confidentiality to data sensitivity?
Negotiable Security Controls	Does the framework allow for negotiation of security controls (including confidentiality) based on data sensitivity, while adhering to minimum trust levels?

Table 0.6: Integrity Requirements (3)

Integrity Data Quality	
Verifiable Data Provenance Standard	Does the framework define a standard for capturing, storing, and verifiably asserting data origin, lineage, and source (e.g., via digital signatures, timestamps)? Possible standards: W3C Verifiable Credentials, W3C PROV-O, W3C PROV-DM

Data Quality Attestation & Disclosure Framework	Does the framework establish a standardized method for data providers to formally attest to and disclose data quality characteristics (e.g., accuracy, completeness, timeliness) with supporting evidence? Possible standards: DAMA-DMBOK principles, W3C Verifiable Credentials
---	---

Table 0.7: Integrity Requirements (4)

Integrity Identity, Authentication, and Authorization	
Credentialing & Identity Verification of Data Sources/Providers	Does the framework offer or integrate with mechanisms to verify the identity and, where relevant, the authority or trustworthiness of original data sources and data providers? Possible standards: eIDAS (Electronic Identification, Authentication and Trust Services for EU)

Table 0.8: Integrity Requirements (5)

Integrity Interoperability	
Standardized Data Description & Metadata	Does the framework mandate a common semantic model and technical standard for describing data products, including content, purpose, and context, enabling machine-readability? Possible standards: W3C DCAT (Data Catalog Vocabulary)
Semantic Interoperability Standards	Does the framework promote or enforce agreed-upon semantic standards (e.g., ontologies, vocabularies) for data representation to ensure common understanding?
Technical Interoperability Protocols	Does the framework specify or endorse technical protocols and interfaces for data access, transfer, and integration, ensuring system compatibility?
Metadata for Interoperability	Does the framework require inclusion of interoperability-relevant metadata in data product descriptions?

Table 0.9: Integrity Requirements (5)

Integrity Security	
Secure Communication Protocol Standards	Does the framework mandate or recommend specific secure communication protocols (e.g., end-to-end encryption, TLS) for data transfer?
Data Integrity Assurance Mechanisms	Does the framework specify mechanisms (e.g., cryptographic hashing, digital signatures) to ensure data integrity during transit and detect alterations?
Mutual Authentication Framework	Does the framework provide or integrate with a strong mutual authentication framework for all participants in data transfer?
Vulnerability Disclosure & Management Policy	Does the framework include a clear policy for responsible disclosure and remediation of security vulnerabilities related to data transfer mechanisms?

Table 0.10: Empathy Requirements (1)

Empathy Accountability	
Defined Dispute Resolution Process	Is a formal, transparent, and accessible dispute resolution process established for addressing grievances related to data transactions or policy non-compliance?

Clear Liability Framework	Does the framework explicitly define the responsibilities and liabilities of each participant type for various scenarios (e.g., data quality, security breaches, misuse)?
Comprehensive Audit Trails	Does the framework mandate the creation and secure retention of immutable, verifiable audit trails for all significant data transactions and policy adherence events?
Enforcement & Sanction Mechanisms	Does the framework outline potential consequences or sanctions for non-compliance with its rules and policies, and provide mechanisms for their enforcement?

Table 0.11: Empathy Requirements (2)

Empathy Data Sovereignty	
Granular Usage Policy Expression	Does the framework define a standard for expressing granular, machine-enforceable usage policies (e.g., "research only," "no redistribution," "duration limits")? Possible standard: W3C ODRL (Open Digital Rights Language)
Verifiable Usage Control & Monitoring	Does the framework provide/integrate mechanisms to technically verify data consumers' adherence to usage policies (e.g., secure processing environments, verifiable deletion)? Possible standards: W3C Verifiable Credentials
Access Control Management	Does the framework define and enforce clear access control mechanisms, ensuring data is only accessible to authorized consumers under specified conditions? Possible standards: W3C Verifiable Credentials
Post-Usage Reporting & Attestation (Optional but enhances trust)	Does the framework enable data consumers to provide verifiable reports or attestations of their data usage in compliance with policies? Possible standards: W3C Verifiable Credentials
	Does the framework mandate auditable logs for all data usage, allowing verification against defined policies?

Table 0.12: Empathy Requirements (3)

Empathy Transparency	
Standardized Disclosure of Practices	Does the framework define a standard format and minimum requirements for participants to disclose their data handling practices, security policies, and operational procedures?
Verifiable Certifications & Badges	Does the framework support a system for participants to obtain and display verifiable certifications or compliance badges? Possible standards: W3C Verifiable Credentials
Transparency Registry	Does the framework maintain or integrate with a publicly accessible registry where participants' declared practices, policies, and relevant certifications can be easily discovered and verified?
Reputation & Trust Scoring	Does the framework explore mechanisms for participants to provide feedback or for the system to generate reputation scores based on historical compliance and successful transactions?

Table 0.13: Operational Requirements (1)

Adaptability & Evolution	
Adaptive Governance Mechanism	Does the trust framework include defined processes for adapting its rules, policies, and technical components in response to identified flaws or evolving needs?

Evolution & Update Mechanism	Does the trust framework have a formal, transparent process for its own evolution, including versioning and updating of standards and protocols?
State-of-the-Art Technology Adoption Policy	Does the trust framework include a policy for actively evaluating and adopting state-of-the-art technologies that can enhance trust guarantees?
Technology-Enabled Guarantee Specifications	Does the trust framework specify how technological guarantees are to be implemented and verified within the data space?
Continuous Technological Evolution Framework	Has the trust framework established a formal process for continuous research, evaluation, and integration of emerging technical enablers?
Future-Proofing & Extensibility Design Principles	Is the trust framework designed with principles of extensibility, allowing for seamless integration of new technologies?

Tabel 0.14: Operational Requirements (2)

Security & Operational Integrity	
Secure Infrastructure Requirements for Trust Framework Services	Does the trust framework specify stringent security requirements for the infrastructure hosting its core services, and does it mandate independent security assessments?
Confidentiality & Integrity Attestation for Hosting Nodes	Does the trust framework define mechanisms to verify that hosting nodes cannot misuse or exfiltrate sensitive information?

Table 0.15: Operational Requirements (3)

Operator management & Accountability	
Transparent Operator Selection Procedures	Does the trust framework establish and publish clear, transparent procedures for the selection, evaluation, and onboarding of any delegated operators?
Due Diligence Standards for Third-Party Operators	Does the trust framework define minimum due diligence standards that its own operator must apply when selecting third-party service providers?
Operational Transparency Standards for Delegated Services	Does the trust framework mandate continued operational transparency for (delegated) operators?
Chain of Trust for Delegated Responsibilities	Does the trust framework define how accountability and trust are maintained across a chain of delegated responsibilities?

Table 0.16: Operational Requirements (4)

Jurisdiction & Legal Compliance	
Cross-Jurisdictional Legal Risk Assessment & Guidance	Does the trust framework provide clear guidance and tools for assessing and mitigating risks posed by extraterritorial laws?
Legal Framework for Data Sovereignty	Does the trust framework integrate principles and mechanisms that reinforce data sovereignty and protect against unwarranted foreign legal demands?
Transparency of Jurisdiction for Trust Services	Does the trust framework clearly disclose the jurisdiction(s) under which its own core services and delegated operations fall?

Table 0.17: Operational Requirements (5)

Operator Trustworthiness & Stability	
Operator Trustworthiness Criteria	Does the trust framework define criteria for assessing the trustworthiness of its operating entity, including financial stability, ethical conduct, and reputation?
Jurisdictional Requirements for Operator	Does the trust framework specify requirements or recommendations regarding the jurisdiction of its primary operator?
Due Diligence & Vetting of Operator	Does the trust framework mandate a transparent and verifiable due diligence process for assessing and continually monitoring the trustworthiness of its operator?
Operator Financial Stability & Transparency	Does the trust framework require its operator to demonstrate and periodically disclose evidence of financial stability and operational certainty?
Contingency Planning for Operator Instability	Does the trust framework define contingency plans or protocols to address potential instability of the operator?
Operator Succession & Transition Protocol	Does the trust framework define a clear and robust protocol for the succession of operators, including a transition plan and migration guidelines?
Participant Notification & Engagement in Transition	Does the trust framework mandate transparent notification and engagement processes with participants during any operator transition?

Table 0.18: Operational Requirements (6)

Flexibility, Interoperability & Growth	
Sector-Specific Customization/Extension Mechanisms	Does the trust framework provide mechanisms for sector-specific customization or extension of its rules and policies?
Affordability & Cost Model Transparency	Does the trust framework define clear and transparent cost models and pricing structures?
Interoperability with Other Trust Frameworks	Does the trust framework define standards and protocols to facilitate interoperability and potential merging with other trust frameworks?
Scalable Participant Onboarding & Management	Does the trust framework provide robust and scalable mechanisms for onboarding, identity management, and governance of a growing number of participants?
Alignment on Growth Strategy	Does the trust framework demonstrate a clear strategy for growth and evolution that aligns with the broader aspirations of the data ecosystem community?

Appendix C – Research Method

This study adopted a pragmatic philosophy, focusing on solving problems with practical solutions rather than seeking absolute truth, and employs various research strategies as needed. **Figure 0.1** illustrates the steps taken during the research. The first phase, Knowledge Acquisition, can be categorized as exploratory and aimed at building a theoretical foundation about trust within a data space. This involved conducting an ad-hoc literature review to overview the research problem. This informal evaluation gathered the main concepts using subjective methods, which were essential for establishing the theoretical background for further research. Our ad hoc literature review was meant to identify hindering factors of trust within data spaces. After identifying barriers, challenges and issues related to data sharing, then we summarized them as a list of data sharing concerns. During this phase, we collected few use cases that helped with the identification of operational aspects of trust frameworks.

The second phase, Conceptualization and Formalization, involved creating artifacts to support the specification of the assessment method for trust frameworks, followed by the specification of the proposed method itself. During this phase, we developed the Trust Triangle for Data Sharing. We also created a set of user stories to help with the extraction of the trust frameworks requirements. Next, we developed the Method for Assessing Trust Frameworks. The third phase, Evaluation, focused on assessing the proposed method.

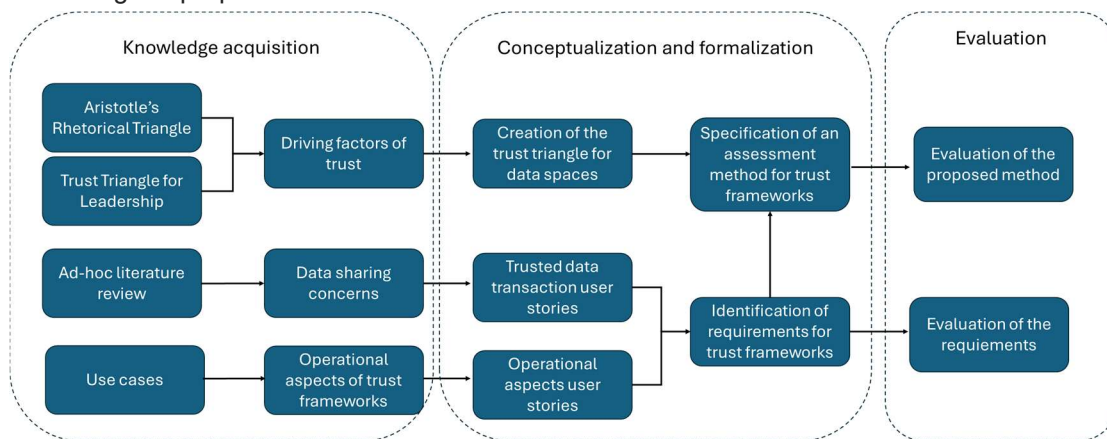
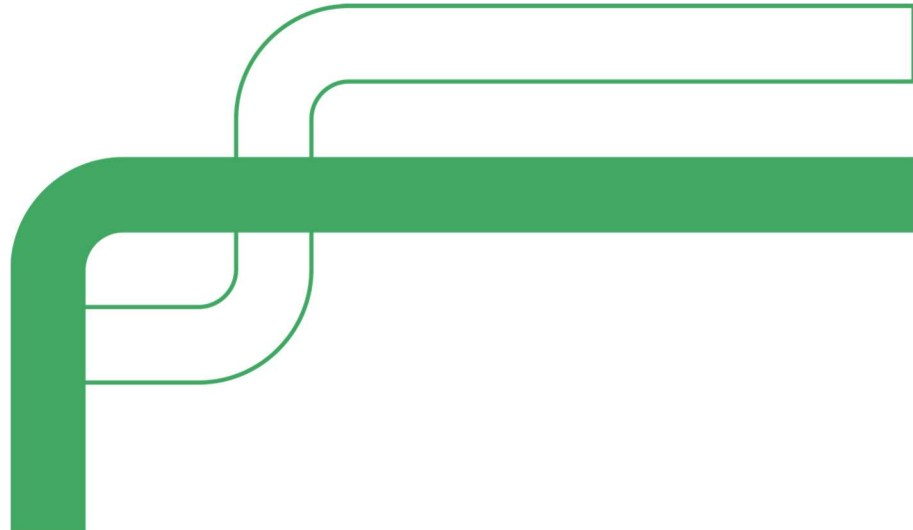


Figure 0.1: Research method steps

To guide us during the development of the assessment method, we defined some principles. This helped us to have a clear and structured foundation for the development process. The guiding principles involve ensuring that the proposed assessment method is comprehensive, targeted, and effective.

- A **comprehensive** assessment method covers, as much as possible, all relevant aspects and factors necessary for a thorough evaluation, providing a complete picture of the trust framework being assessed.
- It is **targeted**, meaning it is specifically designed to address the key areas that are most impactful or critical, focusing on the most important factors that drive outcomes.
- An **effective** assessment method achieves its intended purpose by providing accurate, reliable, and actionable insights, helping in making informed decisions, improving processes, and achieving desired outcomes.

A thorough assessment method ensures that the evaluation covers relevant areas and produces results that can inform future actions.



Colofon

This report paper is a result of the work of the Dutch Centre of Excellence for Data Sharing and Cloud (CoE-DSC, www.coe-dsc.nl), specifically its work on trust frameworks to support data space interoperability.

Trust frameworks are key for the emerging data economy, They are a key success factor for broad adoption of the data space architectures and concepts underlying the EU Data Strategy and its ambition of the Common European Data Spaces.

The goal of this report is to provide a comprehensive evaluation framework of data spaces, grounded in a methodology based on an extensive exploration of data sharing concerns, user stories, operational aspects and assessment requirements.

Authors

- Dr. B. (Bernadette) Farias Lóscio (TNO)
- P. (Pim) Mulder, MSc (TNO)

Contact

The Centre of Excellence for Data Sharing and Cloud (CoE-DSC)

E-mail — info@coe-dsc.nl

Website — www.coe-dsc.nl