

Data sharing economy

Exploring the risk
and assurance
implications

March 2026





Foreword

Sharing is a stalwart strategy to increase access to underused assets. We are all familiar with timesharing or book libraries. The world we live in today sees a new kid on the block: data sharing, fully enabled by digital platforms and high performance computing. The report in front of you discusses the rapid growth of the data sharing economy and its impact on people and society. Hardly any sector is now left untouched by some form of data sharing.

Why is it important to examine and consider the impact of data sharing? This is because data and the possibilities of its wide use are transforming organizations in how they interact, operate, and collaborate to create value. Perhaps even more importantly: data is impacting on the boundaries of these very organizations, as data flows are both simultaneous and continuous, within and outside, due to the power of technology and the interconnectedness of economies.

That poses challenges and opportunities for organizations and therefore requires the attention of

leadership. Leaders must not only understand the strategic potential of data sharing but also champion the cultural and operational shifts required to harness it responsibly. Data governance, risk mitigation and anticipation of new risks and new disruptive events from digital operations are all part of this responsibility.

This report is the result of thoughtful research and collaboration across disciplines. It provides a foundation for dialogue, decision-making, and action. Its findings will provoke reflection and allow you to engage knowledgeably in the dialogue about how your organization can lead with confidence in the data sharing economy.



Stephanie Hottenhuis

CEO and Chair of the Board of
Management of KPMG Netherlands

Preface

The data sharing economy has evolved into a system where businesses treat data as a tradable and shareable product, rather than a valuable secret they keep for themselves. As a product, businesses offer insights about their data, such as predictions and analytics. While it presents a common opportunity for providers to generate new sources of income, for consumers, it creates a different opportunity. Provided data enable the improvement of services, for instance, by making them personalized. Digital business models also allow businesses to function without the need to invest in physical assets such as buildings and machinery. An example is Airbnb, which generates income by enabling homeowners to rent out their homes on the Airbnb platform and charging a commission fee. While this global online marketplace does not own nor rent out homes itself, it receives data from homeowners and uses these data to recommend owners' homes to renters in search of available homes. Airbnb thus uses the data received for a variety of purposes through which a match between supply and demand is facilitated, including presenting the location, size, availability, price, and configuration of offered homes.

There are, however, various risks surrounding the data sharing economy. Some examples are risks of price discrimination, privacy violation, vulnerability to security flaws, and data inaccuracy. Price discrimination entails that data are used by businesses to unfairly raise prices for specific clients. For instance, a transportation company may deliberately offer more expensive bus tickets to dependent people who frequently need to take the bus. Offered data can also violate people's privacy. For instance, the data used to raise bus tickets prices could have been provided by a travel planning app that shares users' travel activities, even though users never gave the app permission to do so. Any security flaw may also result in high-impact consequences. If confidential data such as medical data and identification numbers leak, this could enable hackers to extort victims or commit crimes using victims' names. Some other cybersecurity risks include man-in-the-middle attacks, where hackers modify data while it is shared, and supply chain attacks, where one software supplier under attack opens the door for attackers to attack every business that relies on its solution. Furthermore, data might not always be accurate, with potentially resulting in unwise investments spurring a decline in service quality and revenue.

Not surprisingly, the data sharing economy has changed the nature of audits as well. Some of these changes involve growing attention for continuous

assurance, a change in auditors' role, adjustment to the altered risk landscape, and greater focus on data sovereignty. Since data are shared frequently between businesses, it may no longer be desirable to conduct audits every once in a while. Auditing is changing into a continuous process that monitors data in real time. This enables audits to better detect risks as they are happening, instead of after their occurrence. As a consequence, auditors may also be expected to take more of an advisory role rather than only a reporting one, enhancing the ability of businesses to proactively act on risks that possibly remained undetected in the past.

Considering the aforementioned risk of supply chain attacks, auditors may also need to expand the scope of audits to assess not only the way in which data are handled by their own clients, but also by connected third parties. The result of appropriate improvements would be that cybercriminals find less opportunity to identify a weak spot in the supply chain. Audits must also ensure that data remain sovereign as they may be shared internationally, while such exchange needs to comply with local and international laws. To put this aspect into perspective, privacy laws differ across countries and jurisdictions, with the implication that while gathering and using sensitive data in one country may be legal, it can be illegal to use these same data in another country.



These brief thoughts and examples represent merely a few of the major impacts of the data sharing economy that are challenging and changing the nature of audits. As the data sharing economy evolves, auditing needs to evolve alongside.

The content of this publication reflects a mixture of theoretical insights and knowledge based on professional experience that jointly shed light on the concept and consequences of the data sharing economy. Given its wide scope and variation in related topics, the content should be of interest to a wide range of readers. Professionals to whom the content of this publication will undoubtedly be of interest are mostly those who advocate data-driven businesses, and are responsible for digital, risk, audit, or other chief functions. The target audience includes though is not limited to:

- Chief executive officers who wish to find out more about the economic value of data. This publication could help gaining insights, directions, and examples that are helpful to explore new opportunities.
- Chief data (or digital) officers who are usually the sponsor of digital and data-driven strategies and bear responsibility for them. This publication could support leveraging the opportunities provided by the combination of data and digital technologies, and gain a better understanding of what could go wrong and how to deal with it.
- Chief risk officers who maintain a focus on balancing risk and reward. This publication provides several perspectives and describes their value and complications in the context of the data sharing economy.
- Chief audit executives who are tasked with finding new ways to fulfil their firm's primary audit and assurance tasks. This publication feeds professional and conceptual knowledge, and offers a modern view of how the auditor's role needs to evolve in the data sharing economy.

Overall, this publication highlights some of the vivid opportunities that come along with the evolving data sharing economy. At the same time, it underscores the importance of proper mitigation of related risks and how modern assurance mechanisms enable to provide greater confidence in managing the risks that accompany the opportunities of the data sharing economy.

Prof. dr. H.C. (Henri) Dekker

Head of the Department of Accounting
School of Business and Economics
[Vrije Universiteit Amsterdam](#)

Table of contents

Foreword	2	04 Assurance	42
Preface	3	04.1 Revamping	43
01 Introduction	6	04.2 Sharing	45
01.1 Datafication of the world	7	04.3 Trends	48
01.2 Sharing, why not?	9	04.4 Implications	49
01.3 Data sharing: A business necessity	10	04.5 Concluding principles	51
01.4 Research	12	05 Discussion	52
01.5 Organization	13	05.1 Conclusion	52
01.6 Concluding principles	14	05.2 Follow up	53
02 Data sharing economy	15	05.3 Acknowledgements	53
02.1 Driving forces	15	05.4 Closing words	53
02.2 Delineation and the definition of the data sharing economy	18	06 Board and expert opinion	54
02.3 Digital platforms	20	References	
02.4 Data focus areas	22	Appendix A. Research methodology	
02.5 Enabler technologies	24	Appendix B. List of acronyms	
02.6 Trust	26	Appendix C. Glossary	
02.7 Concluding principles	28	Appendix D. Data sharing solutions	
03 Risk	30	Appendix E. Overview of figures and tables	
03.1 Disruption	30	Appendix F. About the authors	
03.2 Sharing	31	Contact	
03.3 Compounding risks	36		
03.4 Implications	38		
03.5 Concluding principles	41		

01 Introduction

In recent years, the data sharing economy¹ has expanded at a remarkable pace and now touches almost every sector. Still, it is important to distinguish between basic digital transactions and genuine sharing. True data sharing means coordinated access to resources that would otherwise sit idle, supported by platforms that connect people or businesses directly and help manage the exchange from start to finish. This type of sharing includes activities such as matching users with providers online and handling the full order process in a digital environment. While the concept itself is far from new – bartering systems and community-based resource pooling have existed for centuries – the way sharing happens today is shaped by technology. Digital platforms have become the main enablers, shifting the focus from traditional, informal practices to structured, data-driven interactions that can scale quickly and reliably (Sutherland & Jarrahi, 2018).

Today's digital economy is built on advanced computing, large-scale data storage, high-speed communication protocols, and continuous technological innovation. Promising possibilities have been brought into play by revolutionary High-Performance Computing (HPC), the explosive growth of data in volumes, diversity, and pertinence, and the ever-evolving real-time data exchange facilities. Alongside novel tech-based applications, they have been widely noticed as an instrument to markedly reap higher economic impact that includes, among others, increasing the productivity of business fields and competition in the world of work, necessitating workers to always add skills and knowledge (Harahap & Nabillah, 2023). This recognition has encouraged data-savvy business executives to accelerate even more the leverage of their technology-driven data strategies and create business models that never existed before.

In this context, it is essential to recognize data not merely as a raw resource, but as strategic capital. The ability of organizations to transform data into actionable insights increasingly defines their competitive edge. This shift demands a holistic approach that integrates data governance, artificial intelligence (AI) capabilities, and ethical safeguards. Besides this strategic choice, it has become clear that strong leadership is central, and a solid data-centric culture is a must-have, which simply requires their focus to be artfully oriented towards strengthening their commitment in automating data usage to the largest possible extent.

The shift toward data-driven operations is supported by stronger data literacy, growing confidence in data, and reliable access to it across the organization. As companies mature in their use of data, it becomes clear that identifying, governing, and continuously maintaining the right data is critical to realizing its full potential and achieving meaningful economic impact. Along the way, several lessons stand out. One is that effective use of data can help address complex problems, improve how organizations engage with customers, and create new economies of scale.

Today's digital environment produces large, high-dimensional, and increasingly complex datasets. These volumes continue to rise and vary widely in form. This has given rise to what many describe as the "data paradox": organizations gather more data than they can realistically process, yet still feel they do not have enough to support their ambitions (Dell, 2020). Much of this pressure stems from the desire to outperform competitors by collecting, storing, processing, analyzing, and applying data as broadly as possible. The underlying principle is simple: gather data wherever you can so critical insights are not missed and potential value is not lost. This mindset often leads organizations to explore every possible source and leave no opportunity untouched in their push to advance (Sedkaoui & Khelfaoui, 2020; Favaretto et al., 2020; Gartner, 2024a).

¹ The global sharing economy market size was valued at USD 150.8 billion in 2022. The sharing economy market industry is projected to grow from USD 201.32 billion in 2023 to USD 2031.1 billion by 2032, exhibiting a Compound Annual Growth Rate (CAGR) of 33.50% during the forecast period, i.e., 2023 - 2032 (MRF, 2024).

01.1 Datafication of the world

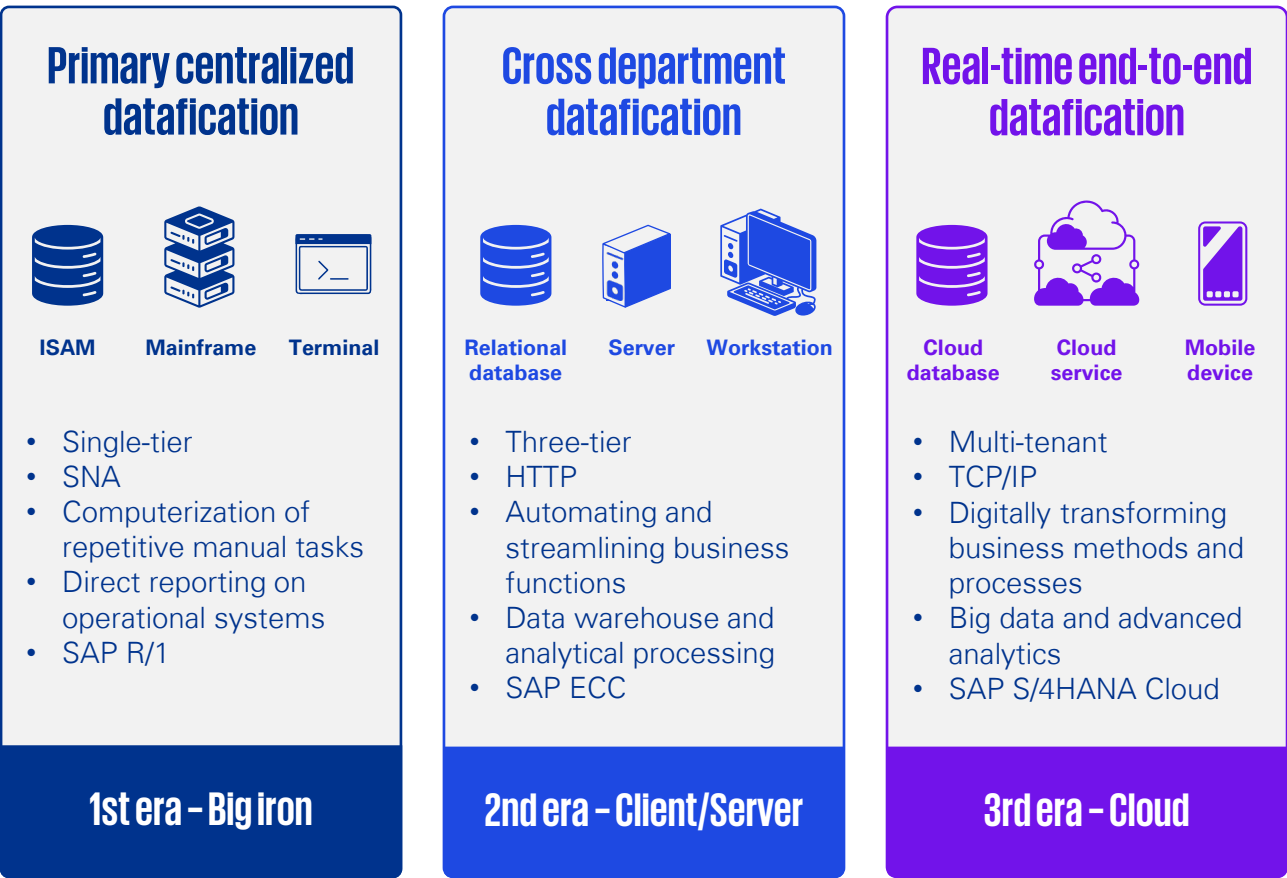
Converting symbolic material into digital form to make it indexable and searchable – as well as transforming various aspects of business into quantifiable data – has been underway for quite some time. The goal is to turn previously unmeasurable or invisible processes, behaviors, and experiences (e.g., customer sentiment and shopping behavior) into data that can be tracked, analyzed, improved, and acted upon. Over time, nearly every business domain has become subject to forms of analysis that can often be substantially automated (Mayer-Schönberger & Cukier, 2013; Mejias & Couldry, 2019).

The increasing role of digital platforms in large-scale data analysis has made datafication a key driver of economic transformation. For instance, tools like Facebook Ads allow businesses to gather data on

target markets and adapt strategies accordingly. Datafication refers to turning various phenomena into data, often relying on technological and big data solutions to uncover valuable insights within large volumes of structured and unstructured data (Mejias & Couldry, 2019; Koenen et al., 2021; Smith, 2024).

Supporting technologies – such as software, infrastructure, and smart devices – have evolved significantly, enabling data from sources like online transactions, social media, sensors, and mobile inputs to move from on-premise storage to cloud-based environments (Domingos, 2024). To illustrate this gradual shift, datafication can be viewed through three main architectural eras, which are outlined in figure 1. Each of these eras has distinct characteristics and components, briefly described below.

Figure 1. Datafication technology evolution



01.1.1 Primary centralized datafication: Big iron era

The first architectural era referred to as the big iron era is symbolized by the iconic mainframe machines dominating the business scene in the early days of commercial computation. Remote communication therewith was possible through a text terminal enabled by the Systems Network Architecture (SNA) data communication architecture. Placed in privately-owned on-premise data centers, those hulking batch-oriented legacy systems were used to centrally computerize repetitive manual tasks and electronically process data using file management systems like Indexed Sequential Access Method (ISAM). The so-called direct reporting was a commonly used concept which was implemented by dedicated reporting tools running directly on operational systems (Inmon, 1986; Inmon, 1996; Shahim, 2005). Back in the day, mainframe computers were mounted in huge and room-sized metal boxes, were designed around a single-tier architecture, were built to support economies of scale (i.e., in particular cost per workload), were positioned as the workhorse of corporate computing, and were shared by many concurrent users doing labor-intensive work (Azadmanesh & Peak, 1995; Thomas, 2014). An example of an information system (e.g., Enterprise Resource Planning (ERP)) that ran on gigantic, age-old legend mainframes was SAP R/1, which was originally launched as standard financial software capable of real-time data processing (Greenstein & Wade, 1998; Reinsel et al., 2017; Shahim, 2017).

01.1.2 Cross department datafication: Client/server era

The second architectural era known as the client/server era is characterized by a system with a two-layer or three-layer design. In the former style, a central server (i.e., a midrange computer supporting multiple users at once) provided data or other services via a computer network to multiple workstations (e.g., a Personal Computer (PC)) that together acted as clients. Located in internal data centers or in those operated by external Information and Communication Technology (ICT) service providers, the architectural model was then identified as an economical solution for large environments. It physically separates the presentation and application layers from the function that looks after processing the data normally held in relational databases (Schussel, 2001; Ardagna et al., 2004). At the time, they were also used to serve as a data warehouse in which structured operational data was saved and administered apart from transactional systems. Without directly affecting their performance,

this repository was the single point of truth to run analytical processing for Business Intelligence (BI) purposes (Shahim, 2005). SAP ERP Central Component (ECC) running on a web-based application server can be mentioned as an information system based on a three-tier client/server structure (i.e., presentation layer, application layer, and database layer) that was released as a customizable software organized in several functionals. It allows us to select specific modules like Customer Relationship Management (CRM), Human Resource Management (HRM), and Supply Chain Management (SCM), and to automatically centralize and streamline these core business functions. Using Hyper Text Transfer Protocol (HTTP), data is processed and made accessible across departments in real-time (Gupta, 2024).

01.1.3 Real-time end-to-end datafication: Cloud era

The third architectural era entitled as the cloud computing (hereinafter referred to as 'cloud') era is featured by a combination of various physical and virtual technology components. Together, they make it possible to quickly pool, share and scale resources (e.g., servers, storage, and virtualization) across a network applying the Transmission Control Protocol/Internet Protocol (TCP/IP) model. Cloud offered in four deployment models (i.e., public, private, community, and hybrid) is considered one of the most transformative economic innovations of the 21st century. Among plenty of other amenities, it especially eases the entrance of new digital-minded players into the marketplace as a consequence of which the competitiveness of businesses is increased (Haucap et al., 2022). Usually accessible by any device (e.g., a mobile phone or another remote facility), public cloud is for instance a multitenant architecture setup by freely approachable Cloud Service Providers (CSPs) that operate large-scale data centers to dynamically assign and reassign cloud resources and service models (i.e., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)) over the internet in accordance with fluctuating demand. Cloud is seen as the flexible foundation of digital transformation by means of which almost every business is rapidly turning into a data-driven business built upon technology which in turn generates vast quantities of data. Hence, big data is logically a key part of this revolutionary change which grounds decision-making in sophisticated analytics (Zen, 2024; Charter, 2024). For this goal, data is uploaded to cloud via an internet connection where it is often spread by CSPs on multiple virtual machines on a physical server.

In their huge data centers located around the world, modern cloud databases organizing and storing structured, unstructured, and semi-structured data with the added flexibility of cloud (e.g., agility and scalability) are also put in operation to launch, run, and scale feature-rich, high-performance file storage systems in the cloud (Bhatti & Bashari Rad, 2017). SAP S/4HANA Cloud is a SaaS edition of SAP HANA with built-in technologies (e.g., advanced analytics applying

AI, visualization and other technologies to uncover data insight beyond traditional BI) that is deployed as a set of integrated applications (e.g., Manufacturing, Sales and Distribution) to transform business methods and processes. This ERP solution offers a unified suite for managing end-to-end processes by providing real-time insights into the business data (Pritzker & Gallagher, 2013; Murphy & Curran, 2023; Gupta, 2024).

01.2 Sharing, why not?

The concept of sharing is not a new phenomenon to humanity. From the very start, humans described the world around them to one another, told stories to explain their experience, and expressed feelings to show their emotions. They shared products with family, friends, and neighbors, and participated in social groups to enjoy social interactions which have always formed a part of human nature. Similarly, neither is the act of sharing new to business communities nor is it pervasive (Sabitzer et al., 2018). In fact, sharing privately-owned assets has also been an inherent part of the nature of entrepreneurship. After all, it is simply all about creating value where it is not recognized or expected. A classic business model is to make use of overcapacity (e.g., business equipment and furniture) that is available in organizations and offer it to others. It is aimed to generate more revenue and to lower operation costs as the demand to procure or the need to invest in new capacity is eliminated (Moratis, 2017). Nowadays, the new element is advanced ICT solutions with an impressive impact on the economy, especially on the way in which goods and services are consumed without the necessity to transfer ownership and the way to exchange services (Basselier et al., 2018). Early real-life examples of such ideas are Ofo and Mobike, founded respectively in 2014 and 2015, and referred to as the famous twin stars of start-ups in China where the demand for mobility is huge. They popularized the concept of sharing dockless and GPS-connected bikes² in major cities across the country that were rented through apps for which a small fee was paid by mobile phone (Wiese, 2020; Zhang, 2022). Also, web services have played their part by supporting collaborative interactions via websites between individuals,

matching, and coordinating supply and demand without owning physical assets, and assisting peer-to-peer transactions regardless of physical locations around the world. With a primary focus on doing business on the internet, many digital giants have implemented similar tech-based models in their services, deployed technical facilities such as social media, protected their online assets and more to enable sureness and prestige which are essentially perceived as a strong contributor to the emergence of the sharing economy (Ransbotham, 2015; Minami et al., 2021; Pouri & Hitty, 2021). Two compelling online brands associated herewith are Airbnb and Uber, which respectively represent the world's largest accommodation provider with millions of listings available worldwide, many of which are just owned by regular people, and the world's largest on-demand ride-hailing provider connecting millions of riders with drivers. Neither Airbnb nor Uber owns real estate or vehicles, but both of them digitally engage participants to cooperatively utilize underused inventory via fee-based sharing activities. As a result, a new digital-centric culture of sharing has arisen that has quickly made it possible for almost anybody and any business across the globe to make their belongings, products, and services accessible through online networks (Richter & Slowinski, 2018; Zhang et al., 2019). These technologically-driven datafied markets are inherently dependent on access to data as a resource for those assets (Rojanakit et al., 2022). A fundamental dilemma in data sharing is ownership versus use. Who owns the data, who can extract value, and under what conditions? This question is answered in the next paragraph.

² Many scholars trace bike sharing to the White Bike Plan, associated with the anarchist movement Provo, in Amsterdam in 1965 (Zhang, 2022).

01.3 Data sharing: A business necessity

The idea of sharing sounds appealing and is often associated with mutual benefit. However, when it comes to data, dynamics differ fundamentally from those of physical assets. Unlike material goods, data does not have a built-in limit on usage – sharing it does not mean losing it. Yet, this also means there is no inherent ‘maximum’ value to unlock through sharing. The strategic question, therefore, is not whether to share data in absolute terms, but how, when, and with whom sharing creates more value than withholding it. The potential to gain or lose through data sharing is never fixed; it depends entirely on the broader business context and competitive environment.

Traditionally, data has always been essential for internal efficiency, often used to populate spreadsheets, dashboards, or reports. For instance, the sales department might share customer data with marketing to support a targeted campaign. Today, data extends beyond internal functions and supports collaboration across organizational boundaries – offering insights into customers, partners, suppliers, and broader market behavior. A common example is a healthcare provider sharing anonymized patient data with research institutions to support medical advancements.

Many organizations are now exploring structured approaches to enable both internal and external data sharing across the value chain. The rise of a digital economy, driven by data, is a key driver of this shift. It encourages businesses to move beyond viewing data as a static input and instead recognize its strategic potential to reshape business models, products, and services.

Despite the concerns (e.g., competitive issues) and the dominant roadblocks (e.g., outdated information systems), data sharing is not an option anymore to just look attentively at, rather it is a must-do to drive value in various business practices that operate worldwide (Barnes, 2021; Nguyen et al., 2023). For instance, Airbnb benefits strategically from data by simultaneously enhancing both the user experience and the overall customer satisfaction and loyalty. This vital objective is achieved through analyzing search and booking patterns, offering personal recommendations, and providing relevant listings. Among other sharing activities, access to data about travel trends and customer behavior – digitally housed by the datafied accommodation giant – is granted to travel partners. Accordingly, these players are empowered to properly

improve the way in which they engage with customers, and to further tailor their go-to-market approach (Minca & Roelofsen, 2019; Revelate, 2022). Data sharing is a necessity to support the digital presence of businesses and accelerate their performance online with key benefits such as a greater cooperation with existing partners, establishing new partnerships, and the ability to create new revenue streams (Nguyen et al., 2023).

Different methods of data sharing have come into play in the past years, three of which are concisely highlighted below to create a certain image. Table 1 shows how they are usually mentioned, what their main feature is, what their high-level technological form looks like along with the way in which data usage takes place. Choosing a data sharing model is not merely technical, but also strategic.

The first method relates to traditional data sharing, which is the most common approach centered around downloading data. Via network access, data along with the right-to-use is allowed to flow from a data provider to a data consumer. It is in fact copied to the ICT environment of the latter actor that either uses it openly or for purposes which have been agreed with the concerned data provider. The second method is on-site data sharing according to which a data consumer remotely connects to an environment that is entirely set up and managed by the data provider. To ensure full alignment with its predetermined conditions, the latter actor decides which tools can be used and what data operations can be executed by the data consumer. The third method is federated data sharing which reflects a way in which different data consumers can exchange data without any need for centralization. This approach represents collaborative environments that are set up for data sharing across multiple decentralized sources under conditions directed and controlled by the data provider. It controls a trusted federated ecosystem and determines which data access is granted and what data is permitted to be collected (CADE, 2024; Costabile, 2024). It is notable that the federated data sharing method is also linked to data spaces³, which is referred to as the next revolutionary concept in data sharing.

They have come to the forefront of attention due to the growing demand for interoperability and data sovereignty. The concept is further described in the following chapter and is currently in the process of bringing specifications and implementations together to construct a common reference for standardization (Bacco et al., 2024).

Table 1. Some data sharing methods

Method	Feature	Form	Usage
Traditional	Data download	Transfer to the ICT environment of the data consumer	Free use or any purpose agreed with the data provider
On-site	Remote data access	Connection with an ICT environment supervised by the data provider	Aligned with the conditions pre-defined by the data provider
Federated	Data space	External access by diverse data consumers to a part of a trusted decentralized data ecosystem	In accordance with the conditions stipulated by the data provider



³ For a practical example, it is, among other cases, referred to the Centre of Excellence for Data Sharing and Cloud (CoE-DSC) funded by the Dutch Ministry of Economic Affairs (<https://coe-dsc.nl/>).

01.4 Research

Data sharing has recently been recognized as a true source of economic potential and opportunities that prompt more research. The world intelligibly revolves around data that is exponentially expanding every day. A recent study estimated that the total quantity of data generated daily is approximately 2.5 quintillion⁴ bytes (Kiourtis et al., 2023). Increasingly, it is examined to generate insights, is made use of to spark innovation, enhances the competitiveness of products and services, is an indispensable part of connected ecosystems, and offers many other advantages (Basselier et al., 2018; Luo, 2022). The desire for economic impact has never been greater, nor has there been such paramount pressure to responsibly deal with data sharing. Today, businesses are rightfully becoming more cognizant of the fact that there also comes a responsibility with creating, running, navigating, administering, and governing large geographically spread data landscapes. The obligation calls for protecting this particular capital and operating it provably in line with the applicable laws, regulations, standards, and frameworks. People are realizing that enjoying differentiated customer loyalty, engagement as well as retention, and mitigating the risks associated with data breaches are inseparable (Cash, 2023; Vallone & Frimpong, 2023). These days, many businesses have come to understand that there is a lot at stake in a world which is, so data-rich and technology-enabled (Wynn, 2023).

01.4.1 Goal

With data at the heart of the sharing economy, an on-demand awareness has risen that ideally goes for sharing-experiencing-feedbacking instead of owning-using-managing. Data is big and is getting bigger, which is considered a blessing and a source of concern at the same time. On the one hand, this growing marketplace appears to be cheaper with a higher ease-of-use, but on the other hand, it has entailed new challenges to tackle (Ransbotham, 2015; Basselier et al., 2018). The research aimed to surface possible resulting implications for common risk and assurance approaches that either were studied before or are already applied in practice.

01.4.2 Trigger

The larger the data, the greater also the shift in complexity, the chance of structural failures and inaccuracies, the likelihood of vulnerabilities due to misconfigurations and improper maintenance, the possibility of flaws in human handlings, and the susceptibility to cyberattacks and other harmful or threatening acts. These serious events are just a few examples of serious risks that are posed to modern tech-heavy businesses for which independent assurance provision has already turned into a hard requirement. Data is most certainly the precious lifeblood of the dynamic as-a-service economy in which sharing is nothing but a common practice. In the new reality, the existing, mostly static, way of dealing with risk and assurance is quite challenged. The question arises whether current approaches are still appropriate to manage risks and provide assurance on them. Perhaps it is now simply time to enrich these usual practices by discussing what needs to be added and transformed in order to meet the economic demands and expectations of the current data sharing era. This calls for more specific research as the scientific and pragmatic interest for the topic evolves and many questions are yet to be answered.

01.4.3 Question and nature

Given the aforementioned, the research question was formulated as follows:

How does the data sharing economy implicate the common risk and assurance approaches?

This exploratory research aimed to gather information and generate value for academia and businesses in both the public and private sectors. This descriptive study helps risk and assurance scholars as well as practitioners to gain a more detailed understanding of the subject matter, identify new dimensions, highlight future directions, and generate input for more focused, in-depth, and thorough investigations and engagements. Appendix A describes the methodology gradually applied to conduct the research. This approach includes four main phases that build upon one another and incrementally progress toward completing the research.

⁴ One quintillion bytes is equal to an exabyte which is enormous. It is roughly the amount of data of a Zoom meeting that lasts 100,000 years (O'Carroll, 2021).



01.4.4 Scope

The research team studied a wide range of specific and relevant literature and considered a large group of businesses. This group included Business-to-Business (B2B), Business-to-Consumer (B2C), Business-to-Government (B2G), Consumer-to-Business (C2B), Consumer-to-Consumer (C2C), Consumer-to-Government (C2G), Government-to-Business (G2B),

Government-to-Consumer (G2C, also abbreviated as Government-to-Citizens (G2C)), and Government-to-Government (G2G) (Jussen et al., 2023). Throughout the research, we aimed to maintain a technological perspective and treat both economic and social aspects of the data sharing economy with equal attention.

01.5 Organization

The structure of the rest of the book is as follows. Chapter 2 launches the idea behind the data sharing economy, explains its drivers and definition, and discusses related data terms and enabling technologies. In the next chapter, risks associated with the main components of this phenomenon, compounding risks and the implications of these adverse events are presented. Chapter 4 demonstrates various assurance concepts connected to the chief parts of the data sharing economy, details the modern assurance trends and describes their implications for this emerged concept. Every single one of the four

mentioned sections encompasses a list of concluding principles and is closed with a specific takeaway message. Chapter 5 comprises the conclusion of this research, a recommendation for further exploration, acknowledgements, and final remarks. Chapter 6 highlights the views on the research topic that were provided by the management board and leadership team of KPMG Netherlands. Also, six appendices accompany this publication that serve as supplementary material, useful for more background information.

01.6 Concluding principles

This chapter lays the basic groundwork for the rest of the present publication. It provides some elementary information in reference to the following:

- In datafying the world, data has turned into a new metaphysical principle of the virtual world. It is a versatile tool that, among other things, lets us better understand the social needs (e.g., mobility needs in growing cities) and enables businesses to launch digital solutions for smartly meeting those needs while on the go (e.g., a transportation app facilitating access to shared transportation, parking and public transport while also taking care of the related administration).
- The transformative nature of digital technology in shaping and reshaping businesses has become apparent soon and will remain a productive key strategy for the future.
- The sharing economy owes its disruptive power mainly to leveraging massively growing data volumes, its velocity, variety, veracity, value, and to ever-evolving technology developments. It has succeeded in extracting value out of idling capacity either with or without a monetary aim.
- To capture the full value from data, it is necessary to identify the right use case as well as to commit the right level of ownership on the business side. Equally so is the cruciality of creating the right technological capabilities that empower the sharing economy to operate on a scale.
- Dynamic data-driven organizations active in various industries depend on data sharing and rely on the digital foundation to ensure business agility in the present marketplace.

- Future research is expected to shed light on any possible consequences for risk and assurance that may result from the convergence of the online and offline world.

Takeaway

Data-driven, not without technology.

Data and technology are at the heart of the sharing economy that fittingly empowers the operationalization of different business and social practices. Advanced exploitation of bulky data landscapes by deploying sophisticated technological capabilities is the core of high value strategies. The power of data plus the transformational nature of technology along with the resulting opportunities have certainly changed how data and technology are perceived. Confidence and probability are the additional key factors in this combination to transparently obtain a bigger impact over time that is meaningful to the stakeholders and third parties.



02 Data sharing economy

It may appositely be stated that the sharing economy is neither a catchy catchphrase nor a promising trend. This phenomenon evolved by digital natives has overshadowed numerous traditional sectors and will undoubtedly persist in the future. It has quickly popularized the idea of using what is needed and only when it is needed and then to carry on with the next task. Sharing has confidently become a competitive business model in which millions of users and many entrepreneurs are active and offers access to expensive goods and services which may have otherwise been out of reach (Zhang et al., 2019).

Digital data is imperative in this collaborative ecosystem and functions as crucial input into the productions of a wide array of products and offerings. It is literally everywhere: in every market segment, in every economy, and in every business domain and its users (Manyika et al., 2011). It has already become the critical borderline where the classic economic order and its institutions uncomfortably face modern economic practices and the upcoming organizational forms. Resulting from the fast-paced technological revolution, digital data has gradually but inexorably been established in the modern high-tech business scene and is fundamentally changing the way in which economic value is created (Alaimo & Kallinikos, 2024). There is barely a dividing line to be drawn between buyers and sellers or consumers and producers, at least in the way that we historically used to clarify the distinction. Price is no longer shaped only by traditional supply-and-demand dynamics. In many cases, prices are not fixed at all, yet significant value is still created (Scelta et al., 2019). It is also clear that data plays a

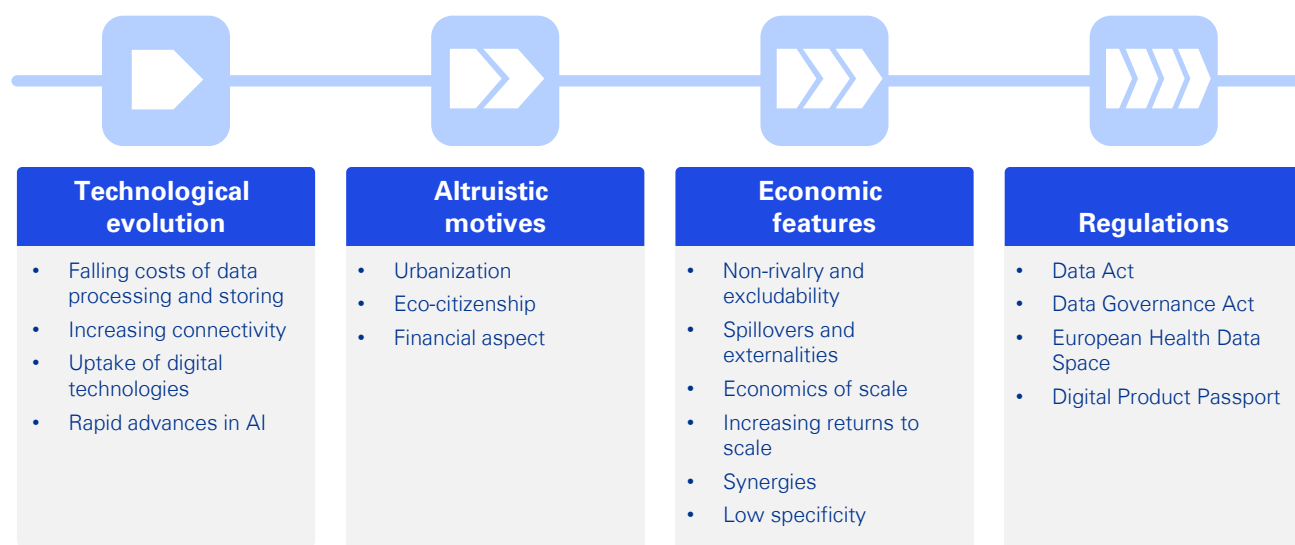
central role in supporting international trade and cooperation. Studies show that restricting cross-border data flows can slow economic growth (HMT, 2018). At the same time, structured data sharing between the public and private sectors can serve a wide range of policy needs. Governments are increasingly requesting access to the large data pools held by major platform companies in the sharing economy, such as Airbnb and Uber, to support regulatory and strategic objectives (CIPL, 2023). There is conformity that data sharing holds the potential to yield economic value for people, businesses and the broader economy (Stiglich, 2021). Although obtaining and organizing may come at a high cost, it is quality, volume, and usage that shape data into a multifaceted class of goods. At last, the benefits derived from data analysis differentiate business models and related value delivery, thereby strengthening a company's position and recognition (Schneider, 2022).

02.1 Driving forces

Data has always been of relevance to offline sharing economic models where resources are mostly shared without the use of ICT services. One such model are community gardens where internet-enabled strangers are denied access. Instead, predominantly unknown residents are allowed to assemble, look after a piece of land, and hence, create social capital (Sabitzer et al., 2018). More importantly, data is nowadays justified as an irreplaceable asset for business confidence and is thus a fundamental key to business recovery (Etherington, 2020). It sheds light on the path to move forward in the sharing economy whose engine is

mainly powered by multiple additional factors. Four of these main drivers are briefly reasoned below and are illustrated in figure 2 (Felländer et al., 2015; Basselier et al., 2018; MRF, 2024): a) technological evolution to which the sharing economy thankfully owes its breakthrough as clarified above, b) altruistic motives that boost others' confidence to change their behaviors, c) economic features that differentiate data from other resources such as oil to which it has been variously compared, and d) regulation that especially mandates acquiring and keeping grip on data handling and content moderation.

Figure 2. **Drivers of sharing economy**



02.1.1 Technological evolution

There are four main aspects related to ever-evolving technology that are paramount for success. The first one is concerned with the falling costs of data processing and storing. Gathering, processing, and housing data are low-cost activities now thanks to the availability of highly sophisticated computer hardware. An economic analysis shows that the actual costs of both processing power and data storage have halved every fifteen months over the course of the second half of the last century. The price of software started dropping at a much more moderate rate of about 2% per year since the early 1980s. The second aspect is increased connectivity. The number of internet users has significantly grown around the world from North America and South America to Europe and the Asia-Pacific. By 2000, only one quarter of the population in these regions was using the internet. By 2020, not only did the number of internet users there had increased close to 90%, but they had also used it more frequently and intensively. The third aspect pertains to the uptake of digital technologies. Smartphones benefit from the advanced solutions and have brought substantial processing capabilities into our lives that are much more powerful in comparison with large computers that were historically a business luxury. Another notable technology is the Internet of Things (IoT) that represents half of online devices across the globe, estimated by 2019 to be 20 billion, up from 8.8 billion in 2010. The fourth and last aspect concerns the rapid advances in AI. Vast amounts of easy-to-collect digital data go hand in hand with impressive advances such as machine learning (ML) that use these datasets

as a basis for predictions. AI is a widely considered potential to drive productivity growth by fostering innovation and enhancing automation. The number of related patents reflects an increased rate of almost 40% per year measured in the period of 2007 to 2021 (OECD, 2022; Penfold, 2022).

02.1.2 Altruistic motives

Social developments are chiefly linked to three factors. The first one concerns the worldwide population shift from rural to urban areas, putting together a large number of players that have created many shared consumable activities. This urbanization has digitally made these actors – however further apart – a positive and potent force for addressing sustainable economics. Research claims that most initiatives associated therewith are the logical response to the challenges and frustrations of living in busy cities (e.g., owning a car and parking problems). The second factor relates to eco-citizenship that actively stimulates sharing economy offerings. The environmental issues have led to a general awareness questioning the way in which resources are individually utilized. This change in terms of norms and values has triggered the emergence of new modes of efficient consumption. The third and last factor, often one of the main reasons to participate in the sharing economy, is the financial aspect. Engagement in this kind of transactions is based on either saving or earning money (Basselier et al., 2018).

02.1.3 Economic features

The economic characteristics of data are associated with six features. The first one is a built-in attribute and reflects nonrivalry and excludability. This means that data can repeatedly be used by multiple players without being exhausted. Also, it is about excluding, implying that businesses can preclude others accessing their data, and thus, protect it and act in alignment with applicable legal frameworks. The second feature is spillovers and externalities. The former takes place if businesses other than the one gathering data can profit or suffer costs. There are positive externalities when these benefits are not included in prices, and there are negative externalities if the incurred costs are transferred to prices. From a social welfare perspective, it makes sense to use positive spillovers in general as solid arguments for broad data sharing to, for instance, restyle production processes. In addition, negative externalities can occur when it comes to, for example, sharing one's personal data as this potentially publishes information about others. The third feature is concerned with economies of scale that is displayed by data generation. This means that the cost of creating a dataset is high compared to that of creating extra copies, which is negligible. In case marginal costs are around zero, it is the demand that completely determines the price. The value attributed to a set of data is consumer-dependent and results in differential pricing. The fourth feature relates to increasing returns to scale, indicating that a rise in economic activities means that more data is generated, which in turn leads to more economic activities, and so on. This feature has the potential to operate at the level of the economy when data is shared among businesses. Data can demonstrate increasing returns to scale as an ingredient in AI. The fifth feature is synergies showing how the value of data grows by disclosing trends or patterns. This helpful increase is exhibited through three common ways: a) data goes with other data of the same type (e.g., a data point about one person combined with data about the same individual over a certain period of time), b) data is accompanied with other data possessing complementary attributes (e.g., historical economic statistics mixed with real-time data from online businesses), and c) data comes with non-data inputs (e.g., a fast-paced adoption of AI can considerably grow the future value of data). The sixth and last feature pertains to low specificity. It indicates that data may be used for a wide range of production activities and may be reused for purposes that are

different from the one originally intended. A good example is anonymized mobile call data records of telecom providers that were reused to monitor and control the spread of COVID-19 (OECD, 2022).

02.1.4 Regulation

This section highlights four key regulations that aim to provide Europe with the tools to responsibly manage and share data in the digital age. The first is the Data Act, which seeks to ensure fairness in the distribution of the value generated from data by establishing clear rules and obligations for data access and use. It ensures that data sharing, storage, and processing align with broader European legal frameworks. The Data Act also builds upon and generalizes some of the B2C concerns initially addressed by the General Data Protection Regulation (GDPR), extending the principles of fairness and transparency into broader data use contexts. Complementing this, the Data Governance Act is positioned as a cross-sectoral instrument focused on establishing structures and processes to support voluntary data sharing. While the Data Act clarifies who can generate value from data and under what conditions, the Data Governance Act defines three types of data-sharing scenarios: a) reuse of certain categories of protected data held by public sector bodies, b) data intermediation services, and, c) data altruism (Akin et al., 2024). Together, these two legislations are designed to promote trustworthy, secure, and effective access to data, particularly in key economic sectors and areas of public interest.

In addition, there are sector-specific and topic-specific regulations, such as the European Health Data Space⁵ (EHDS) and the Digital Product Passport⁶ (DPP). The EHDS aims to create a common infrastructure and governance framework for the secure and trustworthy exchange and use of health data across Europe. It supports both primary use (for healthcare delivery) and secondary use (for research and policymaking) of health data (Hussein et al., 2023). The DPP, on the other hand, is intended to enhance product traceability throughout the supply chain, support environmentally sustainable business practices, and reduce product waste. It provides detailed information on a product's origin, composition, carbon footprint, reusability, and recyclability (Jensen et al., 2023).

⁵ It is referred to [European Health Data Space](#) for a clarification.

⁶ Go to [EUS Digital Product Passport Advancing Transparency and Sustainability](#) for a description.

02.2 Delineation and the definition of the data sharing economy

Presently, a generic definition for data sharing economy is still part of academic conversation and writings. A review of the literature revealed that this comprehensive concept is interplayed with terms including data sharing and sharing economy making the most sense (Awli & Lau, 2023). Therefore, it was continued by applying a straightforward approach that plainly consisted of two steps: definition step and characteristics step. It was intended to parse these two worlds and scope them properly, the results of which are summarized in table 2. It is noted that this list is indicative in nature and may be subject to some variations. It is hence not exhaustive and solely

presents two of the most distinctive elements (i.e., definition and characteristics) that are explicitly articulated in many publications about the topic (e.g., Codagnone & Martens, 2016; EU, 2018; Aaser et al., 2020; Klarin & Suseno, 2021; Goasduff, 2021; Minami, 2021; Michulek et al., 2023; Scott & Munichiello, 2024). In this publication, further clarifications, descriptions, discussions, suggestions, indications, point of views and other comments in relation to data sharing economy are thus interconnected with data sharing and sharing economy either separately or collectively.

Table 2. **Scoping data sharing economy** (Smichowski, 2016; Jussen et al., 2023)

Concept	Definition	Characteristics
Data sharing	The domain-independent process of giving third parties access to the datasets of others. These third parties may be other companies (usually not direct competitors), individuals, or public institutions. The shared data is often used to develop new applications and services. The expectation is to be compensated financially or through other benefits (e.g., receiving data) for providing the data. What the data may be used for and how it is made available is determined within the framework of the (legal) agreements between the data providers, data consumers, and other roles, depending on the use case	• Infrastructure • Technologies • Commercial agreements • Services • Customer groups • Actors • Data types
Sharing economy	A way of producing and/or distributing exchange value and/or use value based on peer-to-peer interactions channeled through digital platforms and where most of the peers' participation is not driven by wage relationships	• Crowd-based networks • Digital enablers • Access above ownership • Experience over maintenance • Power balance • Social implications • Legal frameworks • Data marketplace



02.2.1 Definition

Step one simply started with going across the available definitions of the notions of data sharing and sharing economy. The former is a broad terminology that lacks an uncontested definition (Richter & Slowinski, 2018; Lee, 2021). It is defined by several authors, among whom it is focused on an exchange of data between various stakeholders (e.g., Nokkala et al., 2019), while another study emphasizes access to complementary data sources for innovation purposes (e.g., Vesselkof et al., 2019). A synthesized definition is stated (i.e., in Jussen et al., 2023) that captures the most pertinent aspects addressed in the reviewed publications. Analyzing the existing literature on sharing economy led to a similar outcome. In other words, the definition of this concept is neither consensual nor rigorous and is on the other hand often interchangeably used with terms such as collaborative economy and on-demand economy (Felländer et al., 2015). Some researchers stress a socio-economic paradigm that can foster more social cohesion and collaboration while easing the strain on the environment (e.g., Liu et al., 2020), whereas other writers center the discussion around an economic model facilitated by the digitalization component (e.g., Awli & Lau, 2023). Based on reviewing the existing literature, a definition has been provided (i.e., in Smichowski, 2016) that complements the relevant factors with plainly treating data generated in the sharing economy as a common.

02.2.2 Characteristics

In step two, the characteristics of both data sharing and sharing economy were studied (e.g., in Nguyen et al., 2023 and in Marchi & Parekeh, 2015). It was pointed out that they are diverse in nature and overlap to some extent, which is also partly indicated above. The features associated with data sharing are oriented towards an infrastructure such as that of data sharing facilities for sharing data to various domains. It is built upon terms of using and accessing – usually stated in agreed-upon commercial documents – and is enabled by modern technological advancement such as blockchain. A link is made with services, such as data

analysis execution, that result from data sharing between different parties, including governments and businesses. Naturally, these groups are important to a number of actors such as data providers that are, for instance, interested in delivering anonymous personal data. In addition to the allocation of idle resources, the characteristics of sharing economies are related to an existing network of interconnected individuals at the core of activities that rely on digital enablers (e.g., smartphones) to interact and create economic returns. In fact, it has been claimed that there is no sharing economy if there is no technical online device (Peugeot, 2014). Temporary access is prioritized above permanent ownership, and so is tailored experience over ongoing maintenance. These changes in behavior have a potential to result in an undesirable power balance between users, and more importantly, between owners and the digital platform. One such example is when a customer of an accommodation provider can directly book a house without the host needing to accept it if the profile of this individual is verified in accordance with certain requirements. Another example is when the payment of the customer is processed to the platform while the host receives his money one day after check-in. The inappropriate utilization of confidential and sensitive data potentially causes social implications. A thorough understanding of respective indications needs to be gained to ensure a responsible use of data that is dictated by legal frameworks like laws and regulations. These enablers should help protect the rights and interests of players and ensure fairness and transparency of sharing economies. This prerequisite is equally applicable to data marketplaces because of their contribution to the growth by promoting data-driven innovation, fueling the competitiveness of businesses of all sizes and unlocking job markets (Abbas et al., 2021). This digital marketplace is where the data assets encounter data consumers in one cloud platform (Smichowski, 2016; Constantiou et al., 2017; Jussen et al., 2023; Sestino et al., 2023; MRF, 2024; Mucci, 2024a).

02.3 Digital platforms

Nearly every subject matter research addresses digital platforms as the main innovation in the data sharing economy. These technological components are the prominent base that distinctly empowers this economic model to operate. They are the stable core of the modern ecosystem that, among other amenities, support constructing, running, and administering multifunctional mobile apps as well as deploying digital solutions (e.g., AI) to enable value generation in a way which was not possible in the past. Irrespective of any payment, underutilized products and services are now faster, cheaper and on a larger scale available. These material assets are digitally presented in diverse geographical locations and market segments where a smaller number of players are active and where business opportunities are surfacing that were neither reachable nor sizable before. Broadband internet and the popularity of smartphones have prominently created the pathway for success and have made it not only easier and quicker, but also more natural to execute transactions in digital fashion. With instant matching, offers are linked to those widely spread around the globe that are interested to use them, as a consequence of which a large-scale yield is possible by reaching a larger group (Luo, 2013; Basselier et al., 2018; Coyle & O'Connor, 2019). Technologically, digital platforms enable programmability and reuse of data, and additionally, arrange modularity between a solid core and variable parts. Economically, their chief function is to aid decreasing costs of transactions by combining various data sources and attractively attaching users to suppliers (Richter & Slowinski, 2018). In short, digital platforms are instruments that lay the strong technological ground for each stakeholder to aggregate data for mutual benefit or that of customers (Nokkala et al., 2019; Lim, 2020b). They are the emerged intermediaries that are playing their crucial part in the data sharing economy as they are seen to potentially increase willingness to share data (Richter & Slowinski, 2018). Such a platform is therefore a convergence of digital and economy as it is more than just a passive digital infrastructure that facilitates players to exchange and interact. It is, additionally, an active market organizer model that keeps track of capacity, connects those with common interest, takes part in the peer-to-peer relation, and finally gains profit from the exchanges (Shmidt, 2023).

02.3.1 Definition

Designing, organizing, and orchestrating the new mode of economic and social operations are usurped by digital platforms. Due to their high degree of adoption and multidimensional nature, they have rapidly landed on the research agenda, resulting in a growth of related literature clarifying them from different perspectives (Asadullah et al., 2018). Some writings go for an organizational point of view to explain what they are about (e.g., De Reuver et al., 2018), while another contribution applies a software development and production approach to describe them (e.g., Ghazawneh & Henfridsson, 2013). Taking the broader context of the research into account (i.e., the distributed nature of the data sharing economy, the intertwinement with institutions, sectors, automated advancements and more), a definition of digital platforms is provided here (Nokkala et al., 2019): Products, services, or technologies that act as a foundation upon which external innovators, organized as an innovative business ecosystem, can develop their own complementary products, technologies, or services.

02.3.2 Features

Other features also expound the effectiveness of digital platforms that complement those addressed above (e.g., lowering transaction costs, governance structure of the community, and peer-to-peer exchange). To paint a picture, three of those distinguishing attributes are concisely described in this section. Firstly, it is supported with setting up and managing the technological development of additional products achieved by modularity and proper governance rules. For instance, a CSP encourages and incentivizes external contributors to engage in its application development activities. Secondly, digital platforms can create new outputs that are delivered by a big and varied group of users, a phenomenon that is also referred to as generativity. An example is a crowdsourcing platform that leverages different responses to a certain issue provided by various involved parties. Thirdly, the value of digital platforms for players on one side grows when the number of participants on the other side increases, which is also known as a cross-side network effect. A good example

is an e-commerce platform that offers added value to sellers when there are more buyers on the other side, and vice versa (Asadullah et al., 2018; De Reuver et al., 2018). The discussed features reveal that they are a source of organizational efficiency and exert influence on the mode of power relationships in concerned communities (Smichowski, 2016).

02.3.3 Categories

Some literature either narrowly or generally groups digital platforms on the basis of parameters and aspects (e.g., Richter & Slowinski, 2018). A more detailed categorization of these instruments is described below that makes a distinction between four different dimensions and associated types shown in table 3. The first dimension is a business model that has three types. The first one, called an integrator platform model, concerns a vendor providing a platform that external software engineers can join and create apps on for end users, for instance iOS, which resembles the first feature of digital platforms indicated above. In this manner, Apple can keep track of the transactions on its platform, and accordingly, make a profit from them. The second type, known as a product platform model, is about external developers building apps on top of a platform made available by a third party and selling them directly to end users. This way of working is adopted by cloud providers such as Google that have less control over the transactions completed on its platform. The third type, referred to

as a multisided platform model, pertains to external parties that openly interact with end users via the platform without directly involving its owner, similar to Facebook. In this case, the latter can however identify and enforce rules to be followed. The second dimension is an interaction mode that possesses two types. The first one, called collaborative platforms, is controlled by social norms and flexible rules. It consists of platforms stimulating external contributors to provide open access to information, as is the case with Wikipedia. The second type, known as competitive platforms, support external players to design and develop competitive products and services. Specific preferences are being taken into consideration, so end users on the other side of the platform can choose a selection, one example being video games on consoles. The third dimension is governance mode, and this also entails two types. The first one, referred to as opened platforms, relates to those with a relatively open mode of governance such as Linux. The second type, called closed platforms, refers to those with a tighter governance for the development of apps, such as Google Android. The fourth and last dimension is an ownership structure, which similarly includes two types. The first one is known as property-based platforms, such as Microsoft Windows, and the second type is referred to as open source-based platforms, such as R software packages. Both ownership structures apply different approaches to price, sale, profit-making, and social impact (Asadullah et al., 2018).

Table 3. **Categorization of digital platforms (Asadullah et al., 2018)**

Dimensions of categories	Type	Example
Business model	- Integrator platform model - Product platform model - Multisided platform model	- Apple iOS - Google cloud - Facebook
Interaction mode	- Collaborative platforms - Competitive platforms	- Wikipedia - Video games on consoles
Governance mode	- Opened platforms - Closed platforms	- Linux - Google Android
Ownership structure	- Property-based platforms - Open source-based platforms	- Microsoft Windows - R software package

02.4 Data focus areas

In the literature, plenty of data terms (e.g., data altruism, data sovereignty, data democratization, data deduplication, data analytics, data concatenation, data as a service, data mashup, data silo, data imputation, data deception, data catalogue, data science, Data Lifecycle Management (DLM), data discovery, data subject, and data intermediation service) are discussed. In the context of research, it can be said that approximately the same applies to two previously mentioned concepts that are frequently linked to data focus areas: data markets and data spaces. Along with other driving forces, the Data Governance Act establishes their dominance and importance in Europe by assisting the latter concept and striving to enlarge trust among participants in the former concept (i.e., data market). Therefore, the discussion around them is resumed here (EU, 2022; DSSC, 2024a). In addition, the emergence of a new data focus area is pointed out in the literature, in which it is referred to as data fabric (e.g., see Mezzeta, 2023 or Nexla, 2025). For this reason, it is also further described in this section.

02.4.1 Data market

In general, four classifications of data markets are distinguished, and below, they are concisely described (OECD, 2022). The first one is bilateral markets, known as one-to-one, in which trading with a maximum cardinality of one for every party is exclusively upheld by relational contracts that can lead to high transaction costs like search costs. A good example of such markets is data brokers. The second classification of data markets pertains to dispersal markets, referred to as one-to-many, in which an individual seller transacts with numerous buyers in accordance with standardized terms of exchange. A typical example of this type is markets in which data is exchanged by means of an Application Programming Interface (API). The third classification of data markets relates to harvesting markets, also called many-to-one, in which data is generated by the use of digital services. Sellers make this data available to one service provider, normally in exchange for free access to the service. In this case, the availability of data is heavily dependent on the nature and the success of the service concerned. The fourth and last classification of data markets is concerned with multilateral markets, known as many-to-many, in which a large number of sellers and buyers transact through digital platforms. These activities take

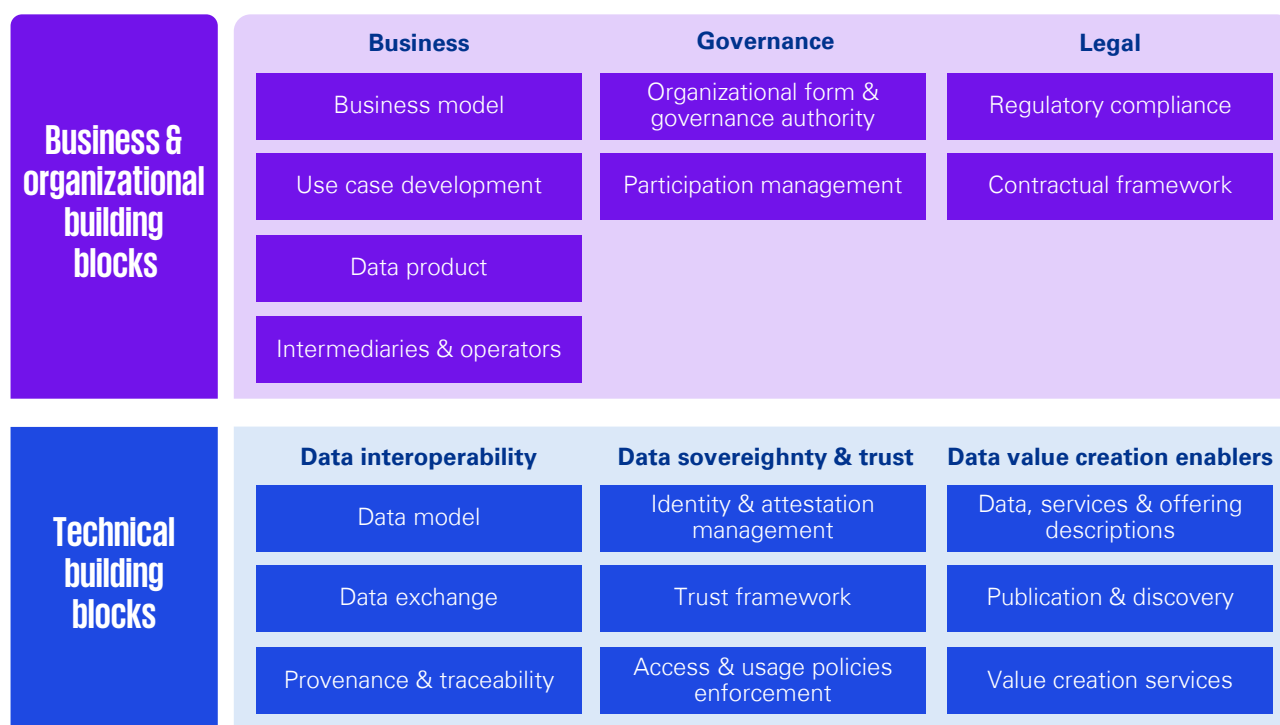
place under standardized licensing models and regulations with respect to data access and usage (Rasouli & Jordan, 2021; OECD, 2022).

02.4.2 Data space

Data spaces are one of the focus areas with a contribution to economic growth and are extensively addressed in a blueprint. This extensive set of guidelines is provided by the Data Spaces Support Centre⁷ (DSSC), funded by the European Commission as part of the Digital Europe Program and constitutes seventeen manageable parts (DSSC, 2024m). Figure 3 collectively schematizes these so-called building blocks in six groups. These categories range from a) business (i.e., business model, use case development, data product, and intermediaries and operators), governance (i.e., organizational form and governance authority, and participation management) and legal (i.e., regulatory compliance and contractual framework) – also referred to as business and organizational building blocks – to b) data interoperability (i.e., data models, data exchange, and provenance and traceability), data sovereignty and trust (i.e., identity and attestation management, trust framework, and access and usage policies enforcement), and data value creation enablers (i.e., data, services and offerings descriptions, publication and discovery, and value creation services) – also called technical building blocks. They are comprised of information about elements and their functions and contain information about specifications of technical capabilities (DSSC, 2024d). In short, building blocks provide guidance. Business, and organizational building blocks are useful instruments for every initiative and participating player to understand the essential components and the way in which they interrelate, and to cohesively set up and run data spaces. The building blocks help the stakeholders to financially maintain these systems, adhere to legal obligations, and meet objectives (DSSC, 2024e). Technical building blocks guide Data Space Governance (DSG) authorities and players to make informed decisions. They mostly point out common standards in enabling the reuse of technical solutions and support to reach interoperability on a technical level (DSSC, 2024m).

⁷ Visit <https://dssc.eu/> for further information.

Figure 3. **Data spaces building blocks** (DSSC, 2024d)



To leverage the building blocks, participants have a set of tools at their disposal to establish and take part in a data space. For the technical building blocks, the toolbox chiefly contains software solutions that include a participant agent, a credential store, or a vocabulary service. In the case of business and organizational building blocks, it is about frameworks, canvasses, rule books and templates (DSSC, 2024b). The link between the blueprint building blocks and the implementations in the toolbox is shaped by three groups of services (DSSC, 2024m). The first one is federation services that fulfill an intermediary function. They support the interplay between the parties active in a data space and empower them to engage in data sharing of all types and forms (e.g., commercial in nature). The second group relates to participant agent services that help implement a) the control plane, i.e., the responsibility to decide the way in which data is managed, routed and processed, and b) the data plane, i.e., the actual sharing of data (DSSC, 2024m) in some cases. These services make it possible for a single participant to join the data space, enable the provision or use of data, determine access and usage policies, and more. The third and last group is value creation services that are additional data space services in connection with value creation (e.g., a data access and ingestion service that is designed to approach and extract data from different sources) as the name suggests (DSSC, 2024m; DSSC, 2024j; Brousseau et al., 2024).

02.4.3 Data fabric

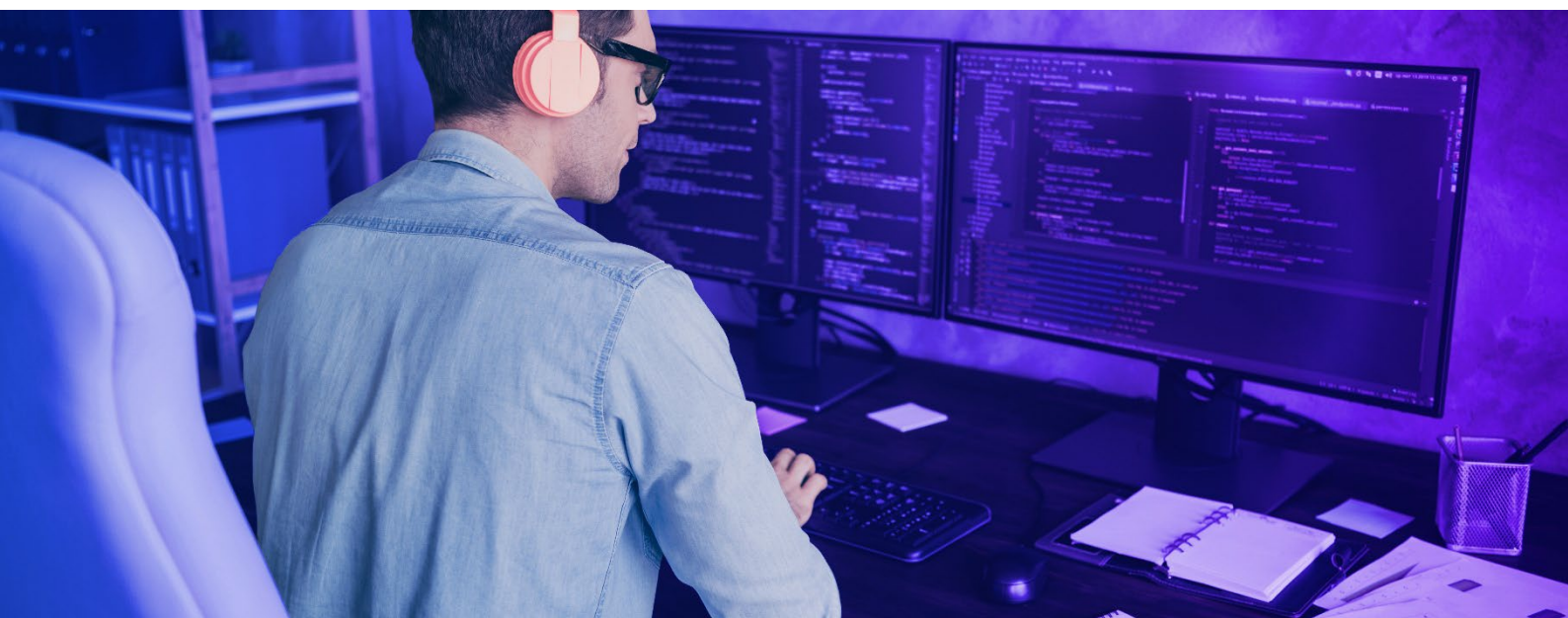
Another upcoming data focus area is data fabric, which is strategically positioned as a modern data management and data integration concept. Its chief promise lies in streamlining data integration infrastructures and facilitating scalable architecture in distributed environments. It decreases the complexity of technical challenges associated with integrating tools, systems and processes intended to construct a unified data landscape. In contrast with the traditional approach to data integration, the data fabric strongly depends on digital technology (e.g., ML) to empower real-time access. In other words, this emerging design choice is expected to enable an end-to-end integration of varied data pipelines and cloud-based landscapes. It goes beyond a cost-effective or elegant design and incrementally proposes data utilization, context analysis and alignment use cases (Zaidi, 2023; IBM, 2024). Given its relevance for data ecosystems building upon technological advancements, data fabrics include three core components: a) data governance, i.e., a mechanism to effectively control and monitor sensitive data in line with various privacy regulations such as General Data Protection Regulation (GDPR), b) data security, i.e., providing extended security levels to ensure proper data access, and c) enhanced data processing capabilities, i.e., multiplying processing speed and pushing predictive analytics to enable quicker and more informed decisions (Kanagarla, 2024).

02.5 Enabler technologies

So far, an array of existing technologies such as the web and internet and a number of emerging technologies like IoT, big data, AI, cloud and blockchain have been pointed out. The discussion about the latter five is briefly continued in this section because they are particularly entitled as the key enabler technologies to which the following fourfold argumentation applies (Sestino et al., 2023; Jussen et al., 2023). These stars on the data sharing economy sky demonstrate a) a fast evolution mostly in terms of power and speed, b) are transformative in nature, c) have almost a direct impact, and d) are above all scalable (Gumi, 2022). It is notable that three other technologies are used in relation to making data sharing possible: Privacy Enhancing Technology (PET), Self-Sovereign Identity (SSI), and digital twin (Pals & Roso, 2024). Therefore, these enabler technologies are also briefly introduced below. Details (e.g., information about branches like ML in case of AI, models such as IaaS for cloud, or hybrid blockchain as one of the blockchain types) with regard to the enabler technologies are not discussed in this section.

IoT, the first enabler technology, represents smaller internet-based objects (e.g., smart devices used across homes and in other forms of equipment and infrastructure) that constantly send and receive information over the internet. They are digital data generators, offer complex computing solutions and provide the possibility to digitally monitor and control the physical world (Gumi, 2022; Levy et al., 2024). Digging into the massively generated datasets – to understand the impact of IoT – is a common necessity in sharing. The second enabler technology, big data, helps to match consumers with what they specifically

look for. Algorithms leverage data points as Global Positioning System (GPS) locations to connect consumers with the providers that most meet their needs (Manyika et al., 2011; Ayers, 2024). AI, the third enabler technology, makes full use of large digital datasets with more variable, longer timescales, and higher granularity to extract serviceable and actionable insights held therein. They are valuably applied by sharing economy platforms to their offerings with the aim of providing more specific and personalized recommendations to consumers (Agarwal et al., 2021; MIT, 2023; Thomas, 2024). The fourth enabler technology, cloud, refers to the on-demand and scalable usage of computing resources. It has been argued that the concept of digitally sharing resources owes its disruptive power to cloud service models (e.g., SaaS) through which millions of people network with their peers worldwide. Every single one of these internet-based environments are in and out of themselves microcosms of the data sharing economy (Thilakanathan et al., 2014; Gupta, 2015; Swaminathan et al., 2024). Blockchain, the fifth enabler technology, is a shared ledger across a network of participants that contains data packages with records of completed transactions, thereby making data simultaneously accessible to all parties. It is a technology that helps the data sharing economy to automate processes in a distributed manner (Menne, 2018; Carson et al., 2024). A good example is a sharing application whose core is based on a smart contract functionality. It supports signing a rental agreement and assists in managing the related process, all of which are stored within the blockchain (Bogner et al., 2016; Babkin et al., 2018).



The sixth enabler technology, PET, encompasses diverse technologies, methods, and tools (e.g., secure Multi-Party Computation (MPC)) that are basically applied to ensure the fundamentals of data protection. Strongly associated with privacy-by-design, these principles, among other functionalities, involve minimizing personal data use, maximizing data security, and empowering individuals (ENISA, 2022; Noble, 2023). It is described that PET facilitates increasing trust in data sharing when generating insights is required while the underlying data needs to remain unrevealed (Molengraaf et al., 2023). SSI, the seventh enabler technology, makes it possible for individuals to take full ownership and control of their digital identities, as a result of which the involvement of a third-party provider is unnecessary. They are accordingly empowered to determine who can view their data and can revoke access to it at all times

(Truvera, 2025). Note that SSI ensures a high degree of trust in digital data exchange, even between parties that mistrust each other, as data upon receipt can electronically be verified for authenticity and validity (Wall Bake & Pals, 2024). The eighth and last enabler technology, digital twin, is a virtual replica of an object, a product, or a service, and is indicated as a potential technology that supports in optimizing the performance of the data sharing economy model. It is argued that it is valuable to, for instance, healthcare, where sharing fresh operational data, leveraging available inventories (e.g., goods and resources) and exchanging them would help save lives (RTLS, 2024). The aforesaid enabler technologies along with their relevance for the data sharing economy are enumerated in figure 4.

Figure 4. **Relevance of enabler technologies**

01	IoT Smaller internet-based objects that generate, send and receive digital data	05	Blockchain A distributed chain of data packages that fuels sharing processes to be automated
02	Big data A solid base for digital points necessary to match consumers with providers of sharing	06	PET Capabilities to safeguard personal data while collected, stored, processed and shared
03	AI A capability obtaining insights from datasets to offer personalization to consumers of sharing	07	SSI A model that increases trust in sharing data by digitally verifying its authenticity and validity
04	Cloud A dynamic and scalable digital foundation that increases agility in sharing of resources	08	Digital twin A virtual reflection of a shared physical product or process aimed to represent and monitor it

02.6 Trust

Trust is an abstract concept and has always been a cornerstone of a successful private and business life. The term is defined as (Mayer et al., 1995): 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. It was indicated that trust had three separable characteristics: a) ability, i.e. a set of skills, competencies supporting a party to exert influence on some specific domain, b) benevolence, i.e., the extent to which a trustee has right intentions with the trustor, and c) integrity, i.e., the trustor view of whether the trustee acts in accordance with the principles to which the former actor agrees. The operationalization of trust was hence based on the level of ability, benevolence, and integrity of the platform that could lead to trust herein plus the level of ability, benevolence, and integrity of the provider that might result in trust in this actor. Meeting these two main requirements was equal to trust in the overall service offered (Mayer et al., 1995).

02.6.1 Sharing economy

The early understanding of trust was primarily manifested by social concerns rather than potential economic values. The initial intention was to join a participative mechanism to foster personal relationships via sharing resources, services, or knowledge. Classic examples are daily activities like driving to another city, having lunch, or doing laundry. It made much more sense to execute them collectively rather than individually, which resulted in a more sustainable as well as delightful way of sharing. At the time, trust was predominantly linked with relational interactions. Especially because of the fast pace of digitalization over the past years, factors associated with sociability, customized experience and pleasurable lifestyle have been deployed by sharing platforms as marketing strategies to drive profitability. The arisen economy also entails the so-called reputation systems being a digital tool by means of which users can create their own reputation, rate products and services of providers, report their opinion about the behavior of other users, and express their positive or negative experience. This unique feature clearly differentiates the sharing economy platforms from the traditional digital markets (e.g., Craigslist⁸),

although the internet as well as the overcapacity of goods and spaces are still a crucial part in both. Accordingly, the personal and direct interrelations that mainly symbolized trust in the past have been transformed by the sharing economy into virtual systems where reputation is mostly determined by ratings, comments and feedback that are provided online by various known and unknown users around the world (Miguel et al., 2022).

The application of contemporary platforms is a common digital way to build reputations and open new possibilities for gaining trust. The latter is perceived by participants as the most distinguished quality of the modern sharing economy. It has already turned into an intangible asset that, on the one hand, visibly attracts customers, and on the other hand, measurably decreases transaction costs (Michulek et al., 2023). Today, trust has shifted towards transactional exchanges as the sharing economy is centered around non-ownership transfer exchanges in the user-provider-platform triad in which the latter acts as an intermediate. In this context, the term thus possesses three differentiating features glued together by the platform. The first one pertains to creating trust between strangers in which digitalization provides a setting to establish trust in the form of cyber trust. The second feature is concerned with democratizing and facilitating evaluations from others, which are made possible by the platform to reduce the uncertainty for the exchange of services. The third and last feature is related to the actors, i.e., users, providers, and nonprofessional peers, whom are coordinated by the platform whose functioning can also include handling financials and evaluations (Pelgander et al., 2022). It is notable that the more recent literature connects trust to responsiveness and trust cues (e.g., description of products or services offered, certificates, profile photos, insurance, and escrow services) in addition to reputations and parties' experiences. These indications are evaluated based on the level of details made available and the fact whether they are backed up by reputational confirmations (Räsänen et al., 2021; Pelgander et al., 2022). A typical example is the case with homeowners that must trust Airbnb to cautiously select users who wish to rent rooms, and their business partners like CSPs, particularly now that security and privacy concerns go hand in hand with

⁸ See [Craigslist Amsterdam](#) for more information.



digitalization (Barsch, 2025). Trust is the key factor that determines whether sharing initiatives lead to the defined outcomes and requires constant focus to remain dependable. In a provable fashion, this concept should explicitly be the solid ground for any effort in the sharing economy. It makes a clear difference by drawing in customers and other actors to willingly follow, show ongoing loyalty, and continue to contribute to steady growth (Vitasek, 2024). It has been pointed out that research has a strong focus on users' trust in the providers to which the following simple argumentation applies. Initially, both users and providers do not presume a frequent exchange with one another, but they could assume so with the platform (Pelgander et al., 2022).

02.6.2 Data sharing

Trust is a critical enabler of effective data sharing. Without it, ecosystems become disrupted, preventing the full potential of data from being realized and limiting both its economic and social value. For data sharing to thrive, trust must exist among four key players within the ecosystem (Frontier, 2021). The first group consists of those who add attributes and dimensions to a dataset. Their contribution makes the data valuable, and trust in the organization sharing it is essential. The second group includes those responsible for collecting, managing, or facilitating access to the data. These participants must demonstrate their capability and integrity to handle data ethically. The third group comprises the data users, who rely on the accuracy and validity of the data to generate insights that enhance or create products and services. The fourth and final group is the broader

community surrounding the data ecosystem. For instance, the general public must recognize the importance of trust to support data flows, which ultimately allows value to be derived from this vital resource (Frontier, 2021). It is thus not a light decision to determine with whom data is shared, which, among other activities, allows them to mine it for its worth. The process for selecting the right partners is normally performed based on regular technical and nontechnical criteria that include and are not limited to: a) commercial/financial, e.g., restricted individual datasets versus numerous datasets and data volume, b) operational/technical, e.g., platform and data storage, and data input and metadata, c) ethical, e.g., ensuring the continual trust in process and level of transparency to users, and d) legal, e.g., scope of use and end of term (Thereaux & Keller, 2021; Bird, 2024; Letourmy, 2024). Operating a framework for trusted data sharing is usually recommended to get a grip and maintain a hold on the entire data partnership process from conception through completion. From this end-to-end perspective, such a framework functions as a guideline for data sharing and points out key considerations that need to be taken into account during the whole trajectory. They intend to help ensure that every participant active therein is capable of handling and managing data assets responsibly. Trust principles are hence centered in the framework to create tangible positive impacts on data sharing. There are six core principles – depicted in figure 5 – that are generally referred to (IMDA, 2019). The first one is about transparency. It reflects the players' revelation of every piece of data that is demanded to make the data

partnership a success. The second core principle is concerned with accessibility. It indicates the importance of the capacity as well as the ability of participants to access the data anytime, anywhere and with any device. The third core principle pertains to standardization. It stresses the relevance of consistently deploying controls with a different nature to the data partnership, such as legal, technical, and organizational measures. The fourth core principle is connected with fairness and ethics. It stresses respect for the data protection and security requirements by also emphasizing the need to use ethical standards in favor of data sharing systems from the very first day of their design. The fifth core principle relates to accountability. It addresses proving compliance with any applicable laws, regulations, rules, and agreements specific to the data partnership. This adherence is additionally supported by steady governance structures and the culture of responsibly handling data. The sixth

and last core principle is linked with security and data integrity. It relates to the operationalization of controls to safeguard data in order to create and run a secure data sharing environment (IMDA, 2019). In light of the abovesaid, it is notable that the literature also addresses trust principles by choosing an indispensable component of a data ecosystem such as digital repositories. For enabling access to data and providing services to use it, there are five principles that are largely covered above, and jointly, they abbreviate as the term trust. Ordered sequentially, they are a) transparency ("T"), i.e., repository data services publicly verifiable, b) responsibility ("R"), i.e., integrity of data holdings, c) user focus ("U"), i.e., data management norms and wishes, d) sustainability ("S"), i.e., continuity of data services, and e) technology ("T"), i.e., infrastructure and capabilities to support these services (Lin et al., 2020; ARDC, 2024).

Figure 5. Data sharing trust principles



02.7 Concluding principles

This chapter provides a glimpse of some general aspects that are pertaining to the data sharing economy. The following principles are raised:

- Data sharing economy is far from being univocally defined and is still contested in the academic debate. It is an emergent phenomenon about which specific literature is yet to grow in numbers and maturity. Data sharing and the sharing economy are its fundamentals which are inextricably intertwined with a sophisticated technological foundation.

- Digital platforms are constructed for collaboration and are at the service of economy. They are surely not a one-hit wonder and have restyled the traditional value creation. These iconic multisided backbones are the recognized face of the sharing economy and data is the language that is spoken by them. They are a central ingredient in formulating and implementing differentiating strategies to uniquely create substantial economic and social value and attract a customer base.

- As a follow-up to the earlier discussion on data regulation, it is important to highlight that trust in digital platforms – particularly in their ability to organize fair and open markets – is supported by regulatory frameworks such as the Digital Markets Act (DMA), which focuses on fairness in Platform-to-Business (P2B) relationships, and the Digital Services Act (DSA), which addresses transparency, accountability, and safety in Platform-to-Consumer (P2C) interactions. These regulations aim to ensure that digital platforms operate in ways that are competitive, trustworthy, and aligned with public interest.
- The sharing economy deemphasizes ownership, is a resource-saving and multifaceted phenomenon with ramifications on the world stage. This global character has given it life and the possibility to annually move serious amounts of capital. It holds a cap on pricing idle or underutilized capacity by sidestepping commercial retailers, making products more accessible, affordable, and enjoyable for everyone.
- Data focus areas are interrelated. Data market is a high-level representation of a model to match demand and supply components (e.g., owners, operators, and third-party providers) and their interactions at the business level. Data space reflects the facilities (e.g., data models, data sharing contracts, and governance structure) that need to be in place to enable the functioning of the data market at the process level. Data fabric technologically arranges what is needed (e.g., data pipelines, metadata, and AI for data integration) at the operational level to make the data market a place where participants transact.
- Technology advances are one the core forces behind the services (e.g., short- and long-term homestay services offered via Airbnb and ride services provided by Uber) that drive the engine of the modern social and business lifestyle. In most cases, a smartphone, an internet connection, and an app are simply enough to engage in the sharing economy.
- Enabler technologies and their possibilities (e.g., low-cost cloud storage, big data analytics, and AI solutions) are the true decisive factor in sharing and data exchange between the players that are active in an ecosystem.
- Traditionally, regulatory compliance has been a core business driver at the international level. The difference is that regulation now possesses a strong technological focus and pays great attention to data and how to share it. In addition, the regulatory settings are nowadays oriented towards the way in which data is exchanged and accessed in a specific sector like healthcare.
- Key principles like reputation and trust are the base of the 'sauce' that sharing businesses digitally establish through crowdsourcing.

Takeaway

No digital platform, no data sharing economy

This rapidly expanding and disruptive model addresses long-standing challenges in the traditional economy, such as poverty, limited access, and social exclusion, while creating new value across products, services, and partnerships. Digital platforms serve as the technical infrastructure enabling this shift, embedding features like reviews, ratings, and reputation scores to build trust where traditional assurance mechanisms are mostly absent. In this context, trust is still essential but functions more informally, earned through platform transparency, user feedback, and ongoing interactions rather than audits or certifications. This shift prompts a strategic question: what role does assurance play now? As platforms grow and risks become more complex, formal assurance can support data integrity, validate platform security, reinforce the trust critical to system stability, and more. Assurance could then evolve easier from back-office control to a front-line enabler of digital trust.

03 Risk

Today, there is no question that data sharing is a business imperative. Hereto, accounting for a next level of speed as well as presuming a modern stage of productivity are mainly central. However, they have a dark side too and require craftsmanship to find, attain, and preserve the right balance. A plan to totally go for the economic or social value of data can come undone due to a wide array of areas that can be unknown, overlooked, misinterpreted, or underestimated. Painful experiences and lessons learned dictate that it is wise to become more critical about what data to share and what data to keep, when to open up and when to withhold data, and how to share data and how not to, and more.

It is quite important to constantly spot and chase opportunities. On the other hand, it is equally important to actively mitigate any intended or unintended consequence to confidently create value, interact and collaborate in a digital style that is obliged by many. After all, the whole idea is to be an attraction in business rather than an easy-to-attack target (Birkinshaw & Cable, 2017). For quite some time now, concerns and issues have noticeably surfaced whether vulnerabilities exist in current sharing practices that are exploitable, gaps are found that can be exposed, and other weaknesses are discovered that generate undesired openings. The fear is growing that these threats may happen with the potential to result in any type of trouble or cause any form of damage. It is real that malicious incidents can actually happen with an adverse impact upon the predefined goals and other planned outcomes. Hazardous barriers and unwanted events can occur in all sorts of forms and mostly lead to doubts, headaches, and uncertainties which in turn, among other unwelcome predicaments, keep consumers from spending and businesses from investing (Dash et al., 2020). These parties still primarily find themselves questioning whether the risks possibly incurred are worth the convenience, low cost of transactions and other advantages. And if so, what types of risks are encountered to re-evaluate whether the existing mitigation strategies and plans need any alteration.

03.1 Disruption

Risks have usually been mitigated by diverse classic sectors such as banking given its sensitive core activities and data-rich nature. This market segment is originally licensed to offer high risk financial services

and executes peer-to-peer transaction of some kind (e.g., transferring money). It has already been forced to additionally deal with new risks posed by tech-centric disruptors like fintech's that are playing in the same field. In the meanwhile, banks have noticed that risks associated with disruption also come from unexpected angles. The phenomenon is the case when the core features are summed that are created by the sharing economy participants such as Uber. Founded in a different sector, the ride-sharing provider has recently announced its entrance into financial services through launching Uber Money⁹ with which it has penetrated the area of customer banking. Based on the so-called cash-right-away idea, the new division is a stored-value balance that digitally empowers paying for the ride by choosing it as the preferred payment method subsequent to registering the destination. Using this mobile account, millions of drivers across the globe are paid forthwith right after every single ride. Banks have then been pushed again to embrace the challenge and move quickly ahead with much more sophisticated capabilities. A thorough re-assessment of their facilities (e.g., bulky, and complex ICT solutions developed in-house) has affirmed the need to increasingly act as an app savvy player. It is apparent that the functionality and the magnificence of the app surprisingly prevail the customer loyalty in most cases. To ensure resiliency is necessary for serving objectives, this digital and data-centric approach seems to be the preferable or probably even the only banking option at the moment. In addition, it mitigates the risk of being left in the cold outside by agile tech-heavy operators while reaping a vast array of benefits including enhanced customer service through chatbots and functionalities to easily freeze and unfreeze debit cards via the app (Horton, 2025; Gupta, 2025).

⁹ Visit [What is Uber Money?](#) for further information.

03.2 Sharing

On the other hand, the disruption has positively supported banks and fintech's to join forces and create a sharing economy. Together in this data ecosystem, they are capable of digitally managing demand and supply, offering distinguished peer-to-peer services, adapting to the changing technological landscape, and sharing revenue (Eriksson, 2016). To better bounce back, whatever that can go wrong should raise awareness and should be outwardly displayed on the road towards the data sharing economy. The simple rationale is to ascertain that more things start to go right and are digitally monitored to stay on track at all times. This standpoint is definitely paramount for the growing sharing practices regardless of from which direction risks may hit, how severe they are, how it is exposed to them, and what their possible impact looks like. Hence, risk areas (i.e., aspects with the potential to be highly exposed to risks), risk drivers (i.e., factors that increase the level of exposure and vulnerability, or reduce capacity), and risk rationales (i.e., a foundation that is laid for a thorough risk analysis) are described. Complemented with an example where necessary, a separate overview is given below for merely data sharing, sharing economy and digital platform to help create a certain image of those risk-centric elements. It is noted that they may be limitative, neither can they be applicable to all sorts of sharing services or products. Given the explorative nature of the research, the likelihood and the potential impact of risks are not discussed.

03.2.1 Data sharing

To re-emphasis and if applicable complement the commonly important issues described above and, in the literature, (e.g., Han et al., 2019; Byabazaire et al., 2020; Li, 2023; DSSC, 2024m), an attempt was made to use the categories of data focus areas to go for a more specific description of impactful risk drivers and associated rationales. It starts with a data market for which five drivers are identified. The first one is concerned with incomplete data catalogue. It is the core of a data marketplace and encompasses various elements including different types of data, query results, data visualizations, metadata, tools to browse the catalogue, approach to diverse sources, and support Explainable AI (XAI). The catalogue improves discoverability and usability of datasets in order to avert insufficient data shopping experience (Kiourtis et

al., 2023). The second driver pertains to free access to a data market. This option does not necessarily imply that either the data or the service offered through the concerned online marketplace is free as well for which different payment models can be deployed like subscription. Players usually hesitate due to possible obligations to remain a member in the network or to share data when there is no fee to be paid (Gieß et al., 2024). The third driver regards the level of advancements of authentication and authorization mechanisms that are in use by a data marketplace. These security processes respectively confirm the identity of a participant and give this player permission to access data. If the implementation of those mechanisms is still in their infancy, consumers and providers tend to assume an insecure data ecosystem and will disengage. The fourth driver is connected to deficient data provenance. It safeguards the integrity and reliability of data by carefully documenting its lifecycle. Deficiencies in this traceability process turn into the origin of inaccurate and illegitimate data sharing (Kiourtis et al., 2023). The fifth driver relates to data oversharing. Unnecessary amounts of data can be shared in pursuit of advancing services and products that are provided to interested consumers. This oversharing activity can, at best, lead to some red faces and may, at worst, result in data breaches or other damaging issues (Caldarulo et al., 2024).

Data space is the second risk area for which nine drivers and related rationales are recognized. The first one is concerned with the way in which a data space is positioned. It is either agnostic to serve a wider group of sectors or is customized for a certain sector such as hospitality. This strategic decision may disinterest parties to join as they need to deal with a variety of standards that are specific to the sector where they operate. The second driver pertains to the structure according to which a data space is willingly funded. During its lifecycle, the finance arrangement is private, public or hybrid and is subject to change. The resulting alteration should remain attractive for enough participants to undoubtedly join so that the concerned data space can fund itself by, for instance, facilitating modern business collaborations. Finance may impact the funding strategy during the data lifecycle of a data. The third driver relates to how participants in a data space are incentivized. Some of them are interested in money, while others may seek promotion. It is hence important to clearly reward both data providers and



data users by letting them decide the motivation that properly fits their purpose. The fourth driver is about low-quality data. Data spaces normally see this aspect as crucial as it defines how to smartly enhance offerings. Its absence strengthens the image of less valuable services (see also technical building blocks described previously) that is avoided in most cases (Gieß et al., 2024). The fifth driver relates to data sovereignty and trust (i.e., a part of the aforementioned technical building blocks) to which it is also refereed as a main pillar in the mission of DSSC for data reuse within and across industries with aid for the European economy and society (DSSC, 2024i). Participants require to exercise sovereignty over their data being shared by ensuring its reliability and authenticity. This enablement is the base to trustfully establish willingness among those actors to engage in data interactions and transactions (DSSC, 2024f; Bacco et al., 2024).

The sixth driver, also pointed out as a main pillar in the mission of DSSC, is data interoperability (DSSC, 2024i). Applying frameworks (e.g., International Data Spaces Association (IDSA¹⁰) and Gaia-X¹¹) facilitates a capability to semantically and technically understand the data to ascertain an accurate consumption in sharing environments. To prevent missteps, this interpretation needs to be traceable to additionally make compliance checks possible (DSSC, 2024f; Bacco et al., 2024; Gieß et al., 2024). The seventh driver is with respect to legal considerations. They span numerous aspects, some of which are cyber security (e.g., participants' security obligations), data privacy and protection (e.g., lawfulness of processing), and data ownership and control (e.g., confidentiality). A single failure in any of them happening in a data space severely impacts the appropriate functioning of this

ecosystem (Curry et al., 2022; Bird, 2024; Mertens & Kuster, 2024). The eighth driver is connected to ethical considerations. Like the previous risk driver, these moral guidelines are required and are closely related to personal information. Careless data handling is not only about sending data to the wrong recipient, but it is also about principles to establish whether executing a data activity is morally a right or a wrong thing to do (Curry et al., 2022; Edquist et al., 2022; Mayer-Schönberger & Cukier, 2024). The ninth driver is the sustainability perspective. Data spaces need to adopt this point of view to foster a low impact on environment by reducing the amount of CO2 emissions, minimizing waste or other impactful actions. Collecting and sharing data are crucial to enable an environmentally sustainable operation (DSSC, 2024j).

Data fabric is the third risk area for which several risk drivers and related rationales are indicated in various publications. It was noticed that they are about inadequate security especially during the data transportation (e.g., Shakoory, 2024), adherence to regulations like GDPR (e.g., TST, 2025), data integrity due to voluminous administration efforts (e.g., Abu Rumman & Al-Abbadi, 2023), skillsets because of for instance the shift from the Extract, Transform and Load (ETL) concept to the Extract, Load, and Transform (ELT) concept (e.g., Gigaom, 2025), data culture as a result of the move from ownership to sharing (e.g., Dilger, 2022), and other relevant fields (e.g., instruments for searchability and findability) all of which are addressed earlier in this publication. Therefore, they are neither described here nor included in table 4 to not duplicate what was said before.

¹⁰ See [Data Spaces Radar](#) for more information.

¹¹ Visit [GAIA X Framework](#) for further clarification.

Table 4. Data sharing risks

Risk area	Risk driver	Risk rationale
Data market	Incomplete data catalogue	Insufficient data shopping experience
	Free access	Hesitations due to obligations to either remain part of the network or share data
	Immature mechanism for authentication and authorization	Insecure digital data ecosystem
	Deficient data provenance	Inaccurate and illegitimate data sharing
	Data oversharing	Breaches of other damaging issues
Data space	Sector indifference	Disinterest to join data sharing spaces
	Continuation of the funding structure	Doubts about engaging in sharing data
	Uncertainty on incentive policy	Demotivation of participants to be part of the network
	Poor data quality	Avoidance of less valuable services
	Data non-sovereignty and mistrust	Unwillingness to participate in data interactions and transactions
	Incapability to interoperate data	Misinterpretation of data consumption
	Legal roadblocks	Malfunctioning of the ecosystem
	Ethical considerations	Disappointments in moral principles
	Sustainability perspective	Negative environmental impact

03.2.2 Sharing economy

Business model is the risk area for which fifteen drivers and corresponding rationales are identified which are listed in table 5. The first driver pertains to businesses that are established to differentiate and become highly rewarding by scalability and strong network effects generated between consumers and providers. These sharing economy models are usually not involved in delivering the service themselves as they just do the matching and enable the resulting transaction. In general, it is hard for this type of business models to monetize such benefits because of their intangible nature, while it is quite easy for the networked participants to just switch to another business model that offers the same service. The second driver is concerned with the level of control over how qualitative the service is provided to consumers. Not being part of this physical delivery builds a competitive advantage over incumbents and

presents new challenges at the same time. Independent supply-side contributors to the business model can show different levels of qualifications that at last determine the customer's experience and satisfaction. This inconsistent quality issue simultaneously leaves the business model with less control and triggers consumers to engage with an identical business model. The third driver relates to fresh entrants that utterly challenge sharing business models that are already active on the market. Leveraging on the same characteristics (e.g., scalability and network effects), those new participants also strive to gain the overcapacity available to defeat others. It is no longer the case that these businesses solely attempt to establish superiority over the traditional business models. They compete with each other as well. The fourth driver is linked to the low frequency of

transactions. A business model may struggle to operate because instances of sharing irregularly take place. Costs are incurred prior to generating revenue from recurring transactions. The fifth driver is about the high cost of developing both sides of the market where it is insufficiently accustomed to the basics of the sharing economy. Business models need to argue about the sharing service or product and invest in creating a critical mass at the demand and at the supply side. The sixth driver is with respect to changes in the legal environment. Space sharing sites like Airbnb are quickly professionalizing, so is the way in which they are formally confronted with the regulatory and taxation system (Täuscher, & Kietzmann, 2017). An example is a legislation in San Francisco that restricts short-stay rentals and demands registration with the city to pay a hotel tax (Superhog, 2024). Legal battles of major sharing economy players show what dependency on the changing legal landscape truly means and how it treats them in practice (Täuscher, & Kietzmann, 2017; Lim, 2020b; Scott & Munichello, 2024).

The seventh driver is associated with fake bookings. These fraudulent activities can appear in different forms and are carried out in an effort not to use or pay. They target unsuspecting participants and seek to acquire marketing rewards, attempt phishing, or engage in other improper exertions (Reid, 2024; Booking, 2025; Houst, 2025). The eighth driver is connected to having need of government oversight. Business models can then act in non-conformity with regulations enforced previously. For instance, several cities reported that Airbnb was uncooperative to transparently communicate whether the correct local taxes were paid. The ninth driver pertains to withdraw from the primary short-term sharing principle. Business models such as Airbnb have created the possibility to temporarily rent out an underutilized room or rent out a house when its owner is away. Instead, hosts buy properties to merely benefit from as long-term rental units (Scott & Munichello, 2024). The tenth driver is concerned with the availability of proper insurance policies. They are traditionally designed for either commercial or personal products while the sharing economy requires both. In case of home-sharing rental, the property can be vandalized by consumers, and they can fall or be injured if it is poorly maintained (Maynard, 2018; WOCI, 2024). The eleventh driver regards the inequality of wealth since rents are generated by means of properties. Their owners get better returns while those owning other assets or without a property

do not gain from the sharing economy. Related business models such as Airbnb may not own the property itself, but the rent is still collected by rentiers that make their income and accordingly accumulate wealth. The twelfth driver is linked to the way in which gig workers are treated by sharing economy platforms, e.g., Uber. They are portrayed as tech giants like Google to which they are also compared in terms of social impact and responsibilities. In contrast with the latter, business models have contributed to the existence of a class of laborers that are considered flexible contractors without job security driven by the inherent uncertain nature of the market demand. This group is not part of the workforce employed by the platform and may as such not fully enjoy legal and optional employee benefits including base salary and health insurance. As a result, sharing economy is dismissed as share-the-scrap-economy although these benefits are arranged to some extent by the platform if the pre-defined conditions are met (Ganapatia & Reddick, 2018; Uber, 2025). The thirteenth driver is about the purported long-term impact on sustainability as the data is not always freely available to independent researchers. Even though some studies reveal that car-sharing has contributed to decarbonization, i.e., reducing greenhouse gas emissions, and resource efficiency, i.e., vehicle usage, it is still critiqued that these environmental benefits could be first round effects. It is argued that cheaper access potentially leads to more consumption which in turn increases the carbon footprint.

This negative growth has resulted from online transactions and physical transportation, all of which could limit the net environmental impact. The fourteenth driver is with respect to manipulated reviews and ratings. Platforms and consumers can fake this valuable input due to the known feature of two-way feedback systems. The customer can refrain from posting critical comments due to fear of retaliation and may face deceiving feedback already posted by the provider (Ganapatia & Reddick, 2018). The fifteenth and last driver are associated with sharewashing. This communication strategy attempts to exploit a new market by deceptively labeling a business model as sharing without delivering a real sharing service. Talking the talk without walking the walk of the sharing economy negatively effects the consumers' intention to use the service, impacts competitive structures in sectors, and influences society as a whole (Kumar et al., 2017; Lehr et al., 2021; Mattsson, 2024).

Table 5. **Sharing economy risks**

Risk area	Risk driver	Risk rationale
Business model	Low customer lock-in	Intangible benefits
	Less control over service quality	Inconsistent level of qualifications
	High competition for idle resources	New entrants' access to supply-side players
	Irregular transactions	Cost occurrence before recurring revenue
	High cost of developing two sides of the market	Creation of a critical mass at the demand and supply side
	Dependency on the changing legal environment	Maturing sharing services and their regulatory treatment
	Fraudulent reservations	Zero intent to use or pay
	Lack of government oversight	Prevalent nonadherence to legislation
	Withdrawal from sharing principles	Rise of full-time businesses
	Unfitting insurance policy	Coverage of physical damage and human safety
	Inequality of wealth	Rentier capitalism
	Precariat labor class	Platform capitalism
	Speculative sustainability impact	Limited net environmental benefits
	Manipulated reviews and ratings	Flawed feedback loops
	Sharewashing	Negative impact on service usage intention and industries

03.2.3 Digital platforms

Similar to data fabric, a variety of digital-oriented (see enabler technologies discussed above) risk drivers and associated rationales are identified in an array of writings due to the obvious technical nature of platforms (e.g., Alwan & Ku-Mahamud, 2020; Zhao et al., 2021; Henke, 2023). Publications concern the growing complexity of distributed architectural arrangements mostly driven by the scale of innovation and the best-of-breed philosophy (e.g., De Reuver et al., 2018 and Chaudhry, 2022), faulty technology procurement process chiefly given the make-or-buy decision (e.g., Bird, 2024), application of imperfect technology for discovery, processing or other data purposes (e.g., Gieß et al., 2024), low range of protection by insurance policies mostly due to their non-compulsory nature (e.g., Chubb, 2017), increasing attack surface as a result of growing connected devices (e.g., WEF, 2024), tightening regulations¹²

such as Digital Operational Resilience Act (DORA) for financial institutions underscoring the need for a stringent oversight of technology risks as well as control over critical data (e.g., AFM, 2025), and more that are already described above. Considering the context of the research, other risk drivers and associated rationales are recognized four of which are mentioned in turn and are presented in table 6. The first one pertains to the social media presence. It is a competitive advantage landscape where businesses digitally need to be in order to reach the online market and transact with the customer, so it remains relevant through cost-effective marketing. At the same time, they may be confronted with alterations in algorithms or other technology modifications that abruptly affect their digital visibility and engagements (SBC, 2023).

¹² See also [NIS2 Directive](#) for more information about Network and Information Systems (NIS) Directive 2022/2555 known as NIS2.

The second driver regards the AI reward profile. It is increasingly embedded in business operations to enhance customer experience, improve decision-making or enjoy other gains. Although AI tools have the potential to be a substantial addition to cyber security measures, among other issues (e.g., lack of standardization of data sourcing), they can themselves serve as a target to be compromised by a data poisoning attack or turn into a launch pad for further attack intended to degrade their integrity and efficacy (Gupta, 2023; Parry, 2025). The third driver is linked with the heavy involvement of third parties. Among other services, it relies increasingly on these players

for data hosting and administration. This dependency brings businesses with multiple points of failure that have a cascading impact on their supply chain (Parry, 2025). The fourth driver is related to biases and unfairness hidden in data. In favor of certain groups or individuals, or against a specific group or individuals, they can occur in different forms including algorithm bias or a simple selection bias and perpetuate unfairness. It has the potential to deliver skewed outputs such as misleading or even inaccurate insights (Donald et al., 2023; Mayer-Schönberger & Cukier, 2024).

Table 6. Digital platform risks

Risk area	Risk driver	Risk rationale
Digital platform	Social media presence	Unexpected effect on digital visibility and engagement
	AI reward profile	Data-integrity attacks or a pad to launch them
	Heavy involvement of third parties	Cascading impact on points of failure
	Hidden biases and unfairness in datasets	Misleading or inexact insights

03.3 Compounding risks

The risk features of the data sharing economy, the majority of which are described above, resemble the idea behind the so-called compounding risks. These events can occur in case two or more risks interact whereby their collective impact may potentially be greater than the sum of the parts (Calcutt & Ranger, 2020). As shown in figure 6, they are categorized into three distinct groups: a) connected risk, b) cumulative risk, and c) novel risk. The first group reflects a threat to a business from diverse sources that are originally not seen as interrelated. A classic example is the decline in both the regional manufacturing capacity and the global container-shipping capacity during the COVID-19 pandemic that only few expected to be initiated by the same event (Charan et al., 2024). The growth of data breaches during the pandemic (50% more attacks per week in 2021 compared to 2020) was

attributed to the rapid rise of the necessity to work from home. The pandemic forced businesses worldwide to quickly close their offices and migrate overnight to a remote workforce. Extending the work outside the office also extended network perimeters that caused widespread vulnerabilities like attack vectors for threat actors because of moving offsite business data to cloud (Zerlang, 2022). Such interconnected incident is applicable to the data sharing economy as well (e.g., in a data space). In this less-controlled data-centric ecosystem, among other handlings, remote working with privately owned devices, connecting to an insecure public Wireless Fidelity (Wi-Fi) network, downloading different apps, and uploading and sharing files (e.g., through Google Drive¹³) are common daily activities (Ilbiz & Kaunert, 2023; DTC, 2025). So are the sheer volume of attacks

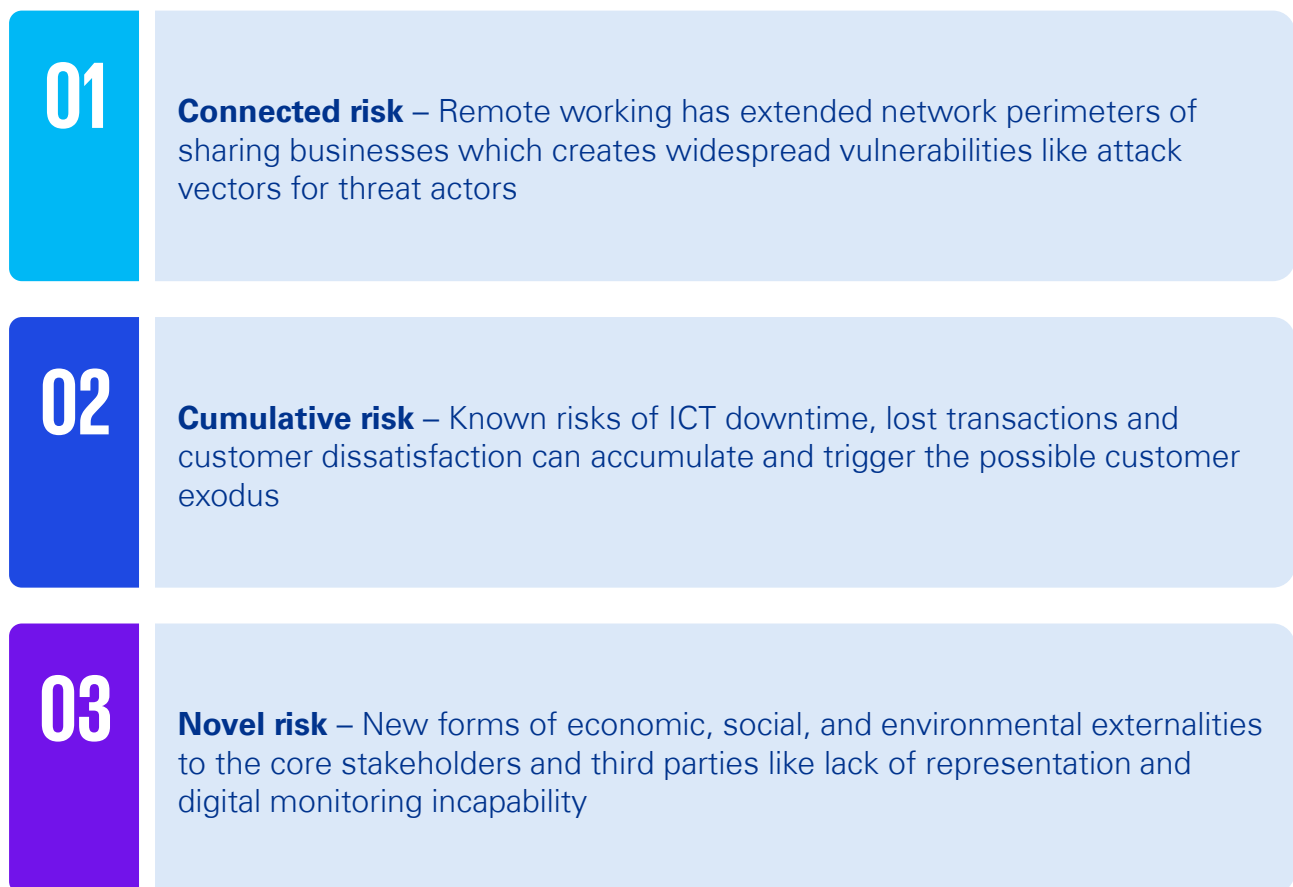
¹³ Visit <https://workspace.google.com/products/drive/> for further information.

(e.g., ransomware attacks¹⁴) and other cyber threats. These threats have become a routine part of operating in digital native environments, regardless of the size of an organization's online presence. (Cyberint, 2024).

Cumulative risk, the second group, is about one or more identified risks that accumulate from multiple sources over time and activate a single major shock. For instance, individual risks of exposure to air pollution, mindless eating, or lack of exercise are known, however, they can interact, compound each other, and adversely affect a person's health. The same can obviously happen in the highly interconnected world of the data sharing economy in which many actors play their part. An ample illustration is when an ICT outage repeatedly occurs in this digital ecosystem that is fixed every time. Risks of downtime, lost transactions, and customer dissatisfaction are known and are as such separately monitored. But they all have an effect, can build up on each other and

consequently initiate possible customer exodus (Charan et al., 2024). The third group, novel risk, is concerned with several recognized risks that are combined to form an unanticipated new risk. A familiar case is the shortage of microchips across the globe triggered by the high demand during the pandemic that induced supply chain problems compelling many manufacturers to shut down their production (Charan et al., 2024). To the core stakeholders (i.e., service providers and customer) and third parties (i.e., incumbents, communities, and governments), data sharing economy has digitally introduced new forms of economic, social, and environmental externalities. Examples include and are not limited to lack of representation and poor service recovery and compensation for the core stakeholders, and disruption of incumbents' business, increase of residents' economic pressure in communities, and digital monitoring incapability of governments for third parties (Mosaad et al., 2023).

Figure 6. Examples of compounding risks



¹⁴ The number of ransomware attacks increased in Q2 2024 to 1,277 cases which is nearly 21.5% increase compared to Q1 2024 (Cyberint, 2024).

03.4 Implications

There are a plenty of publications with respect to options and solutions to mitigate risks of data sharing (e.g., Yates et al., 2022; Carson, 2024), sharing economy (e.g., Hong et al., 2019; GBTA, 2022), and their unique features including digital platform (e.g., Elmore, 2022; Dabija et al., 2023). Numerous contributions are available about a specific domain (e.g., information security: see Xiao, 2021 or insurance: see Walsh & Evans, 2018) in addition to many other generic work regarding risk management with a standard like the International Organization for Standardization (ISO) 31000 or a framework such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) (e.g., Olechowski et al., 2016 and Everson et al., 2017). Despite the insights provided by the aforesaid material, it was carried on with identifying extra writings around risk mitigation for modern economic conditions to better cohesively deal with challenging dynamics of the data sharing economy. The argumentation was that its fast evolution has involved a broader group of stakeholders and third parties, has helped to stabilize employment, and has provided support to develop the economy, just to mention few examples of the made positive impacts (Hira & Reilly, 2017; Liao, 2024). Moreover, its rapid evolution has allowed sharing businesses to principally meet a diverse and complex high-tech risk landscape that calls for a freshly different comprehensive view. It should, among other values, harmoniously oversee the interplay between various types of impactful risks coming from different angles and wisely balance the benefits versus risks. This line

of thinking presents the real picture and encourages you to at least go beyond a static restricted approach which may overlook emerging risks, or an isolated method for a certain important discipline that manually examines the reality of risks (Carson, 2024). Associated mitigation practices then expectedly improve, so does the understandability of the way in which it should strategically be navigated and operated in the data sharing economy. After all, the greatest risks are those that we never see coming as they may have not been experienced yet, wrongly interpret their frequency and severity due to a lax attitude towards risk, or even do not believe that they would ever occur driven by the naivety, most of which can result in serious losses (Lim, 2020a). These and many other lessons are timeless and thus precious to learn from in favor of improving the performance as well as the value of any economic or social practice. AI can help detect compounding risks early through pattern recognition in data streams. This calls for assurance methods that are not only reactive but also predictive.

Today, there is an increasing demand for a more agile approach to risk mitigation, one that is clearly aligned with organizational ambitions, goals, and priorities, while also allowing for rapid response to uncertain market conditions (Mektrakarn, 2025). At this level, the focus is on identifying new, unconventional, or underexplored opportunities. An overview, along with brief descriptions of these opportunities, is presented in figure 7.

Figure 7. Areas of risk mitigation implications



¹⁵ See <https://www.iso.org/standard/65694.html> for further information.

¹⁶ Visit <https://www.coso.org/guidance-erm> for an explanation.

03.4.1 Risk-first mindset

It is recognized that taking risks without a clear standpoint on how to be compensated for them will result in poor performance or probably lead to them becoming insolvent. Adoption of a risk-first mindset is hence considered a business imperative with several amenities, with several amenities - two of which are outlined below. The first one pertains to concentrating on market possibilities that are delineated in the strategic plans while reducing the impact of any risk that may be posed. It is accordingly enabled to react rapidly and convincingly to any upcoming or unexpected opportunity or threat when needed (e.g., acquiring a struggling rival or excluding a non-compliant partner). The second amenity is concerned with incorporating risk in management control (Sheehan, 2010). This system is vital as goals can differ in sectors and communities, and the trade-offs between stakeholders may differently be managed given their history, role, and power (Adib & Zhang, 2019; Simon, 2022). It is a logical consequence that helps to obtain a higher stock price if it can be demonstrated to financial analysts that risks are properly understood and effectively mitigated (Sheehan, 2010). The risk-first mindset supports sharing businesses to proactively identify risks in an integrated fashion, put and prioritize them in the right short-term and long-term context, operationalize specific countermeasures that complement bare minimum, foster the culture of preparedness, and more (Mektrakarn, 2025).

03.4.2 Digitalization

A misalignment is still found between the pace of digitalization in the business space and the speed of deploying digitalization to the risk function even in the highly regulated sectors such as banking (Harreis & Rowshankish, 2017). This technical debt is usually attributed to two main aspects. The first one is about the shortage of the right talent to do the job. It has turned out to be a hard task for several reasons that include, and not limited to, aging workforce i.e., knowledge and know-how gained by pensioners disappear faster than they can be replaced, and skill gap, i.e., difficulty to recruit workers with expertise in AI or other emerging technologies (Soller, 2023; Thykatt, 2025). The second aspect is concerned with the tendency to remain unchanged. This inertia creates an adverse attitude towards tech-based applications in a digital era where the only constant factor is change. By bringing automation, cognitive solutions and other technologies at scale, a system of customized and sector-centric facilities can be constructed. These modern capabilities possess the potential to newly

support in addressing the monolithic structures that still exist in the risk function. They are modularly set up and integrated for which interoperability is enabled by means of data pooling or data sharing. This approach contributes to recognizing and mitigating the evolving risk landscape and helps sharing businesses to easier maintain their competitive edge and ensure their long-term viability (Soller, 2023; Chatterton, 2025).

03.4.3 Data management

Similar to almost any other discipline, data management is also intersecting with risk mitigation although these two fields were once separate. Data is hence turning into a common ground for nearly every part of the risk function, examples of which are mitigation strategy and risk assessment. The former case is nowadays increasingly applying analytics to be informed by tailored data insights to, for instance, develop financial risk hedging plan or implement robust cyber resilience measures. For the later example (i.e., risk assessment), big data and advanced analytics can be deployed to collect, process, and analyze large bulky datasets. With these sophisticated data management tools and techniques, hidden risk patterns are facily revealed, and possible threats are uncovered with ease which might go unnoticed in the past using traditional approaches. Data management and risk mitigation are strategically complementing each other as the latter discipline needs insights delivered by the former field to be effective. On the other hand, data-oriented initiatives are evaluated on the basis of their contribution to risk mitigation (William, 2023a). This coherent integration empowers sharing businesses to closely monitor their supply chain, readily predict possible disruptions, and specifically optimize inventory levels which in the end help lower operational costs, improve customer satisfaction and more (William, 2023b). It is accordingly possible to foresee and navigate risks as well as exploit any opportunity that is spotted (William, 2023a).

03.4.4 Forward-looking

Largely attached to the above-mentioned is the adoption of the so-called forward-looking approach. Unlike the traditional risk management methods (e.g., ISO 31000) deployed to support in achieving objectives, this way of working helps to address upcoming risks, anticipate the adverse scenario's, prepare for these possible events, deal with their impacts, absorb them and adapt to changing circumstances whenever needed. It is a suitable instrument that allows the board to confidently fulfill the oversight role and easily facilitates the

management team to go through the risks faced and incorporate the outcome in a plan to tackle them (Pillai, 2022). PESTLE, the acronym for Political (e.g., tax policy and trade restrictions), Economic (e.g., credit availability and wage rates), Sociological (e.g., cultural norms and population growth), Technological (e.g., Robotic Process Automations (RPA) and AI), Legal (e.g., employment legislation and taxation) and Environmental (e.g., sustainable resources and ethical sourcing) is an illustration of such approach. This future-centric analysis examines these six key external factors that affect businesses, leads in the strategic decision-making process, and directs to simultaneously mitigate risks and maximize opportunities. Among other advantages, it encourages a broader understanding of specific dynamics of the market segment, presents cost saving potentials and signals further investigation to enrich insights (Hayden, 2025). Sharing businesses can benefit from forward-looking risk mitigation to build and maintain resilience in both good and hard times (Pillai, 2022; Natale et al., 2022).

03.4.5 Risk-based compliance

Another aspect intricately linked with the aforementioned is risk-based compliance. Adding the principles of risk assessment is a modern approach to improve efficiency and the effectiveness of the compliance function. ARCHER, 2020). It is simply about not ticking boxes to meet every single requirement, but a profound assessment is conducted to pinpoint the most critical compliance risks. This thorough analysis takes the business operations as the starting point, including regulations, industry standards, commitments, and other obligations, and follows three main steps. The first one, risk prioritization, pertains to assigning preferences to risks with high likelihood of occurring and their potential severity. Targeted controls, the second step, is concerned with designing and operationalizing controls that are targeted to mitigate the prioritized non-compliance risks. The third step, continuous monitoring, relates to implementing an ongoing process to keep an eye on the operating effectiveness of mitigation controls and keeping track of the ever-changing regulations (CSS, 2025). Sharing businesses act in parallel with the incumbent way of doing business which implies that they are also confronted with a different risk landscape. Among others, it emphasizes the new-found power of the customer that must be met to remain in business. This phenomenon shows that they are in the driver seat and combine the digital requirements, e.g.,

connectivity via an app, with the traditional demands, e.g., the lowest price available (STRI, 2018). A risk-based approach is helpful to place focus on the most impactful non-compliance areas, allocate resources accordingly, and deal with them to ensure adaptability to circumstances (CSS, 2025).

03.4.6 Governance

Risk and governance are two classic business topics that are nowadays viewed from a transformative point of view. Both are expected to move away from a static way of working to keep pace with the evolving world of risk occurring in the current digital-driven era. It has rapidly arisen with a modern face that is generally shaped by the technological transformation to which new openings and tradeoffs are also attached. Holding a grip on risks and opportunities accompanied by these changes is where revamped governance is valued. It is argued that the slow pace of development of governance structures is no match to the fast pace of the technological and social evolution. Reasons for concern are mostly growing with respect to whether the existing governance structures in use are sufficient to deal with the risks of the current age like those that are associated with AI and climate change. In addition, there are questions about whether those directive mechanisms are still suited to handle tradeoffs between different and to some extent sometimes even conflicting needs and interests of these days. Operationalization of a solution based on enabler technologies to serve a certain purpose versus the possibility to overlook the related downsides in a business chain can have more severe consequences compared to the same situation in the computerization era in which IT was just a supportive function (IRGC, 2019). A good illustration is when top risks are identified after which a risk map at a high business level is often followed. Next, it is necessary to also take into account in which way minor individual risks with high frequency (e.g., a tech-based interruption) in a partner ecosystem may converge and cause a compounding risk. It allows the board to quickly act upon such adverse event before it reaches a recurring friction point that displeases customers and potentially offers them no option but to leave (Charan et al., 2024). Such manner of governing risks facilitates sharing businesses to strengthen their competitiveness predominantly due to the inherent interconnectedness and the dominant position of digital platforms.

03.5 Concluding principles

This chapter is dedicated to some pertinent aspects that are associated with risk mitigation. The most important principles are as follows:

- Risk analysis and mitigation are becoming increasingly complex. This ongoing change results from the multi-disciplinary nature of the data sharing economy, a diverse array of stakeholders and third parties with sometimes conflicting interests, a demanding marketplace, growing technological complexity, an evolving regulatory landscape, and other influential factors.
- Traditional, manual ERM systems often rely on known data and linear thinking, which is insufficient to prevent risks from materializing. Embracing opportunities from multiple and larger data sources requires adopting a multidimensional view on risk and conducting more comprehensive risk analyses.
- Once digitalized, data enhances cross-reference and improves the effectiveness of sharing businesses. The risk function can now leverage nontraditional data sources such as social media to act more predictively and consistently. Data is no longer an under-exploited asset, but a valuable resource actively utilized for risk management.
- Advanced technologies, particularly AI, should be robustly embraced to build risk-intelligent capabilities. These technologies add value through automated risk identification and mitigation processes, helping sharing businesses navigate complex and interconnected risks.
- The data sharing economy implicates numerous interdependent risks that tend to accumulate and interact. Understanding these risks and their consequences requires continuous effort, not just a one-time assessment.
- Activities in the data sharing economy succeed by effectively addressing challenges related to community-building and fostering trust. Strategically overcoming factors that impede group cohesiveness and discourage participation is essential for business success.
- In a digital world where even a small mistake can cost a business its online presence and reputation, cybersecurity and privacy risk management have rightfully taken a dominant place on board's agendas. Managing these risks demands a digital mindset, aligned capabilities, and organizational transformation.
- Mitigating risks properly is everyone's responsibility. Effective risk management supports both desired performance and resilience against adverse events, with technology and advanced analytics playing a crucial role in faster interventions and better impact reduction.
- The board must transform its approach to controlling business risks by fostering continuous dialogue with management, designing effective relationships for risk oversight, and consistently allocating appropriate resources to risk systems.

Takeaway

No risk, no glory, but share with care.

It is evident that data sharing economy confronts a wave of multi-disciplinary risks that can facilely discredit its performance and effectiveness. Risk-taking and risk mitigation should remain top of mind for the C-level, legislators, investors, and the media. As maturing economic players, sharing businesses need to exercise care to also tackle risks that may harm their public relations and reputations. By using advanced technologies to enhance risk identification, analysis, and mitigation, sharing activities can be proactively guided away from high-risk areas toward safer practices, allowing participants to operate with greater confidence and continue benefiting from both business and social outcomes.

04 Assurance

The rapid growth of the outsourcing industry¹⁷ in the late 1990s, along with the introduction of the Sarbanes-Oxley (SOX) Act¹⁸ in 2002, jointly acted as key drivers for assurance reporting in the context of Information Technology (IT) products and services (Shahim, 2009). During this period, businesses began concentrating on core activities (e.g., specialized product design or high-precision manufacturing) that directly contributed to their competitive position. In contrast, non-core functions (e.g., electronic transaction processing and IT infrastructure management) were increasingly seen as support activities suitable for outsourcing, nearshoring, or offshoring. A pivotal case in this development was Kodak Corporation's decision in 1989 to outsource its IT operations – including data center services – to IBM, DEC, and Business Land, widely viewed as the starting point of the IT outsourcing industry (Hirschheim et al., 2020; AMEG, 2025). This shift contributed to the commoditization of IT services, where "make or buy" decisions became increasingly driven by cost-efficiency rather than strategic value.

However, as IT functions were delegated to third parties, concerns arose regarding how to remain in control of these outsourced services. Organizations still depended on trustworthy and reliable IT systems to support internal controls and deliver accurate business information (Giustiniano & Clarioni, 2013). The SOX Act heightened these concerns by mandating that organizations maintain robust internal processes and verifiable control mechanisms, especially where financial reporting was involved. This need for accountability gave rise to independent Third-Party Audits (TPA), at the time reported under Statement on Auditing Standards No. 70 (SAS 70) (Shahim, 2009; Sherinsky, 2010). A growing lack of confidence in the integrity and availability of outsourced IT systems raised red flags for C-level executives, investors, and regulators. In response, external auditors were engaged to provide assurance over the internal controls of service providers. This was not only a compliance exercise but also a means of restoring trust.

Over time, growing doubts about the integrity of outsourced information processing and the availability of IT systems began to erode the confidence of executives, investors, and regulators. The need for independent verification of service provider controls has become clear. External auditors were engaged to address these concerns and help rebuild trust in the delivery and management of outsourced services.

This development directly connects to the Trust principles described in Chapter 2.6 (Mayer et al., 1995). Assurance practices touch on the three foundational elements of trust: ability, benevolence, and integrity. Audits and certifications provide evidence of a provider's ability by demonstrating competence and control over critical processes. They also reflect integrity, by showing adherence to standards and agreements through verified actions. While benevolence is more challenging to measure directly, the provider's openness to audit and commitment to addressing issues signals a willingness to act in the client's best interest. In this way, assurance reporting contributes meaningfully to building trust—both in the service provider and in the broader service delivery model.

As assurance needs evolved, they came to cover a wide range of subject matters, which typically fall into three broad areas. These include the accuracy and completeness of data being processed, the effectiveness of the internal processes and controls supporting the achievement of objectives, and the reliability of formal reports or statements issued by the service provider. Together, these assurance areas support transparency, accountability, and trustworthiness in complex IT service arrangements.

¹⁷ Tax collection is an early instance of outsourcing that can be traced back to the ancient Roman Empire (Hirschheim et al., 2020).

¹⁸ See <https://www.congress.gov/bills/107/congress/house-bills/3763> for more information.

04.1 Revamping

To understand how assurance needs are evolving, it is important to first revisit the foundational principles of assurance. An assurance engagement typically involves a three-party relationship: the responsible party (i.e., a service provider), the practitioner (i.e., an auditor), and the intended users (i.e., customers or regulators). The engagement focuses on a clearly defined subject matter, such as internal controls, data processes, or compliance with regulations. This subject matter is then assessed against established criteria or standards to determine whether it meets expected quality or performance levels. These principles remain relevant, but the dynamic nature of digital transformation challenges how they are applied in practice.

Taking a closer look at developments in the marketplace highlights the speed and scale of change in recent years. Healthcare providers moved rapidly to telehealth; Asian banks shifted from physical to digital channels almost overnight; and retailers transitioned swiftly to contactless shopping and delivery models. Digital customer channels have become the primary mode of engagement, while automation drives productivity across sectors. As digital technologies now underpin nearly every business interaction, organizations face increasing pressure to mature digitally at both speed and scale in order to meet evolving customer expectations.

Along this irreversible transformation, a new tech-driven business environment has emerged, one that is markedly different from traditional operating models. It is no longer sufficient to treat IT as a supporting function. Instead, organizations must position themselves as digital actors, embedded in broader technology ecosystems. IT has become integral to the business itself, shaping strategy, enabling agility, and blurring the line between physical and digital. As a result, IT-related risks are now directly tied to business risks, requiring new approaches to assurance.

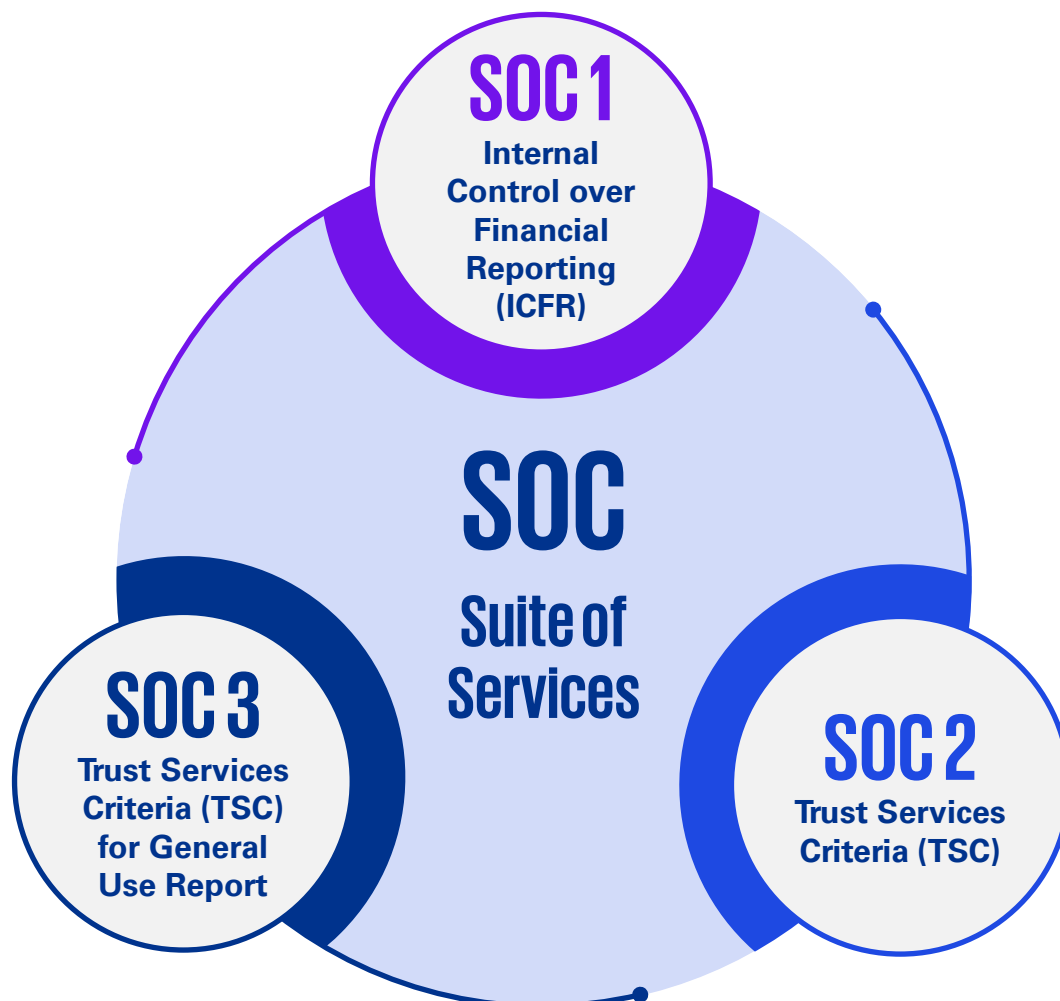
In this ever-changing marketplace where there is almost no space left for low techs to do business, it has increasingly become challenging to advocate the classic approaches to IT assurance reporting. It is commonly issued in line with System and Organization Controls (SOC) that is published by the Association of International Certified Professional Accountants (AICPA) and the Chartered Institute of Management Accountants (CIMA). As listed in figure 8, this suite of services encompasses three components: SOC 1: Internal Control over Financial Reporting (ICFR), SOC 2: Trust Services Criteria (TSC), and SOC 3: TSC for general use report. They still consider IT as a supportive function, relying on static frameworks and assuming more classic characteristics that yet insufficiently demonstrate a visible adaption to the dynamic digital world (Zweers et al, 2022).



Given the increasing dependency on IT, it is barely justifiable to suffice with merely reviewing the basics such as General IT Controls (GITCs). It is apparent that IT is no longer only about the back-office automation and is neither only about providing support to achieve targets. Instead, business models are now built upon IT, and it drives the strategy to achieve the defined objectives (Shahim, 2017). Obviously, sharing businesses are no exception to this modernization shift given their operating model (i.e., creating a virtual marketplace that digitally matches supply and demand). In this arrangement, multiple providers like CSPs are normally engaged, among other players, with which it is usual to have varied IT outsourcing configurations in place (Prinsloo & Thompson, 2015).

Moreover, assurance must evolve to address the full lifecycle of data: from collection and storage to distribution and use. In this regard, critical aspects such as data governance and data quality management are increasingly important. Ensuring that data is accurate, consistent, securely handled, and used responsibly is central not only to operational integrity but also to customer trust and regulatory compliance. Without confidence in how data is managed, any assurance provided over digital services or platforms risks becoming superficial. Hence, the assurance profession must modernize in line with the environment it seeks to support. This includes aligning more closely with the principles of trust (as introduced earlier), expanding coverage across the full data lifecycle, and adapting assurance models to account for the complex, fast-moving nature of digitally enabled business ecosystems.

Figure 8. **Components of SOC suite of services (Shahim, 2021)**



04.2 Sharing

Possible options are considered to better keep pace with a number of business factors that include the varying regulation and changing clients' expectations as well as the specific sharing characteristics and different related risk areas described previously. Stakeholders increasingly seek digital confidence through greater transparency and reliable reporting on the reality of an IT landscape that is increasingly arranged, operated, and maintained by third parties. AI solutions execute routines that were performed by humans, bots are provisioned by means of cloud services that are embedded in internal processes, and digital data is processed through sensory devices that are connected via the cloud. Together with several other technological advancements, they support in riding the wave of ubiquitous digital transformation in

which outsourcing culture is common (Hirschheim et al., 2020). Given this context, it is crucial to obtain deeper insights and understanding of the whole sharing business rather than receiving information that solely covers a narrow scope (AEAA, 2021). Note that several assurance concepts (e.g., security assurance, compliance assurance, and digital identity assurance) are discussed in different writings (see Dela Rosa Algarin & Demurjian, 2014, Van Rietschoten et al., 2022, and CoE-DSC, 2025 respectively). Along with digital platforms, focus is therefore placed here on data and technology as the fundamentals of the delineation of the data sharing economy discussed above. Table 7 presents a list of some assurance concepts that are associated with this phenomenon.

Table 7. A few assurance concepts in data sharing economy

Delineation	Assurance concept	Main drivers
Data sharing	Data assurance	Data trust
	Data quality assurance	Technological advancements
	Information assurance	Information assets and capabilities
Sharing economy	Technology assurance	• Digital transformation • Third parties • Cyber security
	IT service assurance	Critical hybrid IT services
	Software assurance	Digital apps
Digital platforms	Digital assurance	• Customer experience • Unconventional testing
	Platform assurance	High quality software

04.2.1 Data sharing

Three concepts are indicated in this section to help establish a certain image of assurance when sharing data, of which data assurance is the first one. With the growing complexity of large data infrastructures comes the urgency to build trust in data that is gathered, deployed, and exchanged. Data needs to be fit for purpose as it is increasingly expected to be more normally shared between apps and machines with little, or sometimes even no, human interventions.

Eight common aspects are identified to support this future direction and enable legitimate data sharing practices. These generic factors are: a) organizational governance and internal oversight, i.e., strategy to manage risks and accountable leadership to deliver, b) privacy, i.e., protection level implemented for the sensitive data like that of employees, c) security, i.e., keeping data secure and in conformity with standards, d) quality and accuracy, i.e., a consistent way according to which data collection, usage and

exchange take place in line with specifications, e) ethics and transparency, i.e., adherence with ethical principles and willingness to be publicly assessed, f) data access processes, i.e., embedded and resourced data sharing and usage processes, g) skills and knowledge, i.e., availability of training and learning in how to deal with data, and h) engagement and accountability, i.e., addressing the interests and issues of data stakeholders and holding to account when necessary. Their adoption is believed to improve data governance, promote trust and encourage sustainable behavior change (Baker, 2023).

The second concept is with respect to Data Quality Assurance (DQA) to which it is also referred as information quality assurance (see e.g., Zenya, 2021). In addition to several other advantages, technological advancements have re-emphasized the importance of high-quality data in particular when it comes to deploying AI and analytics. DQA is a proactive strategy that is concerned with a good discipline to prevent data errors and maintain data accuracy and completeness throughout its entire lifecycle. An average DQA consists of many elements, five of which are mentioned here to help create a certain image of essential building blocks. They are: a) data profiling and assessment, i.e., determining the current state of data in terms of inconsistencies, inaccuracies and duplication, b) advanced data cleansing techniques, i.e., capabilities to among other actions uniform data formats and eliminate duplicates, c) data standardization and harmonization, i.e., introducing standards to coherently integrate different data sources and analyze their diverse contents, d) real-time data validation, i.e., proactively highlighting data errors prior to mistakes and confusions, and e) automated data lineage and traceability, i.e., applying tools to transparently track the origin of data and the way in which it is altered. It is stated that DQA soundly uplifts the data strategy by utilizing advanced tooling (Vidya, 2024).

The third and last concept is with regard to information assurance. Current threat-filled digital environments are populated by numerous informational capabilities and information systems rightfully deployed to meet the vision and strategy which also make these assets alarmingly vulnerable. The purpose of information assurance is to protect them by means of adherence to regulations, risk management, and organizational policies. The principles related to this overarching approach are described with the use of the Maconachy-Schou-Ragsdale (MSR) model. In accordance herewith, they are formed by three chief

pillars. The first one is concerned with three stages in which information is stored, transmitted, and processed. The second pillar is linked with three crucial areas of countermeasures: technology, policy, and people. The third pillar is about five basic services: a) availability, b) integrity, c) authentication, d) confidentiality, and e) nonrepudiation. They were adopted by the internationally recognized Association for Computing Machinery (ACM) as an extension of the basic confidentiality, integrity, and availability model. The principles are designed to help satisfy common business requirements like being an enabler, determining responsibilities, and protecting interconnecting elements of systems (Schou & Hernandez, 2015).

04.2.2 Sharing economy

Similar to the abovesaid, three concepts are mentioned here with technology assurance as the first one. The fast pace of digital transformation has explicitly elevated the importance of assurance provision on technology which is connected to three main factors. It starts with the increasing adoption of technological advancements (e.g., cloud and AI) with specific associated risks that require a proactive risk assessment and a dynamic mitigation strategy. The next factor is related to involving third parties to a large extent for a variety of services that calls for SOC reporting to provide transparency and so positively impact the trust of the stakeholders. The last factor is connected to evolving cyber threats and updated cyber security frameworks that are implemented to tackle these dangers and achieve a higher level of resilience (Box et al., 2024; Johnson & Huston, 2024). The second concept pertains to IT service assurance. It has gained momentum because of different critical services that are delivered by combining on-premises and cloud-based operations. This movement has brought a new requirement to the game that pushes to keep improving service levels and also demands to guarantee superior IT services. It is achieved through obtaining detailed insights into operations, connecting them to business outcomes, and providing visibility into financials. Tooling for IT service assurance are diverse and are aligned with IT Service Management (ITSM) tooling that are applied to monitor, support, and administer every single aspect of operations. To optimize IT resources and costs, systems to use are closely related to numerous disciplines such as service desk management, configuration management, asset management, contract and license management, change management, and service catalogue management (Watts, 2023; BMC, 2025).



The third concept is about software assurance that has solidly appeared in the forefront of attention due to the indispensable role of apps to execute business functions and drive customer experience. It is an essential part of the Software Development Life Cycle (SDLC) with the goal of dealing with weaknesses and ensuring that the software is trustworthy during its lifetime (Rhodes et al., 2010). Software assurance is an overarching approach that contains practices, processes and tools to make a positive contribution to the cyber security posture and compliance efforts of businesses. This concept usually applies eight chief components to properly work: a) requirements analysis and security planning, i.e., specifying and embedding security requirements from day one, b) secure design and architecture, i.e., creating a stable ground to successfully resist cyber-attacks, c) secure coding practices, i.e., adherence to guidelines for software programming to address common vulnerabilities, d) security testing and verification, i.e., methods used to investigate any possible weakness, e) third party component management, i.e., assessing libraries or components provided by others for potential vulnerabilities, f) ongoing monitoring and updates, i.e., continually keeping an eye on security alerts to make sure that related issues are timely discovered, g) incident response planning, i.e., crafting and maintaining a detailed plan intended to structurally respond to breaches or weaknesses if detected, h) security training and awareness, i.e., generating a security-aware culture so that every member active in the SDLC plays a role in sustaining security (Sentinel, 2025).

04.2.3 Digital platforms

To find pertinent literature on assurance concepts, this term was simply broken down into two equal terms: digital and platform. The first concept, digital assurance, is particularly oriented towards digital transformation and ensures spotless performance of advanced solutions with respect to customer experience, and unconventional testing. Digital assurance is hence not only about testing apps across Social, Mobile, Analytics, Cloud (SMAC) or other modern technologies. Also, it is concerned with arrangements to make sure that intended business outcomes become a reality as a result of the launched digital transformation initiatives. With an array of processes, methodologies, practices and tools, digital assurance adapts to the dynamic digital world through: a) guarding customer experience and brand, e.g., measuring across digital channels in use such as web and smartphones, b) adopting DevOps models to meet delivery agility, e.g., closely cooperating with developers for continuous integration, c) moving from application level to life cycle automation, e.g., deploying AI across the testing life cycle, d) ensuring data quality in big data, e.g., fulfilling accuracy, completeness, security and privacy requirements, e) applying advanced analytics for decision support, e.g., providing better quality insights by predictive and prescriptive decision-making in testing (Qualizeal, 2024). The second concept, platform assurance, is mostly identical to software assurance when it comes to ensuring high-quality software aimed at meeting the need of the current digital landscape. By leveraging AI-enabled tools, test scripts are automated across platforms such as Pega²⁰ and Salesforce²¹, and Continuous Integration/Continuous Deployment (CI/CD) pipelines are integrated by using third party products and services (Virtusa, 2025).

²⁰ Visit [Pega](#) for further information.

²¹ See [Salesforce](#) for an introduction.

04.3 Trends

Assurance is changing and developing in areas with diverse characteristics, five of which are depicted in figure 9. They are briefly treated here with the goal of painting an overall picture of the direction towards which assurance is moving. The first area is expectedly concerned with technological advancements such as big data analytics (e.g., accessing and analyzing larger and various datasets with less restrictions), AI (e.g., applying predictive models to find discrepancies and patterns) and process automation (e.g., conducting conformance checks and generating reports). As expounded above, they help to detect anomalies and errors that occurred in the past, and support in obtaining actionable insights regarding disciplines with potential for improvement. A contribution is accordingly made to efficiency and accuracy of assurance provision. The second area relates to an appropriate balance between technological deployments and human skills. In most cases, it cannot only be sufficed with tailored technology learning options. In addition, the output of an algorithm, for example, still needs to be combined with a review by the subject matter expert to interpret this result in the right context and make decisions (Gemilang et al, 2024). The third area is with respect to cyber security. The ever-increasing pressure from the

stakeholders has prioritized assurance provision with regard to this crucial topic. The need is centered around examining the effectiveness of controls that are in place to safeguard digital assets (e.g., data, devices, and networks). The fourth area is linked with continuous monitoring and auditing. They are no newcomers and have yet solidly remained relevant in the assurance landscape especially due to fast-paced digitalization. The complexity of this challenging world along with its data-intensive nature have led to the demand for continual risk assessments, monitoring and auditing capabilities aimed at increasing confidence in coverage and associated results (Gartner, 2024b). The fifth and last areas pertain to integrated assurance. Among other issues, too much information with insufficient insights because of large numbers of issued assurance reports with less equivalent focus on risks, and serving a wide range of audiences (e.g., board and audit committee members) have given rise to the growing desire for a new assurance concept. It is a holistic and integrated approach that starts and ends with understanding the drivers that deliver business value as there are usually different manners according to which these risks are mitigated, and assurance is provided about them (Patel et al., 2018).

Figure 9. A few trends in assurance



04.4 Implications

A direct association was barely made in the literature between the risks posed to the data sharing economy and the way in which assurance is provided on them. The analysis is threefold. First, given the related multifaceted and high-impact risks (e.g., data sovereignty concerns in data spaces) along with their dynamic nature, it would be hard to simply indicate relationships between every single one of them and common assurance products in use. Nevertheless, in comparison with the SOC suite of services, a standard like International Standard on Assurance Engagements (ISAE) 3000²² offers more flexibility to deal with the issue (Koorn & Zwinkels, 2021). Second, assurance is differently positioned by parties outside the audit profession, some examples of which are discussed above. Also, this concept is defined by players active in sharing initiatives like DSSC²³ that are normally in line with and in favor of their own core activities. Third, although stakeholders and third parties generally find it hard to concretely define assurance needs, they keep demanding more transparency that is necessary for a solid working of sharing businesses. Their increasing expectation is that auditors are totally equipped to provide the required information by delivering assurance services other than Financial Statement Audit (FSA) that are conducted each year (AEAA, 2021). Emphasis is ideally placed on a periodic assurance provision through near real-time channels that is facilitated by the ever-evolving advancements in data and technology including those expounded above. Taking the powerful combination of these two enablers into account, it is justifiable in the current modern digital era to seek alternatives that can responsibly be deployed to go beyond the information that is solely subject to the FSA cycle. The intention is to be able to rely on a mechanism that better supports frequently obtaining assurance on broader kinds of information published by sharing businesses. It would accordingly be easier to shed light on the reality of their inner functioning (ICAEW, 2014).

04.4.1 Assurance over KPIs

Discussed by analysts, investors, executives and others, Key Performance Indicators (KPIs²⁴) are perceived as an alternative to measurably contribute to resolving the aforementioned issues. These

quantifiable metrics are internally utilized for decision-making and are also used for external communication about the progress made towards a set of objectives, targets, and the corresponding outcomes. This regular way of reporting is in the main not part of formal assurance engagements and can therefore benefit from this independent examination at various times and on various types of information. Real-time assurance on KPIs requires a shift from annual audits to continuous monitoring. This implies close collaboration between audit, data science, and IT to make assurance dynamic and contextual. The resulting assurance provision paves the road for a more user-centric model that better keeps up with the market expectations and so possibly comes closer to bridging the gap between what is desired versus what audit delivers. Careful consideration of this misalignment regarding sharing businesses is certainly required because they can deal with divergent stakeholders with varied assurance needs, some of which are fully satisfied by the yearly audit cycle while some may not. It is notably true for non-financial information (e.g., sustainability information) generally housed in systems that are less mature compared to those in scope of the FSA. In such cases, the assurance provider needs to also take three essential factors into account whether 1) the methodology applied to prepare KPIs is suitable to give a solid measure to the concerned elements of performance, 2) the calculation executed for these critical indicators are correct, and 3) the data used to feed them originates from designated sources. Assurance reporting on KPIs may be provided under existing technical standards (e.g., ISAE 3000) and can potentially be valued by sharing models. Using this delivery mechanism, all participants more often receive information that helps to understand the business in addition to that presented in annual reports (ICAEW, 2014). However, it is argued that there are also downsides to the way in which assurance is provided over KPIs. A chief concern is that the desired flexibility of these measurable metrics could decrease if they are independently reviewed by auditors, although these practitioners are natural candidates to accomplish the assurance provision role. In addition to other reporting structures, KPIs are generally seen as one of the means to clearly understand the narratives of businesses (Smith & Heijden, 2017).

²² Visit [IFAC](#) for more information.

²³ DSSC explains assurance as an artefact that helps parties make trust decisions, such as certificates, commitments, contracts, warranties, etcetera (DSSC, 2024g).

²⁴ The idea is also applied to other measurable topics like risk (i.e., by Key Risk Indicators (KRIs)), compliance (i.e., through Key Compliance Indicators (KCIs)), and security (i.e., using Key Security Indicators (KSIs)).

04.4.2 Real-time assurance

Today, it is becoming increasingly common that a high level of data and technology adoption is a necessity for the profession. It is widely realized that assurance efficiency (e.g., in terms of computerizing repetitive tasks and enhancing the speed of extensive data processing) is important. Equally important is to bring more value to the table (e.g., through the ability to predict future assurance needs of clients and to provide recommendations to them when necessary) than just performing the FSA every year. Putting money and effort into building and maintaining these capabilities secures the relationship with a new generation of clients that preferably communicates with the assurance provider using technological means. Also, these investments help to recruit and retain staff that ideally only work with data and technology to be more valuable to the client (IFAC, 2018). The broadly growing application of these two indispensable assets in diverse forms has resumed the discussion around Continuous Assurance (CA) as it potentially aids to digitally transform from traditional manual techniques to modern automated methods (Barros & Marques, 2022). Since the late 1990s, the lack of sophisticated tooling and systems (e.g., a dashboarding software to collect and visualize audit results, and a workflow solution to formally generate an assurance report) was discussed as the missing piece to successfully deploy CA and continually deliver assurance information (Kocken & Hulstijn, 2017). This

concept heavily depends on the strong combination of continuous monitoring and auditing and is capable of providing real-time assurance only if the underlying technological foundation is advanced and properly laid. Given the ongoing stream of digital data, auditors can be facilitated with a comprehensive and detailed technique to reduce errors and risks and easily move towards a more effective decision-making. The arising advantage is surely made possible by automated testing of the whole population of transactions for various audit areas rather than merely examining smaller portions due to time constraints, poor or probably even manual processing (Francken et al., 2022). In practice, the full implementation of CA is however lagging behind despite its attractiveness and importance to, among other amenities, elevate the image of the profession (Barros & Marques, 2022). This technique supports in developing the scope of assurance to embrace a larger set of qualitative and quantitative reports (Vasarhelyi et al, 2018). The corresponding result is valuable to stakeholders and third parties active in a sharing ecosystem by means of which they impartially get insights into how it operates. From their perspective, CA services additionally give the opportunity to view transactions on a real-time basis, intervene in conducting these events, correcting them, and notifying those involved and responsible (Barros & Marques, 2022).



04.5 Concluding principles

From the above description, argumentation and analysis, the following useful principles can be provided:

- The data sharing economy is evidently confronted with a wave of issues that discredit its effectiveness and sustainability. The question of secure and productive collaborations between participants in sharing ecosystems and the challenge of dealing with various laws and legislations are common examples.
- In sharing, trust and compliance are not merely about a belief that all involved parties properly counter business risks and appropriately follow rules and instructions. Also, it is necessary to transparently prove the effective mitigation of these risks as well as the traceable way in which it is adhered to regulatory requirements.
- An impartial assessment conducted by external auditors is a direct path to a practical solution. The resulting assurance report is an acknowledged instrument that helps build confidence in the working of sharing businesses.
- The notion of assurance found in the literature is largely linked to concepts with respect to the implementation of good practices. Audit-related publications mostly associate the term with a thorough examination by an independent and qualified auditor that results in an opinion stated in the corresponding assurance report.
- The vast range of opportunities introduced by the potent combination of technological tools with voluminous datasets have significantly shifted the focus from conventional to technology-based auditing. They are jointly transforming the way in which audits on digital-born sharing models are preferably conducted.
- Traditional assurance on an array of multi-dimensional sharing risks is seen to become ineffective. The expectation is to consider provision alternatives that is in particular shaped by the acceleration of digital adoption by businesses and individuals. This increasing need calls for detailed and near-instant insights based on the broad variety of information that is made accessible by different sources than financial systems alone.
- Given a data-driven ground leveraging on a tech-savvy foundation, existing concepts such as KPI and continuous assurance offer an option for assurance

provision. The aim is to build a mechanism that matures over time, turns into a more dynamic approach, and continuously delivers data ingredients necessary to generate trust.

- Compared with the current setup, sharing participants now rely on a demand-driven provision mechanism that better aligns with their diverse assurance needs. This mechanism continuously draws from a broader range of information types, helping to create a comprehensive view, reveal ecosystem interconnections, highlight dependencies, and provide deeper insights into operational health. As a result, participants can access independent assurance information whenever it is needed, making them more confident and motivated to act decisively.
- In this context, the ability to map critical supply chain dependencies, across both digital platforms (e.g., cloud providers, marketplaces) and data flows, including AI-driven processes, has become a major priority. These dependencies, if not properly understood and monitored, can represent significant operational and compliance risks. Explicit visibility into these layers is therefore essential for reliable assurance, especially as businesses increasingly rely on external providers and automated systems for core processes.

Takeaway

Assure for sure, but no capability, no cure.

Sharing businesses struggle to concretely feed the assurance appetite and yet their demand to constantly receive independent assurance information is getting higher. This growth goes hand in hand with the rise of digital technologies and massive data streams connected to KPIs and real-time assurance to support in obtaining detailed impartial insights. They are underutilized by auditors to help sharing models meet the assurance need and enhance the effectiveness of their own examination. Deploying digital capabilities styles assurance reporting to increase client satisfaction and comply with the profession standards at the same time.

05 Discussion

Technology has introduced transformational advancements that have made it possible to instantly process and exchange bulky amounts of data. Their worldwide application has brought remarkable opportunities to which neither businesses nor individuals could stay blind. In contrast with the traditional economy often operating on a B2C basis and centered around the ownership of items, formal and informal relationships have existed that cohesively cooperate to access idle resources through the common principles of sharing. Although it is not entirely a new concept, a technological newness has been born that is gladly leveraged by the data sharing economy to create decentralized marketplaces, and flexibly empowers massive peer-to-peer networking and extensive collaborative consumption of goods and services around the world. It is evident that digital platforms are the recognized face of the emerging phenomenon that are fundamentally enabled by two main components: internet and key enabler technologies. They are truly inseparable as the former provides the basic functionality to go online and accordingly lays the ground to create the latter. It craftly assembles and runs digital advancements that allow networks of participants to connect, view, search, find, interact, and transact among themselves to efficiently share what is publicly offered or requested. It can be stated that the farthestmost role of technology is undisputable in the data sharing economy which has led to a scalable uniqueness with regard to the way in which demand and supply is managed online. Each party, for instance, acts as either a provider of a resource or a consumer of it stimulating a sense of community and collaboration that ultimately lets a distinguishing factor shine on the stage: technology. It keeps developing and hence supporting the data sharing economy to further mature which has also a downside like many other chief enablers. Surely, it is not without concerns, issues, incidents, hazards, and challenges of diverse nature for parties to globally engage. They obviously demand effective safeguards to counter all of these risks which additionally need to be proved.

05.1 Conclusion

Since its conception, data sharing economy has been confronted with a great deal of multidisciplinary risk drivers. They encapsulate a complex interplay of digital marketplace mechanisms, complicated peer-to-peer instruments, dynamics of large number of actors, constraints of data security solutions, diverse technology governance structures, unfamiliarity with local laws and regulations, numerous user-generated contents, error-prone heterogeneous ICT environments, and much more. Although every related risk in itself has the potential to become adversely impactful, it can also merge with one another whose collective consequence might be more severe compared to the situation in which they individually occur. These compound risks need to be thoroughly understood and mitigated to be able to appropriately respond to resulting uncertainties in sharing ecosystems. Given the above-said implications, an automated and continual risk assessment is inevitable to ensure a systematic and more effective approach. In

this manner, it dynamically enhances the overall resilience of sharing businesses and supports them to proactively mitigate risks rather than just cleaning up after they happened. Although it is in general still the case, managing the diverse risk landscape of sharing certainly requires more than manual procedural exercises with a combination of different static frameworks, guidelines, and standards to be simply effective.

A similar line of reasoning is applicable to assurance as well. For the information delivery associated herewith, emphasis is placed on three particular characteristics: broad, real-time, and continuous. In the sharing context, they concretely imply that assurance information is concerned with a wider sort of independent information that fulfills both financial and non-financials needs, involves sophisticated technological enablers to be instantly processed, and relies on these modern advancements to be constantly

provided. Assurance provision shifts towards a more demand-driven approach that takes the assurance needs of users as the starting point, builds on the output of automated controls, analyses the entire data population, tests by means of digital workforce, and customizes reporting of the results to just mention few revamped features. This productive mechanism not only provides comfort but also provides clarity about the subject matter that expectedly contributes to the success of sharing ecosystems by going beyond vital

compliance with the standards and rules. Auditors are highly informed about the way in which sharing models operate, also deeply understand their technical processes, and identified risks, and consistently connect these inputs with defined assurance needs. The resulting assurance information becomes more valuable as it provides business acumen essential for decision-making purposes that are based on detailed impartial insights.

05.2 Follow up

This explorative study discusses the why and the what of data sharing economy that are mainly described in link with the implications regarding risk and assurance approaches. A logical suggestion for further research is to investigate the how-to of the aspects that are presented above to be transformed. The aim is to gather theoretical and practical knowledge about the way in which sharing businesses can earlier spot any risk, assess and mitigate it effectively by applying sophisticated digital capabilities. The result crafted as

an instructive guideline supports to mature the sharing processes and related operations, define what assurance information is needed, and in what form and frequency it is preferably provided. Based on independency and impartiality, the rationale here is to serve a larger group of assurance consumers with different information needs so that these users trustfully engage in share activities taking place in desired ecosystems.

05.3 Acknowledgements

The authors gratefully acknowledge the close collaboration with the TechLab Innovation Center, established under the IT Audit, Compliance and Advisory (ITACA) program at the Vrije Universiteit Amsterdam. Special appreciation is extended to Robert Kohler (Partner Assurance at KPMG Netherlands) for supporting the research concept, and to Milou van Vliet MSc RE (IT Risk Manager at BNG Bank), manager of TechLab, for her ongoing guidance.

The authors also thank drs. Paul Spaans (Partner Functional Quality & Risk Management at KPMG) and Ir. Enno van der Graaf (Senior Project Leader at KPMG Netherlands) for respectively reviewing and leading the publication trajectory. Finally, the contribution of Koen Klein Tank MSc RE (Partner Technology Assurance, KPMG) during the early stages of this research is sincerely appreciated.

05.4 Closing words

One of the points repeatedly surfaced during the research was the notion of the paradoxical characteristic of regulating the data sharing economy. This phenomenon is inherently innovative with a global reach and faces various adverse consequences. Regulators need to make certain that innovation is kept intact while negative effects are addressed for which three main strategies are usually applied. The first one is proactive in nature and just pertains to the regulate approach. It encompasses a broad range of policies from simply dealing with sharing models like traditional services to rigorously banning sharing activities altogether. The second strategy demonstrates an

avoiding feature and is plainly known as the do not regulate approach. It points out the self-regulating perspective according to which sharing platforms themselves equally serve the interest of both consumers and providers to ensure that they gladly join and loyally come back. The third strategy referred to as passive is concerned with the wait and see approach. To some extent, it fairly respects few forms of regulations and asks additional information for any tailored intervention (Ganapatia & Reddick, 2018). It is reasonable that the strategies also justify revamping risk and assurance practices conventionally in use.

06 Board and expert opinion

Management board is in charge of leveraging from the value that is embedded in bulks of data with the aim to drive tangible outcomes including better decisions and innovation. In this context, the role played by experts is indispensable to help extract the unrealized potential from a variety of sources in which data assets are digitally housed, and deploy it in practice.

Mariska van de Luur

Head of Assurance, member of the Board of Management of KPMG Netherlands

Sharing of data can only exist on the basis of trust. Trust is closely related to ethics: what intent and considerations do data users have with shared data and how do we safeguard data from being manipulated if ownership is obscured. This includes whether classic topics like cost-effectiveness are properly balanced with the concerns of the sharing era such as protecting consumers' data in line with the applicable regulatory requirements. A legitimate and sustainable data sharing economy is expected to take several key ethical considerations into account. Common examples are the confidence between consumers and providers by means of transparent digital platforms, and the informed consent when these capabilities collect, process and exchange personal information.

From my perspective, the report accentuates two things. First, the concept of real-time assurance driven by fast-paced adoption of technological advancements which can instantly handle large datasets. If data is available 24/7, users of that data will also want to know if data used is reliable. A first step might be for

companies to implement continuous monitoring to scan for exceptions in business processes and master data. Combined with target audit procedures this can evolve into continuous assurance, provided of course IT maturity can handle such processes.

And second, the usefulness of digital data along with sophisticated technology in sharing for the audit profession itself. Automation within auditing is not new. But the current digitally enabled mechanisms help to intelligently link data with auditing standards. That transforms audit from a static way of examination into a more dynamic approach that clearly leads to better audit quality and more frequent and value-based reporting. It makes auditors more flexible in adjusting their audit strategy and plans if data suggested different trends or anomalies. Specialized software can provide companies with added value as their data can be anonymously benchmarked against industry averages, sector specific companies to assist in identifying opportunities for improvement.

Edwin Herrie

Head of Advisory, member of the Board of Management of KPMG Netherlands

The data sharing economy is strategically reshaping organizations. Data is not just a byproduct of ongoing operations. It is a strategic asset that can unlock new forms of value creation across companies and economies. Clients today are navigating increasingly complex environments. The ability to access and leverage shared data, whether from partners, platforms, or public sources, can determine the success of digital transformation initiatives. Given that data comes from multiple sources also raises questions on data security and ethical data usage.

What stands out in this research for me is the recognition that end-to-end transformation is necessary

for companies to fully embrace the potential of data and to fully manage the associated risks. I see three stages to achieve that. First, companies need to rebuild their businesses around their customers to create a borderless organization, where people, technology and data interact to achieve new levels of productivity and value creation. Next, companies should harness the latest technologies, business practices and tested solutions to create more agile and nimble business operations. Finally, what the report also shows, companies need to approach risks and regulations in a balanced way to gain trust from stakeholders and shareholders.

John Kamphuis

Head of Assurance Transformation, member of the Leadership Team Assurance of KPMG Netherlands

What I find very exciting are the almost endless possibilities for innovation and new ways of creating value. Data sharing allows companies to combine previously unrelated data for new forms of experimentation, personalization, and co-creation. Insights are now generated at scale bringing jobs and products previously unthought of. It enriches jobs by reducing the need for manual repetitive tasks opening new ways of connecting and relating.

We are also seeing that the human dimension becomes increasingly vital. Inspired by KPMG's AI Vision, this paper also reflects on the need to humanize data practices ensuring transparency, fairness, and trust. Society is now shifting its focus toward securing fair value for personal data, not just in economic terms, but in ways that respect individual agency and foster responsible innovation.

Cybersecurity must obviously neither be overlooked nor underestimated. Its relevance is commonly associated with massive amounts of data and bulky infrastructures involved. The former is exchanged between various parties through decentralized, heterogenous, and widespread platforms that are usually operated by different providers and individual contractors around the world. To this global landscape, end users and customers connect via mobile devices to use billing systems and many other digitally enabled sharing services that are outside their control. It is hence essential to have a multi-layer of effective measures in place to, among other assets, secure third party access to apps and safeguard sensitive data approached by cloud resources.



References

- A Aaser, M., Kanagasabai, K., Roth, M., & Tavakoli, A. (2020). **Four ways to accelerate the creation of data ecosystems**, McKinsey Analytics, McKinsey & Company.
- Abbas, A.E., Agahari, W., Van de Ven, M., Zuidervijk, A., & De Reuver, M. (2021). **Business data sharing through data marketplaces: A systematic literature review**, Journal of Theoretical and Applied Electronic Commerce Research, Res. 2021, 16, 3321-3339, MDPI.
- Abu Rumman, A., & Lina Al-Abbad, L. (2023). **Structural equation modeling for impact of data fabric framework on business decision-making and risk management**, Cogent Business & Management, 10: 2215060.
- Accountancy Europe Audit and Assurance (AEAA) (2021). **Non-audit services and auditor's independence**, Briefing Paper, Views, Accountancy Europe.
- Adib, M., & Zhang, X.Z. (2019). **The risk-based management control system: A stakeholders' perspective to design management control systems**, International Journal of Management and Enterprise Development, Vol. 18, Nos. 1/2.
- Aditi Consulting (Aditi) (2024). **What is Datafication & how is it revolutionizing businesses?**, Blog, Data + Analytics, Aditi
- Agarwal, J., Buckley, S., Van Hoey, M., Van Niel, J., Samek, R., Somers, K., & Wells, I. (2021). **Adopting a smart data mindset in a world of big data**, Metals & Mining Practice, McKinsey & Company.
- Ahmad, S.S., Khan, S., & Kamal, M.A. (2019). **What is blockchain technology and its significance in the current healthcare system?** A brief insight, Bentham Science, Volume 25, Issue 12.
- American Institute of Certified Public Accountants (AICPA) (2015). **Audit analytics and continuous audit: Looking towards the future**, Journal of Emerging Technologies in Accounting, 13(1), 187-188.
- Akin, E.E., Klimbacher, S., & Ziccardi, G. (2024). **Smart cities, artificial intelligence, and digital transformation law: A handbook for students and professionals**, Milan University Press.
- Alaimo, C., & Kallinikos, J. (2024). **Data rules: Reinventing the market economy**, The MIT Press.
- Alation (2024). **Effective data quality assurance: Strategies for reliable data**, Alation.
- Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J.M., Confalonieri, R., Guidotti, R., Del Ser, J., Díaz-Rodríguez, N., & Herrera, F. (2023). **Explainable Artificial Intelligence (XAI): What we know and what is left to attain trustworthy artificial intelligence**, Information Fusion, Elsevier.
- Alter, G., & Gonzalez, R. (2018). **Responsible practices for data sharing**, 0003-066X/18/\$12.00, American Psychological Association, Vol. 73, No. 2, 146-156.
- Alton, L. (2024). **Algorithms and operators: Making the most of analytics**, SmartDataCollective.
- Alwan, H.B., & Ku-Mahamud, K.R. (2020). **Big data: definition, characteristics, life cycle, applications, and challenges**, The 6th International Conference on Software Engineering & Computer Systems, IOP Conf. Series: Materials Science and Engineering 769 (2020) 012007, IOP Publishing.
- Amazon Web Services (AWS) (2024). **What is a chatbot?**, AWS.
- Amazon Web Services (AWS) (2025). **What is DevOps?**, AWS.
- Archer (2020). **8 steps to modernize compliance**, White Paper, Archer.
- Ardagna, D., Francalanci, C., & Piuri, V. (2004). **Designing and rightsizing the information system architecture**, Information Systems Frontiers 6:3, 229-245, Kluwer Academic Publishers, The Netherlands.
- Asadullah, A., Faik, I., & Kankanhalli, A. (2018). **Digital platforms: a review and future directions**, Pacific Asia Conference on Information Systems (PACIS) 2018 Proceedings, 248, Association for Information Systems (AIS) Electronic Library (AISeL).
- Australian Research Data Commons (ARDC) (2024). **TRUST principles**, ARDC.
- Awli, O., & Lau, E. (2023). **Digital and sharing economy for sustainable development: A bibliometric and systematic review**, Economics, 11(4), 105, MDPI.
- Ayers, R. (2024). **5 ways big data is fueling the sharing economy**, SmartDataCollective.
- Azadmanesh, M.H., & Peak, D.A. (1995). **The metamorphosis of the mainframe computer: The superserver**, Association for Information Systems (AIS), AIS Electronic Library (AISeL), Americas Conference on Information Systems (AMCIS), AMCIS 1995 Proceedings.

- B** Babkin, A., Golovina, T., Polyanin, A., & Vertakova, Y. (2018). **Digital model of sharing economy, Blockchain technology management**, SHS Web of Conferences 44, 00011, EDP Sciences.
- Bacco, M., Kocian, A., Chessa, S., Crivello, A., & Barsocchi, P. (2024). **What are data spaces? Systematic survey and future outlook**, Data in Brief 57, 110969, Elsevier.
- Baes, K., Majster, M., Clauwaert, S., & Deweer, S. (2023). **How data sharing is essential to deliver industry wide transformation**, Arthur D. Little.
- Baker, A. (2023). **Data assurance: Building trust in data**, Project, Open Data Institute (ODI).
- Balla, E. (2024). **What is datafication? Exploring its evolution and unforeseen consequences**, IndiaAI.
- Barbu, C., & Bratu, R.S. (2018). **Business models of the sharing economy**, Review of International Comparative Management, Volume 19, Issue 2.
- Barnes, S. (2021). **The importance of data sharing for the economy of tomorrow**, Authoritative Analysis on International Banking, International Banker.
- Barros, C., & Marques, R.P. (2022). **Continuous Assurance for the Digital Transformation of Internal Auditing**, Journal of Information Systems Engineering and Management, 7(1), 11681, e-ISSN: 2468-4376.
- Barsch, P. (2025). **What the sharing economy means for cloud computing**, SmartDataCollective.
- Basselier, R., Langenus, G., & Walravens, L. (2018). **The rise of sharing economy**, NBB Economic Review, 57-78.
- Bhatti, H.J., & Bashari Rad, B. (2017). **Databases in cloud computing: A literature review**, Information Technology and Computer Science, 4, 9-17, Modern Education and Computer Science (MECS) Press.
- Bird & Bird (Bird) (2024). **Trust frameworks for data sharing**, Bird..
- Birkinshaw, J., & Cable, D. (2017). **The dark side of transparency**, McKinsey Quarterly, McKinsey & Company.
- Bloomenthal, A., James, M., & Munichello, K. (2024). **E-commerce defined: Types, history, and examples**, Investopedia.
- Blumberg, S., Chui, M., Yee, L., Javanmardian, K., Singla, A., Smaje, K., & Sukharevsky, A. (2024). **What is AI (artificial intelligence)?**, McKinsey Explainers, McKinsey & Company.
- BMC (2025). **Service assurance and optimization**, BMC.
- Bogner, A., Chanson, M., & Meeuw, A. (2016). **6TH International Conference on the Internet of Things (IoT'16)**, Stuttgart, Germany.
- Booking.com Partner Hub (Booking) (2025). **Understanding, detecting, and reporting fake reservations**, Booking.
- Box, D., Miller, B., & Kipnes, J. (2024). **Technology assurance: Assess risk, build trust and create resilience**, Ernst & Young Global Limited.
- Brodsky, L., & Oakes, L. (2017). **Data sharing and open banking**, McKinsey on Payments, McKinsey & Company.
- Brosh, R. (2024). **Key Compliance Indicators for Financial Institutions**, NContracts.
- Brousseau, E., Eustache, L., & Toledano, J. (2024). **Position paper: Economics of data sharing – Study on the emergence and creation of value within data-sharing ecosystems**, Gaia-X institute, and Paris Dauphine University.
- Byabazaire, J., O'Hare, G., & Delaney, D. (2020). **Data Quality and Trust: Review of Challenges and Opportunities for Data Sharing in IoT**, MDPI, Electronics, 9, 2083.
- Byrne, D. (2025). **What is corporate governance?**, Lexicon, Corporate Governance Institute.
- C** Calcutt, E., & Ranger, N. (2020). **Five reasons you should be thinking about compounding risks now**, Financial Protection Forum, World Bank Group.
- Caldarulo, M., Olsen, J., & Feeney, M.K. (2024). **Oversharing: The downside of data sharing in local government**, DOI: 10.1111/padm.12993, Public Administration, Wiley.
- Campbell, C. (2024). **What are the 4 different types of blockchain technology**, TechTarget.
- Canadian Audit & Accountability Foundation (CAAF) (2024). **What is governance?, Practice Guide to Auditing Oversight**, CAAF.
- Carson, D. (2024). **Understanding and managing the risks of data sharing**, RiskDataControl.com.
- Carson, B., Nadeau, M.C., & Chui, M. (2024). **What is blockchain?**, McKinsey Explainers, McKinsey & Company.
- Cash, A. (2023). **Your guide to customer trust in a privacy-centric world**, Tealium Inc.
- Centre for Information Policy Leadership (CIPL) (2023). **Data sharing between public and private sectors: When local governments seek information from the sharing economy**, Discussion Paper, CIPL.
- Centre of Excellence for Data Sharing and Cloud (CoE-DSC) (2025). **The data sharing coalition reveals the findings of a case study on digital identity assurance for data spaces**, CoE-DSC.

- Česnuitytė, V., Klimczuk, A., Miguel, C., & Avram, G. (Eds.) (2022). **The sharing economy in Europe: Developments, practices, and contradictions**, Palgrave Macmillan.
- Charan, R., Huber, C., & Usher, O. (2024). **How CEOs can mitigate compounding risks**, Strategy & Corporate Finance Practice, McKinsey & Company.
- Chatterton, C. (2025). **Risk management techniques: Understanding different approaches and how to apply them**, Hyperproof.
- Charter Global (Charter) (2024). **How big data is driving business digital transformation**, Charter.
- Chaudhry, R. (2022). **Layered digital architecture can accelerate your digital transformation**, Enterprise Architecture, Medium.
- Chen, J., Mansa, J., & Courage, A. (2024). **Business-to-business (B2B): What it is and how it's used**, Investopedia.
- Chubb (2017). **The sharing economy: digital risks for young professionals**, Chubb.
- Cigniti Technologies (Cigniti) (2024). **How digital assurance is different from traditional QA**, Coforge.
- City of Saskatoon (Saskatoon) (2023). **Continuous assurance: Audit report**, Independent Office of the City Auditor, Saskatoon.
- Codagnone, C., & Martens, B. (2016). **Scoping the sharing economy: Origins, definitions, impact, and regulatory issues**, JRC Technical Reports, Institute for Prospective Technological Studies, Digital Economy Working Paper 2016/01, European Commission.
- Coderre, D. (2005). **Continuous auditing: Implications for assurance, monitoring, and risk assessment (Global Technology Audit Guide)**, Altamonte Springs, FL: The Institute of Internal Auditors, 1-33.
- Connected Automated Driving Europe (CADE) (2024). **Data sharing approaches**, CADE.
- Constantiou, I., Marton, A., & Tuunainen, V.K. (2017). **Four Models of Sharing Economy Platforms**, MIS Quarterly Executive, 16:4.
- Costabile, A. (2024). **Operations data sharing: A critical time to innovate**, Executive Summary, Crisil.
- Cote, C. (2021). **What is predictive analytics? 5 examples**, Harvard Business School Online.
- C. (2022). **What is new-market disruption? 3 examples**, Harvard Business School Online.
- Coyle, D., & O'Connor, S. (2019). **Understanding the sharing economy**, Economics Statistics Center of Excellence (ESCoE), ESCoE Discussion Paper 2019-04, ISSN: 2525-4664, ESCoE, National Institute of Economic and Social Research.
- CSCi (2019). **What is the as-a-service model?**, CSCi.
- Cullen, S., Seddon, P.B., & Willcocks, L.P. (2005). **IT outsourcing configuration: Research into defining and designing outsourcing arrangements**, Journal of Strategic Information Systems 14, 357-387.
- Curry, E., Scerri, S., & Tuikka, T. (Eds.) (2022). **Data spaces: Design, deployment, and future directions**, Springer.
- Cyberint (2024). **Ransomware Q2 2024 report**, Cyberint.
- Cyber Saint Security (CSS) (2025). **What is risk-based compliance management?**, CSS.
- D** Dabija, D.C., Csorba, L.M., Isac, F.L., & Rusu, S. (2023). **Managing sustainable sharing economy platforms: A stimulus–organism–response based structural equation modelling on an emerging market**, Sustainability, 15, 5583, MDPI.
- Dash, P., Smit, S., & Brown, S. (2020). **Choosing the right pad to unlock the economy**, Strategy & Corporate Finance Practice, McKinsey & Company.
- Cote, Data Spaces Support Centre (DSSC) (2024a). **11 foundation of the European data economy concepts**, DSSC.
- Data Spaces Support Centre (DSSC) (2024b). **About the DSSC toolbox**, DSSC.
- Data Spaces Support Centre (DSSC) (2024c). **Alphabetical list of all defined terms in blueprint v1.5**, DSSC.
- Data Spaces Support Centre (DSSC) (2024d). **Building block overview**, DSSC.
- Data Spaces Support Centre (DSSC) (2024e). **Business and organizational building blocks**, DSSC.
- Data Spaces Support Centre (DSSC) (2024f). **Data sovereignty and trust**, DSSC, **Data interoperability**.
- Data Spaces Support Centre (DSSC) (2024g). **Data spaces blueprint v1.5 – Home**, DSSC.
- Data Spaces Support Centre (DSSC) (2024h). **How a data plane and control plane work together**, DSSC.
- Data Spaces Support Centre (DSSC) (2024i). **Mission and vision**, DSSC.
- Data Spaces Support Centre (DSSC) (2024j). **Promote environmental sustainability**, DSSC.
- Data Spaces Support Centre (DSSC) (2024k). **Services for implementing technical building blocks**, DSSC.
- Data Spaces Support Centre (DSSC) (2024l). **Technical building blocks**, DSSC.
- Data Spaces Support Centre (DSSC) (2024m). **Value creation services**, DSSC.

- Dela Rosa Algarin, A., & Demurjian, S.A. (2014). [Chapter 4 – An approach to facilitate security assurance for information sharing and exchange in big data applications](#), Emerging Trends in ICT security Pages 65-83, Elsevier.
- DELL Technologies (Dell) (2020). [The data paradox: Research findings](#), Dell Inc.
- De Reuver, M., Sørensen, C., & Basole, R.C. (2018). [The digital platform: A research agenda](#), Journal of Information Technology 33, 124-135.
- D’Hauwers, R., Van der Bank, J., & Montakhabi, M. (2020). [Trust, transparency, and security in the sharing economy: What is the government's role?](#), Technology Innovation Management Review, Volume 10, Issue 5.
- Diaz, T. (2023). [Consumer-to-Business: C2B definition and examples](#), Study.com.
- Digital-operational-resilience-act.com (DORA.com) (2025). [The digital operational resilience act \(DORA\) – Regulation \(EU\) 2022/2554](#), DORA.com.
- Digital Trust Center (DTC) (2025). [Bring your own device \(BYOD\)](#), DTC.
- Dilger, B. (2022). [What is data sharing? A guide to improving internal data accessibility](#), Narrative.
- Dillahunt, T.R., Wang, X., Wheeler, E., Cheng, H.F., Hecht, B., & Zhu, H. (2017). [The sharing economy in computing: A systematic literature review](#), Proceedings of the ACM on Human-Computer Interaction, Vol. 1, No. CSCW, Article 38.
- DiMaria, J. (2020). [What is a cloud service provider?](#), Cloud Security Alliance (CSA).
- Domberger, S., Fernandez, P., & Fiebig, D.G. (2000). [Modelling the price, performance and contract characteristics of IT outsourcing](#), Journal of Information Technology, 15, 107-118.
- Domingos, P. (2024). [IT breakdown: Datafication](#), White Paper, Aditi Consulting.
- Donald, A.D., Srinivas, A.S., Rekha, K., Anjali, D., & Srihith, I.D. (2023). [The data revolution: A comprehensive survey on datafication](#), International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 3, Issue 1.
- Duncan, A.d. (2022). [Drive business outcomes by measuring the value of data literacy](#), Gartner Research, ID G00761792, Gartner.
- Dye, R., & Stephenson, E. (2010). [Five forces reshaping the global economy](#), McKinsey Global Survey Results, McKinsey & Company.
- E** Edquist, A., Grennan, L., Griffiths, S., & Rowshankish, K. (2022). [Data ethics: What it means and what it takes](#), QuantumBlack, AI by McKinsey, McKinsey Digital, McKinsey & Company.
- Efficient Vision (EV) (2024). [What is datafication and why is it the future of business?](#), Technology, EV.
- Elmore Insurance Brokers (Elmore) (2022). [5 risks that sharing economy platforms face](#), Elmore.
- Ergasheva, S., & Kruglov, A. (2020). [Software development life cycle early phases and quality metrics: A systemic literature review](#), Information Technologies, Telecommunications, and Control Systems (ITTCS), Journal of Physics, Conference Series, IOP Publishing.
- Eriksson, K.B. (2016). [The great decentralization: A sharing economy for the financial services](#), PwC.
- Estavez, E., & Jackson, A. (2024). [What is a smartphone? A mobile phone and computer in one device](#), Investopedia (<https://www.investopedia.com/terms/s/smartphone.asp>).
- Etherington, M. (2020). [Survey: Enterprise data more important than ever since onset of COVID-19](#), Article, Teradata.
- European Banking Authority (EBA) (2019). [Final report on EBA guidelines on outsourcing arrangements](#), EBA/GL/2019/02, EBA.
- European Union (EU) (2022). EUR-Lex, [Access to European Union law](#), Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), Document 32022R0868, EU.
- European Union (EU) (2018). [Study on data sharing between companies in Europe](#), Directorate-General of Communications Networks, Content & Technology, EU.
- European Union Agency for Cybersecurity (ENISA) (2022). [Data protection engineering: From theory to practice](#), ENISA.
- Everson, M.E.A., Chesley, D.L., Martens, F.J., Bagin, M., Katz, H., Sylvis, K.T., Perraglia, S.J., Crader Zelnik, K., & Grimshaw, M. (2017). [Enterprise risk management: Integrating with strategy and Performance](#), Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- F** Favaretto, M., De Clercq, E., Schneble, C.O., & Elger, B.S. (2020). [What is your definition of big data? Researchers’ understanding of the phenomenon of the decade](#), Research Article, Tenth International Conference on Peer Review and Scientific Publication.
- Felländer, A., Ingram, C., & Teigland, R. (2015). [The sharing economy: Embracing change with caution](#), Näringspolitiskt Forum, Rapport # 1 1, Örebro University, Sweden.
- Figueiredo, B. (2022). [Datafication: What it is and how it can transform your business](#), Codepwr.
- Floridi, L., & Taddeo, M. (2016). [What is data ethics?](#), Oxford Internet Institute, University of Oxford, Alan Turing Institute, The Royal Society Publishing.

- Flóttotó, M., Ledbetter, B., Olanrewaju, T., Krivkovich, A., Nadeau, M.C., & Windhagen, E. (2024). **What is fintech?** McKinsey Explainer, McKinsey & Company.
- Francken, M., Heijstek, H.A.S., Shahim A., Schinagl, S., & Rieske, S.W. (2022). **Applying machine learning in audit techniques: Towards (near) real-time assurance**, IT Audit, Compliance and Advisory (ITACA) Program, White Paper, TechLab Edition, Vrije Universiteit (VU) Amsterdam, School of Business and Economics, and BDO, VU Amsterdam.
- Frontier Economics (Frontier) (2021). **Economic impact of trust in data ecosystems: Report prepared for Open Data Institute (ODI)**, Frontier.
- G** Ganapatia, S., & Reddick, C.G. (2018). **Prospects and challenges of sharing economy for the public sector**, Government Information Quarterly, Elsevier, Inc.
- Gartner (2024a). **Drive successful business outcomes with data, analytics and AI**, Data and Analytics Insights, Roadmap.
- Gartner for Audit Leaders (Gartner) (2024b). **Top audit departments priorities for 2025**, Gartner.
- Gartner (2025a). **Gartner Glossary**, Gartner.
- Gartner (2025b). **Gartner Glossary, Information Technology**, Gartner.
- Gazis, A. (2021). **What is IoT? The internet of things explained**, Democritus, School of Engineering, Department of Electrical and Computer Engineering, Greece.
- Gemilang, G.A., Ganish, E.T., Anggraeni, N.D., & Nugrahanti, T.P. (2024). **Latest trends in auditing by uncovering the digital age and best practices for efficiency and accuracy**, Journal Markcount Finance, 2 (1), 158-167.
- Geotab Team (Geotab) (2024). **What is GPS and how do global positioning system work?**, Geotab.
- Ghazawneh, A., & Henfridsson, O. (2013). **Balancing platform control and external contribution in third-party development: The boundary resources model**, Information Systems Journal, 23, 173-192.
- Gieß, A., Schoormann, T., Moller, F., & Gür, I. (2024). **Discovering data spaces: A classification of design options**, Computers in Industry 164, 104212, Elsevier.
- Gigaom (2025). **The business case for data fabric: The essential role of integration in your data fabric design**, Gigaom.
- Giustiniano, L., & Clarioni, G. (2013). **The impact of outsourcing on business performance: An empirical study**, Journal of Modern Accounting and Auditing, ISSN 1548-6583, Vol. 9, No. 2, 153-168.
- Global Business Travel Industry (GBTA) (2022). **Mitigating risks in the sharing economy**, GBTA.
- Goasduff, L. (2021). **Data sharing is a business necessity to accelerate digital Business**, Article, Insights, Information Technology, Gartner.
- Golshanara, L., & Chomicki, J. (2020). **Temporal data exchange**, Information Systems, Volume 87, 101414, Elsevier.
- Greenstein, S.M., & Wade, J.B. (1998). **The product lifecycle in the commercial mainframe computer market, 1968-1982**, The RAND Journal of Economics, Vol. 29, No. 4, 772-789.
- Grosse-Ophoff, A., Hausler, S., Heineke, K., Möller, T. (2017). **How shared mobility will change the automotive industry**, Automotive & Assembly, McKinsey & Company.
- Gu, H., Zhang, T., Lu, C., & Song, X. (2021). **Assessing trust and risk perceptions in the sharing economy: An empirical study**, Journal of Management Studies 58:4, Society for Advancement of Management Studies and John Wiley & Sons, Ltd.
- Gumi & Company (Gumi) (2022). **4 exponential technologies for solving poverty**, Gumi.
- Gupta, T. (2023). **Data-driven AI: Understanding the risks and mitigations**, Cloud Security Alliance (CSA).
- Gupta, R. (2024). **Evolution of SAP ERP system – From mainframe systems to a modern cloud solution**, Medium.
- Gupta, M. (2015). **There is a cloud platform behind every successful sharing economy business model**.
- Gupta, D. (2025). **Uber introduced its digital financial services “Uber Money”**, Appinventiv.
- H** Hamblin, D.J., & Phoenix, D.A. (2012). **A model for managing data assurance in higher education**, Journal of Higher Education Policy and Management, Vol. 34, No. 4.
- Hammergren, T. (1996). **Data warehousing: Building the corporate knowledge base**, International Thomson Computer Press.
- Han, S., Han, K., & Zhang, S. (2019). **A data sharing protocol to minimize security and privacy risks of cloud storage in big data era**, IEEE Access, Volume 7.
- Harahap, A., & Nabillah, M. (2023). **Human and development technology in the modern era**, International Journal of Student Education, Berpusi Publishing, 55-58, ISSN 2344-4890.
- Harreis, H., & Rowshankish, K. (2017). **Risk management goes digital**, McKinsey & Company.

- Hassan, N. (2024). [What is data poisoning \(AI poisoning\) and how does it work?](#), Search Enterprise AI, TechTarget.
- Haucap, J., Fritz, D., & Thorwarth, S. (2022). [The economic impact of cloud computing in Europe](#), A research report commissioned by the European Cloud Alliance, DICE Consult.
- Hayden, D. (2025). [PESTLE analysis](#), CIPD.
- Hayes, R., Wallage, P., & Eimers, P. (2024). [Principles of international auditing and assurance](#), Fifth Edition, Amsterdam University Press.
- Henke, C. (2023). [What is IoT security? Risks, examples, and solutions](#), Emnify.
- Hira, A., & Reilly, K. (2017). [The Emergence of the Sharing Economy: Implications for Development](#), SAGE Publications.
- Hirschheim, R., Heinzl, A., & Dibbern, J. (Eds.) (2020). [Information systems outsourcing: The era of digital transformation](#), Progress in IS, Fifth Edition, Springer Nature Switzerland AG.
- HM Treasury (HMT) (2018). [The economic value of data: Discussion paper](#), OGL, Crown copyright.
- Hong, J.H., Kim, B.C., & Park, K.S. (2019). [Optimal risk management for the sharing economy with stranger danger and service quality](#), European Journal of Operational Research, 279, 1024-1035, Elsevier.
- Horton International (Horton) (2025). [Implications of sharing economy for the financial services industry](#), Horton.
- Houst (2025). [What are Airbnb scams? 9 scams to be aware of while booking](#), Blog, Houst.
- Hussein, R., Scherdel, L., Nicolet, F., & Martin-Sanchez, F. (2023). [Towards the European Health Data Space \(EHDS\) ecosystem: A survey research on future health data scenarios](#), International Journal of Medical Informatics, 170, 104949.
- IBM (2024). [What is a data fabric?](#), IBM.
- IBM (2025). [What is data lifecycle management \(DLM\)?](#), IBM.
- ICAEW Audit & Assurance Faculty (ICAEW) (2014). [Assurance over key performance indicators](#), The journey: Milestone 1, ICAEW.
- ICAEW Audit & Assurance Faculty (ICAEW) (2012). [Assurance sourcebook: A guide to assurance services](#), Assurance Initiative, ICAEW.
- IEEE Digital Privacy (IEEE) (2025). [What is privacy-by-design and why it's important?](#), IEEE.
- Ilbiz, E., & Kaunert, C. (2023). [The sharing economy for tackling cybercrime](#), Advanced Sciences and Technologies for Security Applications, Springer.
- ILR School and the Aspen Institute (ILR) (2025). [What is a gig worker?](#), Gig Economy Data Hub.
- Indeed Editorial Team (IET) (2024). [What is a trend and how does it work?](#) (Including examples), Indeed.
- Inmon, W.H. (1996). [Building the Data Warehouse](#), John Wiley & Sons Inc., Second Edition.
- Inmon, W.H. (1986). [Information systems architecture: A system developer's primer](#), Englewood Cliffs, New Jersey, Prentice-Hall, Inc.
- Inmon, W.H., Zachman, J.A., & Geiger, J.G. (1997). [Data store, data warehousing, and the Zachman framework: Managing enterprise knowledge](#), The McGraw-Hill Companies, Inc.
- International Auditing and Assurance Standards Board (IAASB) (2019). [International standard on auditing 315 \(revised 2019\)](#), Final Pronouncement, IAASB.
- International Federation of Accountants (IFAC) (2018). [Leveraging technology](#), Module 5, IFAC, New York, USA.
- International Federation of Accountants (IFAC) (2021). [Using ISAE 3000 \(revised\) in sustainability assurance engagements](#), IFAC, New York, USA.
- International Risk Governance Council (IRGC) (2019). [What do we mean by risk governance?](#), IRGC.
- J** James, S., & Duncan, A.D. (2024). [Over 100 data, Analytics and AI predictions through 2023](#), Gartner for Data & Analytics Leaders, Gartner.
- Jensen, S.F., Kristensen, J.H., Adamsen, S., Christensen, A., & Waehrens, B.V. (2023). [Digital products passports for a circular economy: Data needs for product life cycle decision-making](#), Sustainable Production and Consumption 37, 242-255, Elsevier.
- Johnson, M.P., & Huston, E. (2024). [Technology assurance](#), KPMG LLP.
- Jussen, I., Schweihoff, J., Dahms, V., Möller, F., & Otto, B. (2023). [Data Sharing Fundamentals: Characteristics and Definition](#). In Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii, USA.
- K** Kanagarla, K.P.B. (2024). [Data fabric: A new approach to data integration](#), International Journal for Engineering and Management Research, Volume 13, Issue 10, ISSN: 2456-5083.
- Kenton, W., Brock, T., & Perez, Y. (2024a). [B2C: How business-to-consumer sales works, types, and examples](#), Investopedia.

- Kenton, W., Kelly, R.C., & Rohrs Schmitt, K. (2024b). [Business-to-government \(B2G\): Selling to the government](#), Investopedia.
- Kenton, W., & Scott, G. (2020). [What is a third party? How their role works and examples](#), Investopedia.
- Khan, M. (2023). [The rise of datafication: Unveiling the evolution and basics](#), Medium.
- Kim, A., Libarikian, A., Brodherson, M., Arora, A., Smaje, K., Dreischmeier, R., Atsmon, Y., Boudet, J., Dörner, K., Roche, P., & Kohli, S. (2025). [What is e-commerce?](#), McKinsey Explainers, McKinsey & Company.
- Kiourtis, A., Mavrogiorgou, A., & Makridis, G. (2023). [Data marketplaces: Best practices, challenges, and advancements for embedded finance](#), 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), IEEE.
- Klarin, A., & Suseno, Y. (2021). [A state-of-the-art review of the sharing economy: Scientometric mapping of the scholarship](#), Journal of Business Research, 126, 250–262.
- Klein, A., Braumann, E., & Posch, A. (2023). [Risk management in the era of digitalization: The role of strategic integration and advanced analytics](#), Vlerick Business School.
- Köbis, N.C., Soraperra, I., & Shalvi, S. (2021). [Journal of Management](#), Vol. 47, No. 1, 317-343.
- Kocken, J., & Hulstijn, J. (2017). [Providing continuous assurance](#), Deloitte Risk Advisory and Tilburg University.
- Koenen, E., Schwarzenegger, C., & Kittler, J. (2021). [Data\(fication\): Understanding the world through data as an everlasting revolution](#), De Gruyter.
- Koilakonda, R.R. (2024). [Holistic risk management strategies for digital transformation: A comprehensive guide approach](#), International Journal of Science and Research (IJSR), Volume 13, Issue 6.
- Koorn, R., & Zwinkels, S. (2021). [SOC2 assurance becomes critical for cloud & IT service providers](#), Compact, KPMG Netherlands.
- Kristensen, I., Chiapolino, M., Del Mar Martínez, M., & Jain, R. (2024). [The six habits of highly successful chief risk officers](#), Risk & Resilience practice, McKinsey & Company.
- Kumar, A., Wyrwich, T., & Waggoner, D.M. (2017). [Shared risks? The top six issues facing the sharing economy](#), Insights, Davis Wirright Tremaine LLP.
- Kushnir, M. (2023). [G2B](#), Snov.
- Lamarre, E., Robinson, H., Galvin, J., Smaje, K., Javanmardian, K., Khan, N., Sohoni, V., Yee, L., Sellschop, R., Zimmel, R., & Blackburn, S. (2024). [What is digital transformation](#), McKinsey Explainers, McKinsey & Company.
- Lee, S.U., Zhu, L., & Jeffrey, R. (2017). [Data governance for platform ecosystems: Critical factors and the state of practice](#), Twenty First Pacific Asia Conference on Information Systems, Langkawi.
- Lee, J.W. (2021). [The data sharing economy and open governance of big data as public cloud](#), Journal of Asian Finance, Economics, and Business, Vol. 8, No.11, 0087-0096.
- Lefebvre, H., Legner, C., & Teracino, E. (2023). [5 pillars for democratizing data at your organization](#), Technology & Analytics, Harvard Business Review (HBR).
- Lehr, A., Büttgen, M., & Bartsch, S. (2021). [Don't Jump on the Bandwagon: Negative Effects of Sharewashing](#), Schmalenbach Journal of Business Research, 73:75–123.
- Lenovo (2025). [What is alignment?](#), Glossary, Lenovo.
- Letourmy, L. (2024). [Data partner selection: Find your perfect match!](#), Devoteam.
- Levy, C., De Boer, E., Richter, G., Patel, M., & Mancini, M. (2024). [What is the Internet of Things \(IoT\)?](#) McKinsey Explainers, McKinsey & Company.
- Li, Z. (2023). [Understanding the sharing economy](#), Thunderbird School of Global Management, Arizona State University (ASU).
- Liao, Z. (2024). [Analysis of the Development Status of the Sharing Economy](#), Proceedings of the 3rd International Conference on Business and Policy Studies, DOI: 10.54254/2754-1169/76/20241575.
- Lim, J. (2020a). [Risk returns](#), Humble Dollar.
- Lim, W.M. (2020b). [The sharing economy: A marketing perspective](#), Australian Marketing Journal 28, 4-13, Australian and New Zealand Marketing Academy, Elsevier Ltd.
- Lin, D., Crabtree, J., Dillo, I., Downs, R.R., Edmunds, R., Giaretta, D., DeGiusti, M., L'Hours, H., Hugo, W., Jenkyns, R., Khodiyar, V., Martone, M.E., Mokrane, M., Navale, V., Petters, J., Sierman, B., Sokolova, D.V., Stockhouse, M., & Westbrook, J. (2020). [The TRUST principles for digital repositories](#), Scientific Data 7, Article number: 144.
- Lingeswara Satyanarayana Tammineedi, R. (2018). [Integrating KRIs and KPIs for Effective Technology Risk Management](#), ISACA Journal, Vol. 4.
- Liu, C., Chan, R.K.H., Wang, M., & Yang, Z. (2020). [Mapping the sharing economy in China](#), Sustainability 2020, 122, 6333, MDPI.

- Luo, J. (2022). **Data-driven innovation: What is it?**, IEEE Transactions on Engineering Management, Volume 70, Issue 2.
- Luo, X., Li, H., & Warkentin, M. (2013). **Understanding technology adoption trade-offs: A conjoint analysis**, Journal of Computer Information Systems.
- M Madgavkar, A., & White, O. (2021). **The promise of open financial data**, Article, Project Syndicate, McKinsey Global Institute, McKinsey & Company.
- Mahesh, B. (2020). **Machine learning algorithms: A review**, International Journal of Science and Research (IJSR), ISSN: 2319-7064, Volume 9, Issue 1.
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byes, A. (2011). **Big data: The next frontier for innovation, competition, and productivity**, McKinsey Global Institute, McKinsey & Company.
- Marchi, A., & Parekeh, E.J. (2015). **How the sharing economy can make its case**, McKinsey Quarterly, McKinsey & Company.
- Maritz, S. (2024). **Understanding the difference between nearshoring**, offshoring, and outsourcing, Blackbear.
- Market Research Future (MRF) (2024). **Global sharing economy market: Market analysis (2018 – 2032)**, ICT, MRF.
- Mattsson, T. (2024). **The sharing economy, a growing problem or a needed change?**, Bacconi Students Capital Markets.
- Mayer, R., Davis, J.H., & Schoorman, F.D. (1995). **An integrative model of organizational trust**, *Academy of Management Review*, Vol. 20, No. 3, 709-734.
- Mayer-Schönberger, V., & Cukier, K. (2013). **Big data: A revolution that will transform how we live, work, and think**, Houghton Mifflin Harcourt, Boston, New York.
- Mayer-Schönberger, V., & Cukier, K. (2024). **What is datafication technology: The future of business explained**, Technology Trends, Blog, Mapsted.
- Maynard, T. (2018). **Sharing risks, sharing rewards: Who should bear the risk in the sharing economy?**, Innovation Report 2018, Lloyd's.
- Mejias, U.A., & Couldry, N. (2019). **Datafication, Internet Policy Review**, Journal on Internet Regulation, Volume 8, Issue 4.
- Mektrakarn, T. (2025). **The risk-based mindset: A modern approach to risk management**, Bright Defense.
- Menne, A. (2018). **Blockchain in the sharing economy: Will blockchain disrupt today's winning business models?**, 29th Twente Student Conference on IT, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, The Netherlands.
- Mertens, C., & Kuster, A. (2024). **The data spaces radar**, Data Spaces Support Center Edition, #4, International Data Spaces Association, Dortmund, Germany.
- Mezzeta, S. (2023). **Principles of data fabric: Become a data-driven organization by implementing data fabric solutions efficiently**, Packt Publishing.
- Michalsons Giles Inc. (Michalsons) (2023). **Data pooling: How to combine data while staying legal**, Michalsons.
- Michulek, J., Gajanová, L., & Blazek, R. (2023). **A state-of-the-art review of sharing economy: Comprehensive bibliometric analysis**, Faculty of operation and economics of transport and communication, Department of economics, University of Zilina, Slovakia.
- Miguel, C., Martos-Carrión, E., & Santa, M. (2022). **A conceptualization of the sharing economy: Towards theoretical meaningfulness**, in: Česnuitytė et al., 2022.
- Minami, A.L., Ramos, C., & Bruscatto Bortoluzzo, A. (2021). **Sharing economy versus collaborative consumption: What drives consumers in the new forms of exchange?**, Journal of Business Research, Volume 128, 124-137, Elsevier.
- Minca, C., & Roelofsen, M. (2019). **Becoming Airbnbeings: On datafication and the quantified self in tourism**, Tourism Geographies, An International Journal of Tourism Space, Place, and Environment, ISSN: 1461-6688, 1470-1340.
- MIT Technology Review Insights (MIT) (2023). **The great acceleration: CIO perspectives on generative AI**, Produced in partnership with databricks, MIT.
- Molengraaf, C., Kapitan, D., Groen, P., & Travkina, Y. (2023). **Privacy enhancing technologies whitepaper**, Center of Excellence – Data Sharing and Cloud.
- Moon, Y. (2007). **Enterprise Resource Planning (ERP): A review of the literature**, International Journal of Management and Enterprise Development, Vol. 4, No. 3.
- Moratis, L. (2017). **Challenging business as usual: Conceiving and creating sustainability value through hybrid business models**, Antwerp Management School, Powered by the University of Antwerp.
- Mosaad, M., Benoit, S., & Jayawardhena, C. (2023). **The dark side of the sharing economy: A systematic literature review of externalities and their regulation**, Journal of Business Research 168, 114186.
- Mucci, T. (2024a). **What is a data marketplace?**, Analytics, IBM.
- Mucci, T. (2024b). **What is a data provenance?**, Analytics, IBM.

- Mullins, C.S. (2025). [What is extract, load, transform](#), Search Data Management, TechTarget.
- Murphy, B., & Curran, P. (2023). [Choosing the right cloud file storage system for your business](#), White Paper, WEKA Data Platform.
- N** Naqvi, A. (2025). [Data utilization: What is it and why is it important](#), Xavor Corporation.
- Natale, A., Poppensieker, T., & Thun, M. (2022). [From risk management to strategic resilience](#), Risk & Resilience practice, McKinsey & Company.
- National Institute of Standards and Technology (NIST) (2025), Information Technology Laboratory, Computer Security Resource Center, [Glossary](#), NIST.
- Nexla, Inc. (2025). [Data fabric architecture](#), Nexla.
- Nguyen, V., Colic, M., Weise, I., Natarajan, S., Thakur, S., Bhankharia, J., Goicochea, G., & Albano, K. (2023). [A new approach to data sharing: Open data sharing and collaboration for data](#), analytics and AI, eBook, Second Edition, Databricks.
- Noble, A. (2023). [From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis](#), The Royal Society.
- Nokkala, T., Salmela, H., & Toivonen, J. (2019). [Data governance in digital platforms](#), Twenty-fifth Americas Conference on Information Systems, Cancun.
- O** O'Carroll, E. (2021). [High-energy physics opens its door to the exabyte era](#), Princeton Research Computing, Office of the Dean for Research, Princeton University.
- OECD (2022). [Measuring the value of data and data flows](#), OECD Digital Economy Papers, No. 345, OECD Publishing.
- Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). [The professionalization of risk management: What role can the ISO 31000 risk management principles play?](#), International Journal of Project Management, Volume 34, Issue 8, Pages 1568-1578.
- P** Paljug, K., & Velasquez, V. (2025). [Social media: Definition, importance, top websites, and apps](#), Investopedia.
- Pals, H., & Roso, J.L. (2024). [Data sharing: The key to further digitalization](#), TNO.
- Parry, J. (2025). [The top 10 digital risks for organizations in 2025](#), Control Risks.
- Patel, M., Rajamani, B., Rayner, T., & Rosenberg, W. (2018). [Integrated risk assurance: Get a clearer understanding of the risks affecting business value](#), Deloitte LLP, and affiliated entities.
- Pelgander, L., Öberg, C., & Barkenäs, L. (2022). [Trust and the sharing economy](#), Digital Business 2, 10048, Elsevier.
- Penfold, M. (2022). [Onwards and upwards: Could digital transformation be key to recovery?](#), The Owner Managed Business View in April 2022, Moore.
- Peugeot, V. (2014). [Interview by Bruno Carballa Smichowski](#), in: Smichowski, 2016.
- Pieślak, B., Turkowski, J., & Trachim, A. (2023). [What is a mobile app?](#), itCraft.
- Pillai, R. (2022). [Conducting forward-looking risk assessments](#), Thought Leadership, Institute of Enterprise Risk Practitioners (IERP).
- Pobuda, P. (2020). [The digital twin of economy: Proposed tool for policy design and evaluation](#), Real-world Economics Review, Issue no. 94.
- Pouri, M.J., & Hitty, L.M. (2021). [The digital sharing economy: A confluence of technical and social sharing](#), Research Article, Environmental Innovation and Societal Transitions 38, 127-139.
- Prinsloo, A., & Thompson, P. (2015). [The sharing economy presents challenges and opportunities for the profession](#), International Federation of Accountants (IFAC).
- Pritzker, P., & Gallagher, P.D. (2013). [NIST cloud computing standards roadmap](#), National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Special Publication 500-291, Version 2.
- Publicis Sapient (2025). [3 proven architecture patterns for integrating digital experience platforms](#), Analysis, Publicis Sapient.
- Pugliese, A.J. (2022). [IFRS S1 general requirements for disclosure of sustainability-related financial information](#), Elevating Impact, The Institute of Internal Auditors (IIA).
- R** Rahaman, M. (2023). [Who is considered a service provider?](#), Riseup Labs.
- Räisänen, J., Ojala, A., & Tuovinen, T. (2021). [Building trust in sharing economy: Current approaches and future considerations](#), Journal of Cleaner Production, 279.
- Ransbotham, S. (2015). [Data at the heart of sharing economy: Without analytics](#), neither the business nor its customers know if they're making a good deal, MIT Sloan Management Review.
- Rasouli, M., & Jordan, M. (2021). [Data sharing markets](#), Theoretical Economics, arXiv.2107.08630, Cornell University.
- Red Hat Inc. (RHI) (2025). [What is a CI/CD pipeline?](#), RHI.
- Reid, J. (2024). [Risks of generative artificial intelligence \(GenAI\)-assisted scams on online sharing-economy platforms](#), The African Journal of Information and Communication (AJIC), 33, 1-21.

- Reinsel, D., Gantz, J., & Rydning, J. (2017). **Data age 2025: The evolution of data to life-critical**, An IDC White Paper sponsored by SEAGATE.
- Revelate (2022). **Creating a data sharing business model: Opportunities and benefits**, Blog, Revelate.
- Rhodes, T., Boland, F., Fong, E., & Kass, M. (2010). **Software assurance using structured assurance case models**, Journal of Research of the National Institute of Standards and Technology, Volume 115, Number 3, 209-216.
- Rice, R.E., & Leonardi, P.M. (2014). **Information and communication technology use in organizations**, The Sage Handbook of Organizational Communication.
- Richter, H., & Slowinski, P.R. (2018). **The data sharing economy: On the emergence of new intermediaries**, Article, IIC, Springer.
- Rietschoten, M. van, Schmidt, P., & Kleef, J. van (2022). **Compliance assurance: How do you stay in control of your compliance processes?**, Compact, Publication 2022/4.
- Ritvo, S.E., & Alison, R.S. (2017). **Designing for the exceptional user: Nonhuman animal-computer interaction (ACI)**, Computers in Human Behavior, Volume 70, Pages 222-233, Elsevier.
- Rojanakit, P., Torres de Oliveira, R., & Dulleck, U. (2022). **The sharing economy: A critical review and research agenda**, Journal of Business Research, Volume 139, 1317-1334, Elsevier.
- Romney, M.B., Steinbart, P.J., Summers, S.L., & Wood, D.A. (2021). **Accounting information systems**, Fifteen Edition, Global Edition, Pearson Education Limited.
- Ronthal, A., & Feinberg, D. (2023). **The impact of data ecosystems: A cloud architectural perspective**, Gartner Research, Gartner.
- RSA (2020). A how-to guide to managing digital risk today, RSA.
- RTLS Solutions (RTLS) (2024). **The best digital twin in a shared economy**, Ripples.
- Russom, P. (2011). **Big data analytics**, TOWI Best Practices Report, Fourth Quarter, TOWI Research.
- S** Sabitzer, T., Hartl, B., Marth, S., Hofmann, E., & Penz, E. (2018). **Preventing conflicts in sharing communities as a means of promoting sustainability**, Article, MDPI.
- SAP Business Technology Platform (SAP) (2025). **What is process automation?**, SAP.
- Scelta, G., LaFleur, M.T., Cheng, H.W.J., & Parra-Lancourt, M. (2019). **Data economy: Radical transformation or dystopia?**, Frontier Technology Quarterly, ResearchGate.
- Schaefers, T., Narayanamurthy, G., Moser, R., & Leban, M. (2021). **The sharing economy at the base of the economic pyramid: How access-based services can help overcome ownership risks**, Psychology & Marketing, Wiley Periodicals LLC.
- Schneider, H. (2022). **The value of data**, Economy, GIS.
- Schou, C., & Hernandez, S. (2015). **Information assurance handbook: Effective computer security and risk management strategies**, McGraw-Hills Education.
- Schussel, G. (2001). **Client/server: Past, present, and future**, Digital Consulting Inc.
- Scott, G., & Munichello, K. (2024). **Sharing economy: Model defined, criticism, and how it's evolving**, Investopedia.
- Sedkaoui, S., & Khelfaoui, M. (2020). **Sharing economy and big data analytics**, Information Systems, Web, and Pervasive Computing Series, ISTE Ltd.
- SentinelOne (Sentinel) (2025). **What is software assurance? Key components of cybersecurity**, Sentinel.
- Sestino, A., Kahlawi, A., & De Mauro, A. (2023). **Decoding the data economy: A literature review of its impact on business, society and digital transformation**, European Journal of Innovation Management, ISSN: 1460-1060.
- SG:D, Infocom Media Development Authority (IMDA), & Personal Data Protection Commission (PDPC) (IMDA) (2019). **Trusted data sharing framework**, IMDA and PDPC.
- Shahim, A. (2005). **A new era without data warehouses, An architectural vision**, Sdu Uitgevers bv, Den Haag.
- Shahim, A. (2010). **Economics of IT assurance**, Nederlandse Orde van Register EDP Auditors (NOREA).
- Shahim, A. (2021). **IT auditing and assurance: An introduction**, School of Business and Economics (SBE), Vrije Universiteit (VU) Amsterdam.
- Shahim, A. (2009). **IT governance attestation: In search of proving compliance**, Academic Service, Sdu Uitgevers, Den Haag.
- Shahim, A. (2017). **Think technology: Towards an orientation of IT auditing**, School of Business and Economics, School of Business and Economics, Vrije Universiteit (VU) Amsterdam.
- Shahim, A., Rahali, A., & Van Praat, J. (Eds.) (2024). **Research in big data and AI: An IT audit and advisory perspective**, Vrije Universiteit Amsterdam SBE, Amsterdam, The Netherlands.
- Shakoor, Z. (2024). **Data fabric: A complete guide – Architecture**, benefits and implementation, Astera.

- Sheehan, N.T. (2010). **A risk-based approach to strategy execution**, Journal of Business Strategy, Vol. 31, No. 5.
- Sherinsky, J.M. (2010). **Replacing SAS 70: New standards for engagements involving outsourcing**, Journal of Accountancy, The Association of International Certified Professional Accountants.
- Shmidt, M. (2023). **Sharing economy as a field: Revisiting debates and introducing new research avenues**, Review Article, Department of Sociology, Uppsala University, Uppsala, Sweden, John Wiley & Sons Ltd.
- Simic, V., & Liem, A. (2023). **The sharing economy's success: Advantages, drawbacks, and applications**, International Conference on Engineering Design (ICED) 23, 24-28 July, Bordeaux, France.
- Simon, H. (2022). **A guide to risk management**, Risk Guide.
- Small Business Commissioner (SBC) (2023). **Social media and digital platforms: Balancing opportunities and risks**, SBC.
- Smichowski, B.C. (2016). **Data as a common in the sharing economy: A general policy proposal**, HAL Id: hal-01386644, HAL Open Science.
- Smit, S., Condon, J., & Kwiatkowski, K. (2024). **Economic conditions outlook**, December 2024, Strategy & Corporate Finance Practice, McKinsey & Company.
- Smith, M. (2024). **What is datafication, and how is it beneficial for businesses?: Transforming data into strategic assets for enhanced decision-making and innovation**, Medium.
- Smith, S., & Heijden, H. van der (2017). **Analysts' evaluation of KPI usefulness, standardization and assurance**, Journal of Applied Accounting Research 18 (1), 63-86.
- Soller, H. (2023). **Bringing digital to risk management: An interview with Mark Cooke**, McKinsey Digital, McKinsey & Company.
- Stiglich, L. (2021). **Policy to unlock the economic value of data**, Blog, Open Data Institute.
- Strategic Risk (STRI) (2018). **Managing the risks of the on-demand and sharing economies**, STRI.
- Stryker, C. (2024). **What is advanced analytics?**, IBM.
- Stulz, R.M. (2008). **Risk management failures: What are they and when do they happen?**, Journal of Applied Corporate Finance, A Morgan Stanley Publication, Volume 20, Number 4.
- Sun, R., Gregor, S., & Felt, E. (2021). **Generativity and the paradox of stability and flexibility in a platform architecture: A case of the Oracle Cloud Platform**, Information & Management, Volume 58, Issue 8, 103548.
- Superhog (2024). **San Francisco Airbnb laws**, Superhog.
- Sutherland, W., & Jarrahi, M.H. (2018). **The sharing economy and digital platforms: A review and research agenda**, International Journal of Information Management, Volume 43, 328-341.
- Swaminathan, A., Gnanasambandam, C., Carson, B., Smaje, K., Santos, L., & Forrest, W. (2024). **What is cloud computing?**, McKinsey Explainers, McKinsey & Company.
- T** Talend, Inc. (2025) (Talend). **Structured vs. unstructured data: A complete guide**, Talend.
- Tamboly, N. (2024). **What is a third party audit?**, Types of IT audits, IT auditor training course, Audit Guru.
- Tarver, E., Kindness, D., & Perez, Y. (2024). **What is C2C? How does the customer-to-customer model work**, Investopedia.
- Täuscher, K. & Kietzmann, J. (2017). **Learning from failures in the sharing economy**, Management Information Systems Quarterly Executive, 16(4): 253–263.
- The AME Group (AMEG) 2025. **A history of IT outsourcing**, AME Group.
- The Dutch Authority for Financial Markets (AFM) (2025). **Digital Operational Resilience Act (DORA)**, Digitalization, AFM.
- The Fullstory Team (TFT) (2024). **What is data processing? Definition, steps & methods**, Blog, Fullstory.
- The Institute of Internal Auditors (IIA-) Australia (IIA) (2022). **Integrated assurance**, Factsheet, IIA.
- The Strategy Team (TST) (2025). **What is data fabric and why are businesses using it?**, Strategy.
- Thereaux, O., & Keller, J.R. (2021). **Economic impact of trust in data ecosystems**, Report prepared for the Open Data Institute (ODI), ODI.
- Thilakanathan, D., Chen, S., Nepal, S., & Calvo, R.A. (2014). **Secure Data Sharing in the Cloud**, Security, Privacy and Trust in Cloud Systems, DOI: 10.1007/978-3-642-38586-5_2, Springer-Verlag Berlin Heidelberg.
- Thomas, E. (2024). **AI is aiding the growing sharing economy**, Verdict.
- Thomas, G. (2023). **How to do your research project: A guide for students**, 4th Edition, SAGE Publications Ltd.

- Thomas, J.J. (2014). **Understanding mainframe economics**, An IBM Redbooks Point-of-View Publication, IBM Corp.
- Thykatt, R. (2025). **The human side of risk: Talent shortage as an emerging risk factor**, Infosys BMP.
- Truvera. (2025). **Self-sovereign identity: The ultimate guide 2024**, Truvera.
- Turban, E., & Volonino, L. (2010). **Information technology for management: Transforming organizations in the digital economy**, International Student Version, 7th Edition, John Wiley & Sons (Asia) Pte Ltd.
- Turban, E., Poland, C., & Wood, G. (2021). **Information technology for management: Driving digital transformation to increase local and global performance, growth and sustainability**, Twelfth Edition, International Adaption, John Wiley & Sons, Hoboken, New Jersey.
- Turner, L., Weickgenannt, A.B., & Copeland, M.K. (2023). **Accounting information systems: Controls and processes**, Fifth Edition, John Wiley & Sons, Inc.
- Twizeyimana, J.D., & Andersson, A. (2019). **The public value of e-government: A literature review**, Government Information Quarterly 36 (2019), 167-178, Elsevier.
- U** Uber Technologies Inc. (Uber) (2025). **Health insurance marketplace for driving rewards**, Uber.
- Umami, N., Amelia, S., & Sulistiani, H. (2023). **Digital economy opportunities and challenges in the era of connection**, the 4th International Conference on Information Technology and Security (IC-ITECHS): Leveraging technology for effective e-learning, E-ISSN: 2580-7234, P-ISSN: 2356-4407.
- V** Vallone, S.K., & Frimpong, E. T. (2023). **State of cyber awareness in the boardroom**, Harvard Law School Forum on Corporate Governance.
- Vasarhelyi, M.A., Alles, M.G., & Kogan, A. (2018). **Principles of analytical monitoring for continuous assurance**, ISBN: 978-1-78743-414-1.
- Verizon (2024). **WiFi**, Verizon.
- Vesselkof, A., Hämmäinen, H., & Töyli, J. (2019). **Design and governance of mHealth data sharing**, Communications of the Association for Information Systems, Volume 45, ISSN: 1529-3181.
- Vidya (2024). **Data quality assurance 101: Elevate your data strategy with reliable solutions**, Data quality & Reliability, Acceldata.
- Virtusa Corp. (Virtusa) (2025). **Platform assurance: Leveraging partner solutions to enable high-quality release orchestration**, Virtusa.
- Vitasek, K. (2024). **5 timeless ways to build a trustworthy reputation for your business**, Forbes.
- W** Wall Bake, A. van den, & Pals, H. (2024). **Self-sovereign identity: A simple and safe digital life**, TNO.
- Walsh, N., & Evans, P. (2018). **Squaring risk in the sharing age: How the collaborative economy is reshaping insurance products**, Innovation Report, Lloyd's.
- Watts, S. (2023). **Service assurance for IT, telecom, & cloud**, Splunk.
- Wiese, S. (2020). **Sharing in an urbanised world**, Dinolift Oly.
- William.tc (William) (2023a). **Convergence of risk and data management: A data-driven risk management**, Medium.
- William.tc (William) (2023b). **Data-driven risk management in action: Illuminating insights from real-world case studies**, Medium.
- Winniford, M.A., Conger, S., & Erickson-Harris, L. (2009). **Confusion in the ranks: IT service management practice and terminology**, Information Systems Management, 26: 153-163.
- Wisconsin Office of the Commissioner of Insurance (WOCI) (2024). **Share with care: Understanding the insurance risks of the sharing economy**, FAQ Sheet, PI-235, WOCI.
- Wolford, B. (2025). **What is GDPR, the EU's new data protection law?**, GDPR.EU.
- World Economic Forum (WEF) (2024). **5 cybersecurity risks posed by emerging technology – and how we can defend against them**, Cybersecurity, WEF.
- Worm, D. (2024). **Secure multi-party computation**, TNO.
- Wynn, R. (2023). **Big data, big risks: How startups can safeguard their customers' information**, Forbes Technology Council.
- X** Xiao, J. (2021). **Information security management of sharing economy based on blockchain technology**, Hindawi Wireless Communications and Mobile Computing, Volume 2021, Article ID 9931460, Wiley.
- Y** Yates, D., Allen, L., Evans, E., Tennison, J., Szasz, D., & Wilson, R. (2022). **Assessing risk when sharing data: A guide**, Open Data Institute (ODI).

- Zaidi, E. (2023). **Data and analytics essentials: how to define, build and operationalize a data fabric**, Gartner Research, ID G00790376, Gartner.
- ZenBit Tech (Zen) (2024). **Trends in cloud computing development in 2024**, Medium.
- Zenya (2021). **Information quality assurance and secure document sharing**, Zenya.
- Zerlang, J. (2022). **The pandemic's lasting effects: Are cyber attacks one of them?**, Forbes Technology Council, Forbes.
- Zhang, J. (2022). **A history of bicycle mobility in urban China: Shared bikes, technology, and infrastructure** (part 2 of 2), The Mobility Technology and Wellbeing Lab (MoLab) Max Planck Institute for Social and Anthropology, Inventory of Mobilities and Socioeconomic Changes.
- Zhang, P., & Melguizo, A. (2022). **Data 4.0: Rethinking rules for a data-driven economy**, World Economic Forum (WEF).
- Zhang, T.C., Gu, H., & Farboudi Jahromi, M. (2019). **What makes the sharing economy successful? An empirical examination of competitive customer value propositions**, Computers in Human Behavior, Volume 95, 275-283, Elsevier.
- Zhang, Y., Pinkse, J., & McMeekin, A. (2019). **Governance of sharing economy organizations: Exploring social bonding and economic transaction**, Academy of Management Proceedings.
- Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2021). **Raising Awareness about cloud security in industry through a board game**, Information, 12, 482, MDPI.
- Zhu, S. (2022). **Managing the risks of peer-to-peer goods sharing**, Law, Technology and Humans, Volume 4 (2).
- Zimmermann, H.D. (2000). **Understanding the digital economy: Challenges for new business models**, Institute for Media, and Communication Management (MCM-HSG), University of St. Gallen.
- Zweers, J., Shahim, A., & Henriks, H. (2022). **Pooled audits op public clouddiensten: Assurance op naleving van de EBA-richtlijnen**, IT Audit, Compliance and Advisory Program, Vrije Universiteit (VU) Amsterdam and Rabobank.

Appendix A. Research methodology

A literature review was employed to address the formulated research question that was informed by a straightforward approach. It consisted of four main phases depicted in figure 10 which are concisely described here. Among other purposes, these gradual steps were designed to focus on and inspect the scholarly as well as practitioner writings (e.g., peer-reviewed research papers, university publications, executive insight journals, and magazines for professionals) that were directly related to the subject matter. The first phase, initiation, was about formulating the research question, defining its objective, and creating a protocol to structurally start the investigation. Execution, the second phase, was concerned with establishing the formal review criteria, searching for the specific material, and studying this literature extracted from the different sources mentioned above. In the third phase, verification, few board members and experts were selected, the initial findings and results were checked with them, and their comments and insights were collected. The fourth and last phase, completion, analyzed these externally gathered inputs, consolidated them, and drew final conclusions, and issued the developed report after which the research was closed.

Figure 10. Research methodology



Appendix B. List of acronyms

An overview of the abbreviations used in this book is presented in table 8.

Table 8. Acronyms

AI	Artificial Intelligence	ICT	Information and Communication Technology
AICPA	Association of International Certified Professional Accountants	IDSA	International Data Spaces Association
AIS	Association for Information Systems	IMDA	Infocom Media Development Authority
AISeL	AIS Electronic Library	IoT	Internet of Things
AMCIS	Americas Conference on Information Systems	IP	Internet Protocol
API	Application Programming Interface	ISAE	International Standard on Assurance Engagements
B2B	Business-to-Business	ISAM	Indexed Sequential Access Method
B2C	Business-to-Consumer	ISO	International Organization for Standardization
B2G	Business-to-Government	ITACA	IT Audit, Compliance and Advisory
BI	Business Intelligence	ITSM	IT Service Management
C2B	Consumer-to-Business	KCI	Key Compliance Indicator
C2C	Consumer-to-Consumer	KPI	Key Performance Indicator
C2G	Consumer-to-Government	KRI	Key Risk Indicator
CA	Continuous Assurance	KSI	Key Security Indicator
CAGR	Compound Annual Growth Rate	LED	Law Enforcement Directive
CI/CD	Continuous Integration/Continuous Deployment	MECS	Modern Education and Computer Science
CIMA	Chartered Institute of Management Accountants	ML	Machine Learning
CIPL	Centre for Information Policy Leadership	MoLab	The Mobility Technology and Wellbeing Lab
CoE-DSC	Centre of Excellence for Data Sharing and Cloud	MPC	Multi-Party Computation
COSO	Committee of Sponsoring Organizations of the Treadway Commission	MSR	Maconachy-Schou-Ragsdale
CRM	Customer Relationship Management	NIS2	Network and Information Systems Directive 2022/2555
CSP	Cloud Service Provider	NIST	National Institute of Standards and Technology
DLM	Data Lifecycle Management	OLTP	Online Transaction Processing
DMA	Digital Markets Act	P2B	Platform-to-Business
DORA	Digital Operational Resilience Act	P2C	Platform-to-Consumer
DPP	Digital Product Passport	PaaS	Platform as a Service
DQA	Data Quality Assurance	PC	Personal Computer
DSA	Digital Services Act	PDPC	Personal Data Protection Commission
DSG	Data Space Governance	PESTLE	Political, Economic, Sociological, Technological, Legal and Environmental
DSSC	Data Spaces Support Centre	PET	Privacy Enhancing Technology
ECC	ERP Central Component	RPA	Robotic Process Automations
EHDS	European Health Data Space	SaaS	Software as a Service
ELT	Extract, Load, and Transform	SAS 70	Statement on Auditing Standards No. 70
ERM	Enterprise Risk Management	SCM	Supply Chain Management
ERP	Enterprise Resource Planning	SDLC	Software Development Life Cycle
ETL	Extract, Transform and Load	SMAC	Social, Mobile, Analytics, Cloud
FSA	Financial Statement Audit	SNA	Systems Network Architecture
FTP	File Transfer Protocol	SOC	System and Organization Controls
G2B	Government-to-Business	SOX	Sarbanes-Oxley
G2C	Government-to-Consumer/Government-to-Citizens	SQL	Structured Query Language
G2G	Government-to-Government	SSI	Self-Sovereign Identity
GDPR	General Data Protection Regulation	TCP/IP	Transmission Control Protocol/Internet Protocol
GITC	General IT Control	TPA	Third Party Audit
GPS	Global Positioning System	TSC	Trust Services Criteria
HPC	High Performance Computing	VU	Vrije Universiteit
HRM	Human Resource Management	Wi-Fi	Wireless Fidelity
HTTP	Hyper Text Transfer Protocol	XAI	Explainable AI
IaaS	Infrastructure as a Service		
ICFR	Internal Control over Financial Reporting		

Appendix C. Glossary

Here, the definitions of some relevant terms directly connected to the subject of this book are presented.

Access – Opportunity to make use of an information system resource (Schou & Hernandez, 2015).

Accounting – The systematic and comprehensive recording of an organization's financial transactions, including summarizing, analyzing, and reporting these transactions to all users (Romney et al., 2021).

Advanced analytics – A collection of sophisticated techniques and tools that are used to analyze large volumes of data, uncover hidden patterns, and provide actionable insights (Stryker, 2024).

Agility – Being able to respond quickly (Turban et al., 2021).

Alignment – Positioning or arrangement of elements in a specific order or configuration. In the context of technology, computing, programming, and communications, alignment often refers to the arrangement of text, images, or other objects on a digital platform. It determines how these elements are positioned relative to each other and how they are presented to the user (Lenovo, 2025).

Application – Software program that performs a specific function directly for a user and executed without access to system control, monitoring, or administrative privileges (Schou & Hernandez, 2015).

Application programming interface – A software component that facilitates the interaction with other software components and enables them to share data (EU, 2018).

Architecture – A style or method of design and construction; an orderly arrangement of parts (Hammergren, 1996).

Artificial intelligence – A machine's ability to perform some cognitive functions we usually associate with human minds (Blumberg et al., 2024).

As-a-service – With this delivery model, the need for costly, protracted implementations is shifted to subscription-based technology designed to reduce upfront IT spend, enhance client flexibility, as well as give access to the latest technologies. All this is accomplished while the as-a-service provider maintains their infrastructure entirely. Cloud helped create the foundation for this service model (CSCi, 2019).

Assertion – Representations, explicit or otherwise, with respect to the recognition, measurement, presentation, and disclosure of information in the financial statements which are inherent in management representing that the financial statements are prepared in accordance with the applicable financial reporting framework. Assertions are used by the auditor to consider the different types of potential misstatements that may occur when identifying, assessing, and responding to the risks of material misstatement (IAASB, 2019).

Asset – Any tangible or intangible thing that has value to an organization (Schou & Hernandez, 2015).

Assurance engagement – Engagements in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users (other than the responsible

party) about the outcome of the evaluation or measurement of a subject matter against criteria (Hayes et al., 2024).

Attributes – The properties, identifying numbers, and characteristics of interest of an entity stored in a database. Examples are employee number, pay rate, name, and address (Romney et al., 2021).

Audit – A systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between these assertions and established criteria and communicating the results to interested users (Hayes et al., 2024).

Authentication – The process of validating the identity provided by a user (Schou & Hernandez, 2015).

Authorization – The process of restricting access of authenticated users to specific portions of the systems and limiting what actions they are permitted to perform (Romney et al., 2021).

Availability – A condition in which information or processes are reasonably accessible and usable by an authorized party and are timely and critical (Schou & Hernandez, 2015).

Back-office operations – They support accounting, inventory management, and shipping processes in the fulfillment of orders (Turban et al., 2021).

Batch processing – Occurs when data is collected over a period of time and processed together at a predetermined time, such as hourly, daily, or weekly (Turban et al., 2021).

Business to business – A form of transaction between businesses such as a manufacturer and wholesaler or a wholesaler and a retailer (Chen et al., 2024).

Business to consumer – The process of selling products and services directly between a business and consumers who are the end-users of its products or services (Kenton et al., 2024a).

Business to government – The sale and marketing of goods and services to federal, state, or local agencies (Kenton et al., 2024b).

Big data – A group of data from conventional and digital bases inside/outside the enterprise that characterizes a basis for continuing detection and analysis (Alwan & Ku-Mahamud, 2020).

Big data analytics – Where advanced analytic techniques operate on big data (Russom, 2011).

Blockchain – By and large, blockchain is treated as a conveyed record to store social insurance related information for allocation, trading, dissecting, footage, and affirming purposes among accomplices. The advantage of blockchain databases versus traditional dispersed databases is that they are decentralized, permanent, and perfected with advanced digital payment frameworks and hash chain occasion structure. The blockchain code is an unlocked resource and can be utilized, altered, and customized by its clients (Ahmad et al., 2019).

Blueprint – A consistent, coherent, and comprehensive set of guidelines to support the implementation, deployment, and maintenance of data spaces (DSSC, 2024c).

Building block – A description of related functionalities and/or capabilities that can be realized and combined with other building blocks to achieve the overall functionality of a data space (DSSC, 2024c).

Business Intelligence – A set of tools and techniques for acquiring and transforming raw data into meaningful and useful information for business analysis purposes in the form of reports, dashboards, or interactive visualizations (Turban et al., 2021).

Business model – A company's core strategy for making a profit. It defines the products and/or services it will sell, its target market, costs associated with doing business and the company's ongoing plans for achieving its goals (Turban et al., 2021).

Business process – A prescribed sequence of work steps performed to produce a desired result for the organization. A business process is initiated by a particular kind of event and has a well-defined beginning and end (Turner et al., 2023).

Business risk – A risk resulting from significant conditions, events, circumstances, actions, or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies (IAASB, 2019).

Business strategy – Sets the overall direction of an organization and defines how it will achieve its mission, vision, and organizational goals (Turban et al., 2021).

Consumer to business – A commerce model where consumers provide various products or services to businesses. Through the C2B model, businesses obtain information from their consumers to produce high-quality goods and services (Diaz, 2023).

Consumer to consumer – A business model whereby customers can trade with each other, typically in an online environment (Tarver et al., 2024).

Consumer to government – A way for individuals to interact with government. For example, a taxpayer requests a refund for the amount that might be overpaid through the Tax Department website (Bloomenthal et al., 2024).

Chatbot – A program or application that users can converse with using voice or text usually for sales or customer service support online. The bots simulate human conversation and attempt to answer queries before passing them on to a human representative (AWS, 2024).

Cloud computing – Cloud computing allows companies to store their infrastructures remotely via the internet, ultimately reducing costs and creating value (Swaminathan et al., 2024).

Cloud services – Services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider (EBA, 2019).

Cloud service provider – A company that offers some components of cloud computing (DiMaria, 2020).

Common European data spaces – Sectoral/domain-specific data spaces established in the European single market with a clear EU-wide scope that adheres to European rules and values (DSSC, 2024a).

Community cloud – Cloud infrastructure that is available for the exclusive use by a specific community of organizations, including several organizations of a particular group (EBA, 2019).

Confidentiality – Assurance that information is not disclosed to unauthorized individuals, processes, or devices. This is the condition in which sensitive data is protected and disclosed to authorized parties only, such as by using encryption disclosed or other methods (Schou & Hernandez, 2015).

Consent – Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (DSSC, 2024a).

Context analysis – Understand the situational, technical, physical, organizational, cultural and social settings where the systems will be used (Ritvo & Alison, 2017).

Continuous assurance – An approach used to assess the effectiveness of business process controls on an ongoing basis through analysis and the use of technology. This includes analyzing large volumes of data to provide control assurance on the entire population and closer to the occurrence of transactions. The objective of the audit was to assess the effective (Saskatoon, 2023).

Continuous auditing – A methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a brief time after, the occurrence of events underlying the subject matter (Coderre, 2005).

Continuous integration/Continuous deployment pipeline – A series of established steps that developers must follow in order to deliver an updated version of software. CI/CD pipelines are a practice focused on improving software delivery throughout the software development life cycle via automation (RHI, 2025).

Continuous monitoring – A process by which online and real-time systems are used to manage the performance of corporate processes, on (or close to) a real-time basis. Continuous monitoring typically results in a timely detection of significant variances from expected performance with resulting rapid intervention and corrective action (AICPA, 2015).

Control – Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance (IAASB, 2019).

Corporate governance – A set of rules, practices, and processes used to direct and control an organization. Boards of directors are the primary force determining corporate governance. Accounting, transparency, fairness, and responsibility are the four fundamental principles of corporate governance (Byrne, 2025).

Crowdsourcing – A collaborative way of working/collaborative work involving multiple contributions channeled via internet platforms (EU, 2018).

Customer experience – Describes the cumulative impact of multiple interactions over the course of a customer's contact with an organization (Turban et al., 2021).

Cyber security – Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (NIST, 2025).

Dashboard – Interactive real-time display of key indicators of operating performance (Romney et al., 2021).

Data – Recorded information in structured or unstructured formats, including text, images, sound, and video. The term data is also used to refer to Internet Protocol (IP) traffic or the volume of digitized information stored on servers and other hardware (OECD, 2022).

Data-as-a-service – An information provision and distribution model in which data files (including text, images, sounds, and videos) are made available to customers over a network by a service provider (Turban et al., 2021).

Data assurance – The process, or set of processes, which increase confidence that data will meet a specific need, and that organizations collecting, accessing, using, and sharing data are doing so in trustworthy ways (Baker, 2023).

Database – Repository of enterprise data that business applications create or generate, such as sales, accounting, and employee data. An organized logical grouping of related files (Turban & Volonino, 2010).

Datafication – The process of converting human actions, social relations, and everyday interactions into quantifiable data that can be tracked, analyzed, and used for various economic or political purposes (Mejias & Couldry, 2019).

Data act – A European regulation that establishes European Union (EU-) wide rules for access to the product or related service data to the user of that connected product or service. The regulation also includes essential requirements for the interoperability of data spaces (Article 33) and essential requirements for smart contracts to implement data sharing agreements (Article 36) (DSSC, 2024a).

Data altruism – The voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest (DSSC, 2024a).

Data analytics – Use of software and algorithms to find and solve problems and improve business performance (Romney et al., 2021).

Database – Collection of datasets or records stored in a systematic way (Turban et al., 2021).

Data broker – A company that aggregates data from a variety of sources, cleanses and/or analyses them to license these data to interested companies (EU, 2018).

Data catalogue – The place where an organization's data assets are listed in detail. It is built to aid data specialists to identify the best data for any analytical or commercial objective, making use of metadata to build a thorough and searchable inventory of all data assets within an organization (Kiourtis et al., 2023).

Data center – A facility containing mission-critical information systems and components that deliver data and IT services to the enterprise (Turban & Volonino, 2010).

Data concatenation – The combining of data from two or more fields into a single field (Romney et al., 2021).

Data deception – A graphical depiction of information, designed with or without an intent to deceive, that may create a belief about the message and/or its components, which varies from the actual message (Romney et al., 2021).

Data deduplication – These processes remove duplicates and standardize data formats (Turban et al., 2021).

Data democratization – An enterprise's capability to motivate and empower a wider range of employees — not just data experts — to understand, find, access, use, and share data in a secure and compliant way (Lefebvre et al., 2023).

Data discovery – The process of using BI to collect data from various databases and consolidate it into a single source that can be easily and instantly evaluated (Turban et al., 2021).

Data ecosystem – A cohesive data management environment that supports the entire range of data workloads, from operational and transactional data to exploratory data science and production data warehousing. Built on the foundation of the data fabric, data ecosystems have a common governance and metadata management framework, provide unified access management, and integrate augmented data management capabilities with a set of services accessible by the business user. Data ecosystems leverage distributed components that may run on multiple clouds and/or on-premises but are treated as a logical whole. This makes it easier to meet new requirements, increase productivity and thus return on investment (Ronthal & Feinberg, 2023).

Data ethics – The branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (e.g., right conducts or right values) (Floridi & Taddeo, 2016).

Data exchange – The problem of transforming data that is structured under a source schema into data structured under another schema, called the target schema, so that both the source and target data satisfy the relationship between the schemas (Golshanara & Chomicki, 2020).

Data fabric – A data management design concept for attaining flexible, reusable, and augmented data pipelines and services in support of various operational and analytics use cases. Data fabrics support a combination of different data integration styles, and utilize active metadata, knowledge graphs, semantics and machine learning to augment data integration design and delivery (Zaidi, 2023).

Data flow – The movement of data among processes, stores, sources, and destinations (Romney et al., 2021).

Data governance – The overall management of the availability, usability, integrity, and security of data used in an enterprise (Turban et al., 2021).

Data Governance Act – A European regulation that aims to create a framework to facilitate European data spaces and increase trust between actors in the data market. The act entered into force in June 2022 and applies from September 2023. It defines the European Data Innovation Board (EDIB) (DSSC, 2024a).

Data holder – A legal person, including public sector bodies and international organizations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data (DSSC, 2024a).

Data imputation – The process of replacing a null or missing value with a substituted value (Romney et al., 2021).

Data integrity – Maintenance of data accuracy and validity over its lifecycle including the prevention of unintended modification or corruption (Turban et al., 2021).

Data intermediation service – A service that is legally defined in the Data Governance Act and enforced by national agencies. An operator in a data space may qualify as a data intermediation service provider, depending on the scope of the services (DSSC, 2024a).

Data lake – A single store of structured, semi-structured, and unstructured enterprise data stored in its natural format (Turban et al., 2021).

Data lake house – A popular infrastructure choice. It combines the best data warehouses and data lakes, offering an open architecture that combines the flexibility and scale of data lakes with the management and data quality of data warehouses (MIT, 2023).

Data latency – The elapsed time (or delay) between when data is created and when it is available for a query or report can significantly impact database performance (Turban et al., 2021).

Data lifecycle management – A series of five phases (i.e., a) data creation, b) data storage, c) data sharing and usage, d) data archival, and e) data deletion) over the course of the useful life of data. Each phase is governed by a set of policies that maximizes the data's value during each stage of the life cycle. DLM becomes increasingly important as the volume of data that is incorporated into business workstreams grows (IBM, 2025).

Data literacy – The ability to read, write and communicate data in context, including an understanding of data sources and constructs, analytical methods and techniques applied, and the ability to describe the use-case application and resulting value (Duncan, 2022).

Data management – The management of the flow of data from creation and initial storage to the time when the data becomes obsolete and is deleted (Turban et al., 2021).

Data marketplace – A multi-sided platform that matches data providers and buyers. It facilitates business data sharing among enterprises. Key actors providing data marketplace functionalities include owners, operators, and third-party providers (Abbas et al., 2021).

Data mashup – The integration of two or more data sets from various business systems and external sources without relying on the middle step of ETL into a data warehouse or help from ETL (Turban et al., 2021).

Data model – An abstract representation of database contents (Romney et al., 2021).

Data poisoning attack – It occurs when threat actors inject malicious or corrupted data into these training data sets, aiming to cause the AI model to produce inaccurate results or degrade its overall performance (Hassan, 2024).

Data pooling – The process of combining data from multiple sources to create a larger and more comprehensive dataset (Michalsons, 2023).

Data processing – The series of operations performed on data to transform, analyze, and organize it into a useful format for further use (TFT, 2024).

Data product – A data sharing unit, bundling resources (data and/or data services) and metadata that describes the license terms, the resources, and other information in a machine-readable way (DSSC, 2024c).

Data provenance – The historical record of data that details data's origins by capturing its metadata as it moves through various processes and transformations. Data provenance is primarily concerned with authenticity, providing details such as who created the data, the history of modifications and who made those changes (Mucci, 2024b).

Data quality assurance – The systematic process of ensuring that data meets defined quality criteria. This involves various techniques and practices aimed at improving data accuracy, completeness, consistency, and reliability. High-quality operational and reporting data is crucial for making informed business decisions, optimizing operations, and maintaining regulatory compliance (Alation, 2024).

Data recipient – A natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law (DSSC, 2024a).

Data re-use – The process by which a company re-uses data from another company, which is not a direct market competitor, for its own business purposes (excluding contractor-subcontractor relationships). These data were either accessed for free or acquired against some remuneration or other kind of compensation, including the provision of a service (EU, 2018).

Data science – A multidisciplinary field that uses domain expertise, methods, programming skills, algorithms, and statistics to extract knowledge and insights from structured, semi-structured and unstructured big data sets to predict future behavior and prescribe actions (Turban et al., 2021).

Data security – The protection of data from malicious or unintentional corruption, unauthorized modification, theft, or natural causes such as floods. The purpose of data security is to maintain data integrity (Turban et al., 2021).

Data service – A collection of operations that provides access to one or more datasets or data processing functions. For example, data selection, extraction, data delivery (DSSC, 2024c).

Data sharing – The provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licenses subject to a fee or free of charge (DSSC, 2024a).

Data silo – Stand-alone data stores. Their data is not accessible by other information systems that need it outside that department (Turban et al., 2021).

Data source – The entity that produces or sends the data entered a system (Romney et al., 2021).

Data sovereignty – The ability of individuals, organizations, and governments to have control over their data and exercise their rights on the data, including its collection, storage, sharing, and use by others (DSSC, 2024a).

Data space – It is considered as an umbrella term encompassing any ecosystem of data models, datasets, ontologies, data sharing contracts, and specialized management services (i.e., as often provided by data centers, stores, repositories, individually, or within a data lake), together with soft competencies around it (i.e., governance, social interactions, business processes) (Bacco et al., 2024).

Data space governance authority – The body of a particular data space, consisting of participants that is committed to the governance framework for the data space, and is responsible for developing, maintaining, operating, and enforcing the governance framework (DSSC, 2024g).

Data space infrastructure – A technical, legal, procedural, and organizational set of components and services that together enable data transactions to be performed in the context of one or more data spaces (DSSC, 2024g).

Data space interoperability – The ability of participants to seamlessly exchange and use data within a data space or between two or more data spaces (DSSC, 2024g).

Data subject – it an identified or identifiable natural person that personal data relates to (DSSC, 2024a).

Data supplier – A company that holds data (either self-generated, collected or acquired from others with sub-licensing rights) and makes them available to other companies which are neither direct market competitors nor sub-contractors. This company represents the supply side of the data market (EU, 2018).

Data transaction – Any kind of exchange in a business context in which data are the key trading element (EU, 2018).

Data utilization – The process of continuously using data to achieve improved business outcomes like higher productivity and profitability (Naqvi, 2025).

Data user – A company that re-uses data from other companies, which are neither its direct market competitors nor contractors, by analyzing or exploiting the data to improve or develop its own business. This company represents the demand side of the data market (EU, 2018).

Data value – The actual value stored in a field. It describes a particular attribute of an entity. For example, the customer's name field would contain "ZYX Company" if that company was a customer (Romney et al., 2021).

Data volume – The amount of data created and stored by an organization (Romney et al., 2021).

Data warehouse – A data warehouse is a subject oriented, integrated, non-volatile and time variant collection of data in support of management's decisions (Inmon, 1996).

DevOps model – The combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes. This speed enables organizations to better serve their customers and compete more effectively in the market (AWS, 2025).

Digitalization – The process of transforming any kind of activity or information into a digital format that can be collected, stored, searched, and analyzed electronically and efficiently (Turban et al., 2021).

Digital identity – Any data existing online that can be traced back to an individual or organization. Identifiable data includes passwords, usernames, bank accounts, and social media photos (Truvera, 2025).

Digital operational resilience act – It addresses a critical gap in EU financial regulation. Prior to DORA, financial institutions primarily managed operational risks by allocating capital to cover potential losses. This approach failed to encompass all aspects of operational resilience, particularly in relation to ICT (DORA.com, 2025).

Digital transformation – The rewiring of an organization, with the goal of creating value by continuously deploying tech at scale. A clear digital transformation strategy focused on specific domains and enabled by a set of specific capabilities is critical for organizations to not only compete but survive. Digital transformations are not a one-and-done project; most executives will be on this journey for the rest of their careers (Lamarre et al., 2024).

Digital twin – A set of virtual information constructs that fully describes a potential or actual physical manufactured product from the micro atomic level to the macro geometrical level. At its optimum, any information that could be obtained from inspecting a physical manufactured product can be obtained from its digital twin (Pobuda, 2020).

Disruption – The process by which a smaller company—usually with fewer resources—moves upmarket and challenges larger, established businesses. In both low-end and new-market disruption, incumbent businesses are motivated by higher profit margins to not fight the new entrant for market share (Cote, 2022).

E-commerce – The buying and selling of goods and services over the internet, on websites, mobile apps, or social media. By optimizing e-commerce as part of a broader digital-commerce transformation, sellers stand to attract more customers and earn more profits (Kim et al., 2025).

E-government – Government's use of ICT combined with organizational change to improve the structures and operations of government. Also, the implementation of e-government is expected to help governments deliver services and transform relations with citizens, businesses, and other arms of government (Twizeyimana & Andersson, 2019).

Enterprise resource planning – An enterprise information system designed to integrate and optimize the business processes and transactions in a corporation (Moon, 2007).

Enterprise risk management – It is a risk-based approach to managing an enterprise developed by COSO (Turban et al., 2021).

Ethics – The values and customs of a particular group that identify what is considered right and what is considered wrong (Turban et al., 2021).

European data innovation board – The expert group established by the Data Governance Act to assist the European Commission in the sharing of best practices, in particular on data intermediation, data altruism and the use of public data that cannot be made available as open data, as well as on the prioritization of cross-sectoral interoperability standards, which includes proposing guidelines for common European data spaces (Data Governance Act Article 30). The European Data Innovation Board (EDIB) will have additional competencies under the Data Act it (DSSC, 2024a).

Explainable artificial intelligence – Given an audience, an Explainable AI is one that produces details or reasons to make its functioning clear or easy to understand (Ali et al., 2023).

Extract, load and transform – A data integration process for transferring raw data from a source server to a data system (such as a data warehouse or data lake) on a target server and then preparing the information for downstream uses (Mullins, 2025).

Extract, transform and load – Data center databases from transaction systems. Data of interest is extracted from databases, transformed into clean and standardized it, and then loaded into a data warehouse. The three processes are called ETL (Turban et al., 2021).

File – A set of logically related records, such as the payroll records of all employees (Romney et al., 2021).

Financial statement audit – In conducting such audit, the overall objectives of the auditors are: 1) to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatements, whether due to fraud or error, thereby enabling the auditor to express an opinion on whether the financial statements are prepared, in all material aspects, in accordance with an applicable financial reporting framework; and 2) to report on the financial statements, and communicate as required by the ISAs in accordance with the auditor's findings (Hayes et al., 2024).

Fintech – Companies that rely primarily on technology and cloud services—and less so on physical locations—to provide financial services to customers (Flötotto et al., 2024).

Government to business – An integral part of e-government that refers to business-specific transactions (such as payments, selling and acquisition of goods and services, etc.) and the provision of business-focused services online (Kushnir, 2023).

Government to consumer – An integral part of e-government that reflects programs meant to make it easier for citizens and consumers of public services to communicate with the government. This covers interactions, including the delivery of public services and participation in consultation and decision-making processes (Kushnir, 2023).

Government to government – An integral part of e-government that involves sharing data and conducting electronic communications between government agencies. This consists of intra- and inter-agency interactions at the national level and exchanges between the national, provincial, and local levels. (Kushnir, 2023).

Generativity – A platform's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences (Sun et al, 2021).

General data protection regulation – The toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros (Wolford, 2025).

General IT control – Controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information processing controls and the integrity of information (i.e., the completeness, accuracy and validity of information) in the entity's information system (IAASB, 2019).

Gig worker – Non-standard or gig work consists of income-earning activities outside of standard, long-term employer-employee relationships (ILR, 2025).

Governance – While governance includes oversight, it is a broader concept. Governance refers to the structures, systems, and practices an organization has in place to: a) assign decision-making authorities, define how decisions are to be made, and establish the organization's strategic direction, b) oversee the delivery of its services; the implementation of its policies, plans, programs, and projects; and the monitoring and mitigation of its key risks, and c) report on its performance in achieving intended results and use performance information to drive ongoing improvements and corrective actions (CAAF, 2024).

Global positioning system – A navigation system using satellites, a receiver, and algorithms to synchronize location, velocity and time data for air, sea, and land travel (Geotab, 2024).

Hybrid blockchain – A type of blockchain technology that combines elements of both private and public blockchain. It lets organizations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored in the blockchain, and what data will be opened up publicly (Campbell, 2024).

Hybrid cloud – Cloud infrastructure that is composed of two or more distinct cloud infrastructures (EBA, 2019).

Information and communication technology – Devices, applications, media, associated hardware, and software that receive and distribute, process and store, retrieve and analyze, digital information, between people and machines (as information) or among people (as communication). In the organizational context, ICT refers to a broad range of computer-based digital systems from transaction and information processing to wired and wireless communication media, connected through internal intranet or external Internet and wireless networks (Rice & Leonardi, 2014).

Information assurance – (1) Technical and managerial controls designed to ensure the confidentiality, possession of control, integrity, authenticity, availability, and utility of information and information systems. (2) Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities (Schou & Hernandez, 2015).

Information processing control – Controls relating to the processing of information in IT applications or manual information processes in the entity's information system that directly address risks to the integrity of information, i.e., the completeness, accuracy and validity of transactions and other information (IAASB, 2019).

Information system – A combination of information technology and people's activities using the technology to support business processes, operations, management, and decision-making at different levels of the organization (Turban et al., 2021).

Infrastructure as a service - The most basic of services and refers not to a machine that does all the work but to a cloud facility where a business has access to extra storage space and data centers. The cloud service provides fundamental computing services (such as a server, storage, and a network as an on-demand service). In this model the cloud user is responsible for maintaining the operating systems and applications software (IFAC, 2018).

Integrated assurance – A way for internal audit and other assurance providers to work together to align their assurance processes so the audit committee and senior management are given insights on governance, risk management and control arrangements from a comprehensive holistic perspective. This helps to provide consistent messaging, is more efficient, provides a common view of risks, and delivers more effective oversight (IIA, 2022).

Integrity – (1) A condition in which data has not been changed or destroyed in an unauthorized way, such that the current state is identical to the original state. (2) A condition exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. (3) Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Schou & Hernandez, 2015).

Interface – To connect and exchange data with apps and systems (Turban et al., 2021).

Internet – The world's largest collection of networks ranging from those of small organizations to those of large corporations, universities, or governments (Schou & Hernandez, 2015).

Internet of things – One of the enabling technologies of the industry 4.0. Its goal is the connection of humans with machines and smart technologies. It refers to the vast interconnected network of computer devices (e.g., sensors) which exchange substantial amounts of data at rapid speed (Gazis, 2021).

Internet protocol – Standard protocol for the transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks (Schou & Hernandez, 2015).

Interoperability – The ability of different systems to work in conjunction with each other and for devices, applications, or products to connect and communicate in a coordinated way without effort from the users of the systems. On a high-level, there are four layers of interoperability: legal, organizational, semantic, and technical (see the European Interoperability Framework (EIF)) (DSSC, 2024g).

Intranet – A computer network like the internet except access is restricted by the intranet's owner, and users must sign into the intranet with a username and password. Many companies create intranets for their employees and business partners (Turban et al., 2021).

ISAE 3000 – A comprehensive standard that applies to non-financial information assurance engagements, which includes environmental, social and governance (ESG), or sustainability, disclosures (IFAC, 2021).

IT environment – The IT applications and supporting IT infrastructure, as well as the IT processes and personnel involved in those processes, that an entity uses to support business operations and achieve business strategies (IAASB, 2019).

IT outsourcing – The practice whereby a client firm contractually uses an external provider (or vendor) to effectively deliver IT or IT-enabled products and services that may previously have been provided using the client's in-house staff (Domberger et al., 2000).

IT outsourcing arrangement – A high-level description of the set of choices the organization makes in crafting its IT outsourcing portfolio (Cullen et al., 2005).

IT services – The application of business and technical expertise to enable organizations in creating, managing, optimizing, and accessing information and business processes (Turban et al., 2021).

IT service management – It focuses on defining, managing, and delivering IT services to support business goals and customer needs. ITSM is broad, encompassing IT planning, delivery, support, and security. In contrast to the traditional technology-oriented approaches to IT operations, ITSM is a discipline for customer-defined, process-oriented IT services, and is a move toward managing IT 'like a business.' ITSM seeks to align IT operations-related activities and the interactions of IT technical personnel with business processes (Winniford et al., 2009).

Key compliance indicators – Benchmarks that measure compliance and forecast risk. They enable banks, credit unions, and other financial institutions to grow sustainably by identifying potential issues and ensuring adherence to laws and regulations (Brosh, 2024).

Key performance indicators – A set of quantifiable measures used to evaluate factors that are critical to the success of an organization (Turban et al., 2021).

Key risk indicators – Metrics capable of showing that the enterprise is, or has a high probability of being, subject to a risk that exceeds the defined risk appetite. They are critical to the measurement and monitoring of risk and performance optimization. These metrics help effectively report risk management performance results (risk communication) to stakeholders and enable management to take informed risk management decisions. While KPIs focus on business performance, KRIs focus on risk management performance (Lingeswara Satyanarayana Tammineedi, 2018).

Key security indicators – Values based on metrics obtained by comparing logically related attributes about the behavior of an activity, process, or control within a specified time. These critical indicators are derived from predefined criteria, and they may be predictive of the overall security posture of an organization. The indicators are guided by security rules and regulations, as determined in policies and standards (Gartner, 2025b).

Knowledge – Adds understanding, experience, accumulated learning, and expertise as they apply to a current problem or activity, to information (Turban et al., 2021).

Legacy systems – They are older information systems that have been maintained over several decades because they fulfill critical needs (Turban et al., 2021).

Machine-generated data – Raw data created without direct human intervention by computer processes, applications, or services, or by sensors processing information retrieved from equipment, software of machinery, whether virtual or real, and with application in a variety of domains. It can be personal or non-personal in nature (EU, 2018).

Machine learning – The field of study that gives computers the ability to learn without being explicitly programmed. It is used to teach machines how to manage the data more efficiently. Sometimes after viewing the data, we cannot interpret the extract information from the data. In that case, we apply ML (Mahesh, 2020).

Management control – The process of guiding organizations within the environments in which they operate, to achieve both short-term and long-term objectives (Adib & Zhang, 2019).

Many-to-many relationship – A relationship between two entities where the maximum cardinality of both entities is a lot. For example, each inventory item can be sold to many different customers, and each customer can order many different inventory items (Romney et al., 2021).

Marketing management – The process of planning and executing the creation, pricing, promotion, and distribution of ideas, goods, and services to create market exchanges that satisfy customers and organizations (Turban et al., 2021).

Metadata – Data that describes other data (Romney et al., 2021).

Mindset – A mental attitude, a way of thinking, or a frame of mind (Romney et al., 2021).

Mobile app – A software applications designed to run on mobile devices such as smartphones and tablet computers. While they may be small in functionality (but do not have to be), they deliver a high-quality service or experience to users. Apps range from simple games to highly sophisticated solutions – it all depends on the needs and expectations of the targeted audiences (Pieślak et al., 2023).

Multi-party computation – A toolbox of cryptographic techniques that enables multiple parties to compute data jointly, as if they had a shared database. Because the data has cryptographic protection, the parties can never view each other's data. The participating parties decide who is allowed to view the outcome of the computation (Worm, 2024).

Nearshore – A rising business strategy that involves relocating business operations to an external firm located outside but close to the nation's borders, i.e., a country in its immediate region (Maritz, 2024).

Nonrepudiation – A term used for the service that ensures entities are honest in their actions (Schou & Hernandez, 2015).

Normalize – A data modelling technique that is typically utilized in OLTP systems. The focus of this design technique is to maintain a data structure in which the data within an individual entity maps in a one-to-one relationship to its parent key (Hammergren, 1996).

Offshoring – The practice of outsourcing business functions in another country in order to reduce costs, typically where the costs of labor are lower (Giustiniano & Clarioni, 2013).

One-to-many relationship – A relationship between two entities where the maximum cardinality for one of the entities is 1, but the other entity has a maximum cardinality of many (Romney et al., 2021).

One-to-one relationship – A relationship between two entities where the maximum cardinality for each entity is 1 (Romney et al., 2021).

Online marketplace – Websites that provide a platform for multiple retailers to promote and sell products and services, usually for a fee commission, or other type of remuneration (Turban et al., 2021).

Online transaction processing – A system which supports entering data reliably into a database (Inmon et al., 1997).

Optimizing – The process of finding an alternative that is most cost effective or produce best achievable performance under given constraints by maximizing desired effects and minimizing undesired effect (Turban et al., 2021).

Outsourcing – The procurement of supplies or services related to a whatever value chain activity from legally independent firms (outsourcers). More specifically, outsourcing is defined as domestic, if firms source from suppliers from the same (home) country (Giustiniano & Clarioni, 2013).

Peer-to-peer – A system where assets or services are shared between consumers, private individuals (Shmidt, 2023).

Peer-to-peer network – A mechanism that is used to boost the security of the blockchain (Turban et al., 2021).

Personal data – Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (DSSC, 2024a).

Platform as a service – A cloud solution for the creation of applications. In this model, software developers have access to computing platforms including operating systems, programming language, and execution environments without the underlying infrastructure costs (IFAC, 2018).

Predictive analytics – The use of data to predict future trends and events. It uses historical data to forecast potential scenarios that can help drive strategic decisions (Cote, 2021).

Privacy-by-design – An approach that aims to protect individual privacy and data protection through intentional design choices. Unlike traditional privacy methods that view privacy as an afterthought, privacy by design makes privacy protection central starting from the very initial stages of design (IEEE, 2025).

Private blockchain – A blockchain technology that works in a restrictive environment like a closed network or is under the control of a single entity. While it operates like a public blockchain network in the sense that it uses peer-to-peer connections and decentralization, this type of blockchain is on a much smaller scale. Instead of just anyone being able to join and provide computing power, private blockchains typically are operated on a small network inside a company or organization. They are also known as permissioned blockchains or enterprise blockchains (Campbell, 2024).

Private cloud – Cloud infrastructure that is available for the exclusive use by a single organization (EBA, 2019).

Process automation – The use of software and technologies to automate business processes and functions in order to accomplish defined organizational goals (SAP, 2025).

Public blockchain – A technological platform that is non-restrictive and permissionless to which anyone with internet access can sign on to become an authorized node. This user can access current and past records and conduct mining activities; the complex computations used to verify transactions and add them to the ledger. No valid record or transaction can be changed on the network, and anyone can verify the transactions, find bugs, or propose changes because the source code is usually open source (Campbell, 2024).

Public cloud – A standard cloud computing model in which a service provider makes resources, apps, or storage available to the general public over the internet either free or on a pay-per-usage model (Turban et al., 2021).

Query – Ad hoc (unplanned) user request for specific data (Turban et al., 2021).

Ransom – A portmanteau word that is a merger of ransom and malware. It is categorized as malicious software like viruses, Trojan horses, spyware, and rootkits (Ilbiz & Kaunert, 2023).

Ransom attack – The perpetrator typically infiltrates the victim's computer system and encrypts digital files or renders the system inaccessible to the user. The victim is then forced to pay a ransom to regain access to the encrypted files and devices (Ilbiz & Kaunert, 2023).

Real-time processing – Also referred to as online transaction processing (OLTP) – occurs when transactions are processed as they occur to keep account balances and inventories up to date and ensure the system always reflects the current status of the data (Turban et al., 2021).

Record – A set of fields whose data values describe specific attributes of an entity, such as all payroll data relating to a single employee. An example is a row in a spreadsheet (Romney et al., 2021).

Relational database – A system in which data is organized into normalized table structures that consists of rows and columns. The relationships among tables are defined among data values rather than pointers or location (Hammergren, 1996).

Resources – Things that have economic value to an organization such as cash, inventory, supplies, factories, and land (Romney et al., 2021).

Risk – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood (Pugliese, 2022).

Risk mitigation – The action taken to reduce threats and ensure resiliency (Turban et al., 2021).

Robotic process automation – A productivity tool that allows a user to configure one or more scripts (which some vendors refer to as “bots”) to activate specific keystrokes in an automated fashion. The result is that the bots can be used to mimic or emulate selected tasks (transaction steps) within an overall business or IT process. These may include manipulating data, passing data to and from different applications, triggering responses, or executing transactions. RPA uses a combination of user interface interaction and descriptor technologies. The scripts can overlay on one or more software applications (Gartner, 2025a).

Router – Links computers to the internet to enable users to share a network connection. It acts like a dispatcher, choosing the best paths for data packets to travel from their source to their destination based on IP addresses (Turban et al., 2021).

Sales management – It involves sales procedures and tasks from the generation of leads and quotes, and moving to customer conversation, purchases, returns, and support (Turban et al., 2021).

Scalability – The ability of the system to increase in size to handle data growth or the load of an increasing number of concurrent users, that is, scalable systems efficiently meet the demand of high-performance computing (Turban et al., 2021).

Semi-structured data – Data that would normally be considered unstructured data, but that includes metadata which identifies certain characteristics. The metadata contains enough information to enable the data to be more efficiently cataloged, searched, and analyzed than strictly unstructured data. Think of semi-structured data as in between structured and unstructured data. A good example of semi-structured data would be a tab delimited file containing customer data (Talend, 2025).

Server – A central repository of data and various programs that are shared by users in a network (Turban et al., 2021).

Service provider – A person, a business, or even a government entity that delivers services to individuals or other organizations. These services can encompass a vast spectrum, including ICT, healthcare, education, legal advice, and more (Rahaman, 2023).

Sharewashing – Misleading communication that erroneously asserts a firm's offer as part of the sharing economy (Lehr et al., 2021).

Smart contract – A script that is stored on the blockchain and is executed automatically when addressing a transaction to it. The given transaction data is then processed according to the protocol defined for the smart contract (Menne, 2018).

Smartphone – A handheld electronic device that provides a connection to a cellular network. Smartphones were introduced to the world in 1994 by IBM but have since expanded to include companies like Apple and Samsung. Although they were originally meant to allow individuals to communicate via phone and email, smartphones now allow people to access the internet, play games, and send text messages in addition to making phone calls and sending emails (Estavez & Jackson, 2024).

Social media – A form of digital communication that allows users to form online networks and communities for socializing, sharing information, and posting user-created content (Paljug & Velasquez, 2025).

Software – A set of machine-readable instructions (code) that makes up a computer application that directs a computer's processor to perform specific operations (Turban et al., 2021).

Software as a service – Cloud computing applications that are hosted by a service provider and accessed by customers over the internet, often with a simple web browser, but sometimes with a small application automatically downloaded from the hosting (IFAC, 2018).

Software development life cycle – The time required for the activities such as defining, developing, testing, delivering, operating, and maintaining the software or the system. The development team's productivity and the software quality depend on the effectiveness of defining and analyzing the software process metrics throughout the SDLC (Ergasheva & Kruglov, 2020).

Structured data – Data that has been predefined and formatted to a set structure before being placed in data storage, which is often referred to as schema-on-write. The best example of structured data is the relational database in which the data has been formatted into precisely defined fields, such as credit card numbers or address, in order to be easily queried with Structured Query Language (SQL) (Talend, 2025).

Structured query language – The standard language for accessing relational databases to retrieve and manipulate data (Hammergren, 1996).

Sub-outsourcing – A situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider (EBA, 2019).

Supply chain – Starts with the acquisition of raw materials or the procurement (purchase) of products and proceeds through manufacture, transport, and delivery – and the disposal or recycling of products (Turban et al., 2021).

Sustainability – The ability to create and maintain conditions that enable humans and nature to exist in productive harmony to support present and future generations (Turban et al., 2021).

Template – A sample document that demonstrates required/suggested formatting and already has some details in place (Turban et al., 2021).

Third party – An individual or entity that is involved in a transaction but is not one of the principals and, thus, may have a lesser interest in the transaction. An example of a third party would be the escrow company in a real estate transaction; the escrow party acts as a neutral agent by collecting the documents and money that the buyer and seller exchange when completing the transaction (Kenton & Scott, 2020).

Third party audit – Systematically examining an organization's procedures, processes, and activities by an independent and objective external organization or individual. This type of audit is conducted by a party with no financial or other interest in the organization and is not part of its internal operations. TPAs serve as a critical tool for assessing the effectiveness and efficiency of an organization's operations and identifying areas for improvement (Tamboly, 2024).

Tracking – Remotely entering end-user's terminal equipment to monitor their activities online, collect information about them and/or identify the location of their devices (EU, 2018).

Trend – General patterns that change and develop, moving up, down, and diagonally. They can appear in pop culture, entertainment, the market, and politics. A trend can be serious or fun and can last for an undetermined amount of time. They are constantly wavering and evolving. As an example, when something is trending on social media, it is the subject of many posts. Meanwhile, in sales, a trend can influence the monthly change in sales volume for a small business (IET, 2024).

Transaction – A logical unit of work that constitutes a business action (Hammergren, 1996).

Unstructured data – Data stored in its native format and not processed until used, which is known as schema-on-read. It comes in a myriad of file formats, including email, social media posts, presentations, chats, IoT sensor data, and satellite imagery (Talend, 2025).

Value creation service – Any service aimed to create value out of the data shared in the data space (DSSC, 2024m).

Vulnerability – (1) A flaw or weakness in procedure, design, implementation, or internal controls that can be exploited and can result in an information security breach or a violation of information security policy. (2) Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited (Schou & Hernandez, 2015).

WiFi network – An internet connection that is shared with multiple devices in a home or business via a wireless router. The router is connected directly to the internet modem and acts as a hub to broadcast the internet signal to all your Wi-Fi enabled devices. This gives you flexibility to stay connected to the internet as long as you are within your network coverage area (Verizon, 2024).

Appendix D. Data sharing solutions

In table 9, three types of data sharing solutions and few related aspects are replicated that have come over the last few decades.

Table 9. Three forms of data sharing solutions (Nguyen et al., 2023, pp. 9-13)

Solution	Description	Advantage	Disadvantage
Homegrown	Based on legacy technologies such as email, FTP or APIs	• Vendor agnostic • Flexibility	• Data movement • Complexity of sharing data • Operational overhead for data recipients • Security and governance • Scalability
Proprietary vendor	Popular option among those that do not want to devote the time and resources to building an in-house solution yet also want more control	• Simplicity	• Vendor lock-in • Data movement • Scalability • Cost
Cloud objects storage	Good fit for the cloud because it is elastic and can more easily scale into multiple petabytes to support unlimited data growth. The big three cloud providers all offer object storage services (AWS S3, Azure Blob, Google Cloud Storage)	• Sharing data in place • Scalability	• Limited to a single cloud provider • Cumbersome security and governance • Complexity • Operational overhead for data recipients

Appendix E. Overview of figures and tables

The following figures are illustrated in this publication:

1. Datafication technology evolution.
2. Drivers of sharing economy.
3. Data spaces building blocks.
4. Relevance of enabler technologies.
5. Data sharing trust principles.
6. Examples of compounding risks.
7. Areas of risk mitigation implications.
8. Components of SOC suite of services.
9. Few trends in assurance.
10. Research methodology.

This book includes the tables listed below:

1. Some data sharing methods.
2. Scoping data sharing economy.
3. Categorization of digital platforms.
4. Data sharing risks.
5. Sharing economy risks.
6. Digital platform risks.
7. Few assurance concepts in data sharing economy.
8. Acronyms.
9. Three forms of data sharing solutions.

Appendix F. About the authors

Prof. dr. Abbas Shahim RE is full professor of IT auditing and is the head of the IT Audit, Compliance and Advisory program at the Vrije Universiteit Amsterdam. He is the co-founder of the Digital Auditing program at this university, is active in conducting research, and manages a working group in the area of IT Assurance and Audit at the International Federation for Information Processing (IFIP). In addition to being a member of the Ethical Council at NOREA (The Dutch professional organization of IT auditors), Abbas pursues a business career as well. He served several senior and leadership roles related to Governance, Risk and Compliance (GRC), cybersecurity, and Environmental, Social, and Governance (ESG). Currently, Abbas works as a partner in the IT Assurance and Advisory practice at KPMG Netherlands.

Drs. Jacco van Kleef RA, Digital MBA is partner in the IT Assurance and Advisory practice at KPMG Netherlands. With a strong foundation in accountancy and IT auditing, Jacco has built a career at the intersection of financial audit, internal control, and digital transformation. He holds degrees in Information Management and Audit from Nyenrode Business University, IT Auditing from Erasmus University Rotterdam, and a Digital MBA from Vlerick Business School. In addition to his professional practice, Jacco contributes thought leadership through publications on topics such as compliance assurance and cultural reporting in outsourcing. He is committed to advancing governance and internal control frameworks and is actively involved in initiatives that promote transparency and accountability in service organizations.

Dr. Alexander Boer is Senior Manager and R&D Lead in KPMG Netherlands' Responsible AI team. Alexander has 25 years of experience working with Artificial Intelligence, specializing in the Artificial Intelligence and Law field, in AI governance, risk management, and compliance (AI GRC), and in AI audits. Within the Responsible AI team, which delivers AI in-control business services, Alexander is a specialist in implementing compliance with AI and data-related legislation. Prior to joining KPMG, Alexander worked at the University of Amsterdam for decades, engaging with research in the areas of Linked Open Data and Artificial Intelligence and Law. Alexander still regularly lectures about controlling AI risk and doing AI audits at universities.

Aram Falticeanu RA is Director of Audit Innovation at KPMG Netherlands. He leads a team of over 100 experts, connecting auditors with data specialists to deliver technology-driven audit solutions. With experience across 1,000+ clients and multiple sectors, Aram supports digital transformation through innovative audit practices. Starting as an audit trainee in 2009, Aram has grown into a tech-savvy leader. As a Dutch certified financial auditor (RA), IT auditor and product manager, he develops scalable, AI-powered tools that generate actionable insights. He excels at uniting diverse teams to co-create digital audit solutions tailored to client needs.

Albert van der Sluis EMFC RC is a PhD candidate at the Vrije Universiteit Amsterdam. His main research focus is placed on the digital transformation of the audit profession. In this field of study, he is especially interested in the area of digital ethics. Albert is active in practice as well and is currently employed by the Dutch Ministry of Justice and Security where he holds the position of business controller. Albert acts on his own behalf with regard to his contribution to this publication.

Contact

KPMG Nederland
Laan van Langerhuize 1
1186 DS Amstelveen



John Kamphuis
Head of Assurance Transformation
KPMG Netherlands

kamphuis.john@kpmg.nl
+31 (0)6 29 59 03 73



Abbas Shahim
IT Assurance & Advisory
KPMG Netherlands

shahim.abbas@kpmg.nl
+31 (0)6 28 32 10 40



kpmg.nl



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

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

All rights reserved.