When Crisis Hit the Firm: Insights from Cloud Computing during Covid-19 for Tech-Enabled Corporate Resilience

Jorge Zips

Dissertation written under the supervision of Professor Peter V. Rajsingh

Dissertation submitted in partial fulfilment of requirements for the MSc in Management with Specialization in Strategy, Entrepreneurship & Impact, at the Universidade Católica Portuguesa, June 2025.

Abstract

This thesis explores how cloud computing enhanced corporate resilience during the COVID-19 crisis and what strategic insights can be drawn for future disruptions. It focuses on cloud's role in supporting operational continuity, technological adaptability, and strategic transformation.

A mixed-methods approach was applied. First, twelve expert interviews from technology, strategy, and crisis management were conducted and analyzed using the Gioia Method. Second, a perception-based online survey (N = 137) captured end-user views across sectors. Finally, findings were triangulated to uncover patterns and implications.

The results revealed that cloud-native systems, modular architectures, and scalable platforms enabled rapid crisis response and long-term adaptation. However, technology alone was insufficient. Strategic alignment, transparent leadership, and organizational culture emerged as critical enablers. Quantitative analyses confirmed that perceived digital responsiveness and communicative clarity significantly shaped resilience perceptions.

These findings showed that resilience is not a byproduct of digital tools but the result of deliberate integration across people, systems, and strategy. Cloud computing is a catalyst, but only when embedded into proactive, cross-functional transformation efforts. The thesis contributes a multidimensional model of tech-enabled resilience and offers practical guidance for firms navigating future uncertainty.

Keywords: Cloud Computing, Corporate Resilience, Digital Transformation, Crisis Management, Dynamic Capabilities, Strategic Adaptation

Title: When Crisis Hit the Firm: Insights from Cloud Computing during Covid-19 for Tech-Enabled Corporate Resilience

Author: Jorge Zips

Resumo

Esta tese explora como a computação em nuvem reforçou a resiliência corporativa durante a crise da COVID-19 e quais aprendizagens estratégicas podem ser extraídas para futuras disrupções. O foco recai sobre o papel da nuvem na continuidade operacional, adaptabilidade tecnológica e transformação estratégica.

Aplicou-se uma abordagem de métodos mistos. Foram conduzidas doze entrevistas com especialistas em tecnologia, estratégia e gestão de crises, analisadas pelo método Gioia. Em seguida, um inquérito online baseado na perceção (N = 137) recolheu opiniões de utilizadores de diferentes setores. Os dados foram triangulados para identificar padrões e implicações.

Os resultados indicam que sistemas nativos em nuvem, arquiteturas modulares e plataformas escaláveis facilitaram respostas rápidas e adaptação sustentável. Contudo, a tecnologia, por si só, foi insuficiente. Alinhamento estratégico, liderança transparente e cultura organizacional emergiram como fatores críticos. As análises confirmaram que perceções de agilidade digital e comunicação clara influenciam fortemente a resiliência percebida.

A investigação mostra que a resiliência não resulta apenas de ferramentas digitais, mas da integração estratégica entre pessoas, sistemas e processos. A computação em nuvem atua como catalisador—quando inserida em transformações proativas e interfuncionais. A tese propõe um modelo multidimensional de resiliência tecnológica e oferece orientações práticas para empresas que enfrentam contextos de incerteza.

Palavras-chave: Computação em Nuvem, Resiliência Corporativa, Transformação Digital, Gestão de Crises, Capacidades Dinâmicas, Adaptação Estratégica

Título: Quando a Crise Atinge a Empresa: Lições da Computação em Nuvem durante a Covid-19 para uma Resiliência Corporativa Baseada em Tecnologia

Autor: Jorge Zips

AI Usage Acknowledgement

In this master's thesis, AI tools were used to support selected stages of the research process. ChatGPT-4 and Connected Papers were consulted during the literature exploration phase to identify additional keywords and potential sources. The author independently retrieved, reviewed, and cited all literature included in the thesis.

ChatGPT was also used throughout the writing and revision process to enhance clarity, structure, and language quality. It helped streamline formulations, improve transitions, and ensure overall coherence. Additionally, AI provided guidance on how to use SPSS, specifically on locating relevant functions and formatting tables and graphs correctly. However, the actual analysis, statistical interpretation, and reporting were conducted by the author.

No AI tools were used for data collection, conceptual development, or critical interpretation of findings. The author verified and adapted all AI-assisted suggestions to ensure accuracy, coherence, and academic rigor. The responsibility for the entire content remains solely with the author. This usage aligns with Católica-Lisbon’s standards for transparency and responsible academic conduct.

Acknowledgements

This thesis marks the conclusion of my Master's journey at Católica Lisbon School of Business and Economics. It has been a formative and enriching experience, both academically and personally.

First and foremost, I would like to sincerely thank my supervisor, Peter V. Rajsingh, for his continuous support, sharp guidance, and inspiring mentorship throughout the thesis process. I am particularly grateful for the opportunity to learn from him not only in class but also beyond the academic setting, including his invaluable encouragement during extracurricular projects such as the ABC Business Challenge. I also extend my gratitude to all other professors at Católica Lisbon, whose courses and perspectives have shaped my thinking during these past two years.

I am equally thankful to all participants who contributed to my research, whether by sharing their insights in interviews or taking the time to respond to the survey. Their openness, engagement, and willingness to support this project were fundamental to its success.

A special thanks goes to my family, especially my mother, who has always made everything possible, and to my sister, whose presence and support were invaluable throughout this journey. I also want to thank all other family members who stood by me whenever I needed them.

Many others deserve recognition, but I am especially grateful to Simon, whose early encouragement was crucial in pushing me to pursue a Master's abroad and who supported me throughout the scholarship process. Without him, this path might never have happened.

Lastly, I would like to thank all my fellow students for the great time we shared at Católica, the friendships we built, and the mutual support that defined this chapter.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AI	Artificial Intelligence
AWS	Amazon Web Services
BAIT	Bankaufsichtliche Anforderung an die IT
BCP	Business Continuity Management
CCPA	California Consumer Privacy Act
CRM	Customer Relationship Management
DCF	Dynamic Capabilities Framework
DevOps	Development and Operations
DORA	Digital Operational Resilience Act
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
GPC	Google Cloud Platform
IaaS	Infrastructure-as-a-Service
IoT	Internet of Things
ISO	International Organization for Standardization
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MaRisk	Mindestanforderung an das Risikomanagement
MTTR	Mean Time to Recovery

MVP	Minimum Viable Product
PaaS	Platform-as-a-Service
RBV	Resource-Based View
SaaS	Software-as-a-Service
SME	Small and Medium-sized Enterprises
SOC	Security Operations Center

1 Introduction

Firms are subject to a variety of challenges in their efforts to compete and succeed. For example, Porter famously points to threats from new entrants and threats of substitution as factors that firms must manage if they are to compete in an industry (Porter, 1985). The disruption to firm activities from so-called black swan events (Taleb, 2010) is significant. The COVID-19 pandemic was a major global crisis that forced companies to adapt to unprecedented challenges. While lockdowns and disrupted supply chains challenged most companies, some demonstrated remarkable resilience. According to chaos theory, seemingly stable systems (such as the global economy) can quickly transform from order to chaos (Rajagopal, 2015). A key technology that has helped companies stay flexible and operational during this time was cloud computing.

Cloud computing, which originated in the 1960s through the principle of "*time-shared computers*", has become a core component of modern corporate infrastructures since the 2000s (Salesforce, n.d.b). With the introduction of Amazon Web Services (AWS) in 2006 (Amazon Web Services, n.d.a) and the increasing use of platforms such as Google Cloud (GCP) and Microsoft Azure, technology has become indispensable for many companies. During the pandemic, cloud computing proved its worth as the basis for working from home, virtual collaboration, and scaling business processes (Microsoft Azure, n.d.).

According to Statista, global cloud computing revenues increased from approximately $243 billion in 2019 to over $400 billion in 2021, a growth of nearly 65% within two years. This highlights how companies around the world relied on cloud services to adapt to the challenges posed by the pandemic.

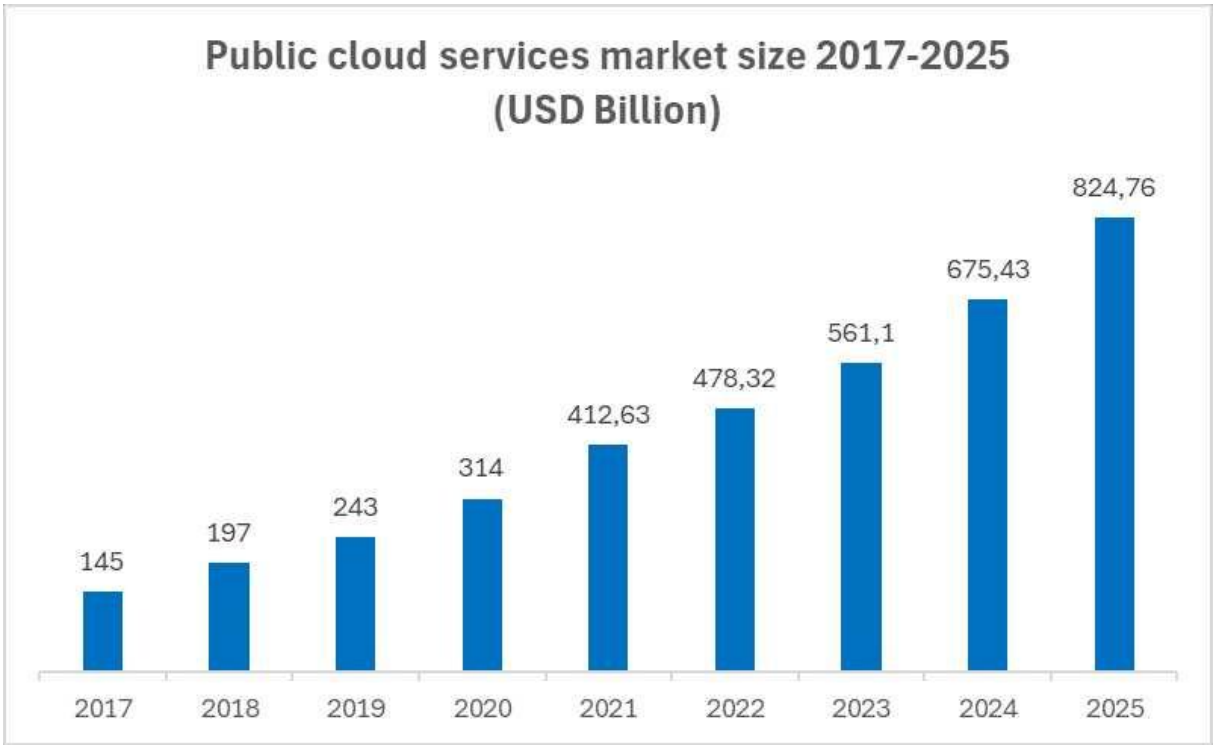

Figure 1: Public cloud services end-user spending worldwide from 2017 to 2025

Source: Reproduced from (Vailshery, 2024)

But key questions remain. How does cloud computing illustrate specific factors that contribute to corporate resilience? What strategic insights can be derived from its use during the pandemic crisis? This thesis investigates how cloud computing helped firms manage vulnerabilities and enhance resilience during COVID-19, providing insight into its role as a strategic enabler during crises, based on theory and data. It aims to:

1. Analyze how cloud technologies supported business continuity during the pandemic;
2. Explore perceptions of resilience among professionals and end-users;
3. Derive strategic recommendations for strengthening resilience in future crises.

The **Research Question** is:

"How did factors associated with Cloud Computing enhance corporate resilience during the COVID-19 pandemic, and what strategic insights can be drawn for future crises?"

2 Literature Review

2.1 Theoretical Foundations of Corporate Resilience

2.1.1 RBV: Competitive Advantage through Resilient Resources

The Resource-Based View (RBV) explains sustainable competitive advantage through firm-specific resources that are valuable, rare, inimitable, and non-substitutable (VRIN). These resources, tangible and intangible, such as organizational knowledge, managerial skills, and internal processes, determine performance differences across firms, even within the same industry (Barney, Wright and Ketchen, 2001).

Applied to resilience, RBV highlights how firms with robust resource bases can better absorb shocks and maintain strategic stability. Resilient organizations develop routines and knowledge that support adaptability in dynamic environments, enabling faster recovery after disruptions (Helfat *et al.*, 2023).

In digital contexts, RBV has been used to conceptualize IT assets, like databases and analytics capabilities, as strategic resources. When paired with analytics expertise, data represents a VRIN asset and a basis for competition (Helfat *et al.*, 2023). Similarly, cloud infrastructures can be sources of advantage if firms uniquely integrate and apply them. While cloud services are widely available, the ability to implement them effectively is not. Cloud-related skills are scarce and hard to replicate, making them a potential source of competitive advantage (Mitra, O'Regan and Sarpong, 2018).

2.1.2 DCF: Adaptability & Sensing-Seizing-Reconfiguring

The Dynamic Capabilities Framework (DCF) builds on the RBV by emphasizing a firm's ability to adapt and transform its resource base in dynamic environments (Teece, 2007). While RBV focuses on static advantages, DCF stresses the importance of continuous reconfiguration to sustain competitiveness in fast-changing markets. Dynamic capabilities are defined as "*the ability of a firm to integrate, build and reconfigure internal and external competencies to adapt to rapidly changing environments.*" (Teece, Pisano and Shuen, 1997). Barreto (2010) added to the definition by stating that dynamic capabilities are "*the firm's potential to systematically solve problems, formed by its propensity to sense opportunities and threats, to make timely and market-oriented decisions, and to change its resource base*".

This framework comprises four core processes. *Sensing* refers to identifying emerging risks, opportunities, and shifts in market or technology trends before they fully materialize. *Seizing* involves mobilizing resources, making strategic investments, and adapting operations to act on these opportunities. *Reconfiguring* denotes the ongoing transformation of business structures, leadership, and resource configurations to meet evolving challenges. And these should be done in a *timely manner* relative to opportunities and threats (Barreto, 2010). Firms excelling in these areas tend to be more resilient, as they can proactively adapt rather than react under pressure (Teece, Pisano and Shuen, 1997).

Well-known examples include Amazon and Netflix, which successfully adapted their business models in response to early signs of disruption (Christensen and Bower, 1996). Dynamic capabilities also support the development and protection of intangible assets that drive sustained performance (Teece, 2007).

Research confirms that organizations engaging in sensing, seizing, and reconfiguring are better equipped to withstand and recover from crises (Spender, 2014). Learning routines, scenario planning, and agile decision-making support long-term resilience (Garcie-Valenzuela, Jacob-Hernandez and Flores-Lopez, 2023). IBM's strategic shift from hardware to cloud and AI exemplifies the power of deliberate resource reallocation (O'Reilly and Tushman, 2007).

In turbulent environments, dynamic capabilities enable firms not just to survive but to emerge stronger. The DCF also provides a useful lens for understanding digital transformation, as companies must continually adapt through routines like digital opportunity scanning, IT infrastructure adaptation, and agile strategy development (Helfat *et al.*, 2023). These practices help firms reallocate legacy resources to capitalize on innovation. The Technology S-Curve further explains why firms with strong dynamic capabilities are more successful in transitioning between technological paradigms. As shown in Table 1, companies in fast-changing industries tend to perform better due to their inherent adaptability – a pattern echoed in firms adapting cloud for resilience (Christensen, Suarez and Utterback, 1998).

2.1.3 Resilience as a Strategic Goal: Definitions & Theoretical Perspectives

Resilience refers to an organization's ability to withstand, adapt to, and recover from disruptions, crises, and change. Rooted in psychology and systems theory, it has been widely applied in organizational studies. High-Reliability Organization (HRO) theory, for instance,

examines how firms in high-risk settings reduce errors through mindfulness, redundancy, and a strong error management culture (Weick and Sutcliffe, 2007). Other approaches define resilience as a set of cognitive, behavioral, and contextual capabilities that enable firms not only to endure shocks but also to learn and grow from them (Lengnick-Hall, Beck and Lengnick-Hall, 2011; Klöckner, Schmidt and Wagner, 2023).

More recent literature frames resilience as a dynamic, processual capability encompassing three stages: anticipation, coping, and adaptation. This view emphasizes resilience as a meta-capability grounded in learning, proactive governance, and organizational culture, not as a static condition (Duchek, 2020). Unlike robustness, which focuses on resistance, resilience centers on adaptation and renewal (Kindermann *et al.*, 2021).

However, most traditional resilience frameworks overlook the role of digital infrastructure and cloud computing. Historically, these technologies were seen primarily as tools for efficiency and scalability (Armbrust *et al.*, 2010; Marston *et al.*, 2010). Only more recently has research begun to recognize their strategic relevance for business continuity, adaptability, and crisis response (Papagiannidis, Harris and Morton, 2020; Seetharaman, 2020). This gap highlights the need to reframe digital infrastructure, especially cloud computing, as a key enabler of multidimensional corporate resilience (Mitroff, 1988). In this context, Contingency Theory also emphasizes that resilience strategies must align with environmental and regulatory conditions. It helps explain sectoral differences and complements capability-based views by reinforcing the contextual embeddedness of resilience strategies (Oesterle *et al.*, 2020). Existing resilience models offer valuable perspectives but often lack integration of digital infrastructure as a strategic enabler, a gap this thesis addresses by linking cloud computing to multidimensional resilience in practice.

2.2 Resilience as a Multidimensional Concept

Corporate resilience refers to an organization's ability to anticipate, absorb, adapt to, and recover from disruptions while maintaining operational continuity and long-term competitiveness. Unlike robustness, which emphasizes resistance, resilience combines stability with transformation in response to evolving threats (Sheffi, 2013).

Resilience has become a strategic imperative, especially in volatile, tech-driven, and highly regulated industries (Duchek, 2020). This thesis conceptualizes resilience as a multidimensional construct, grounded in the RBV, DCF, and, contextually, Contingency

Theory. RBV emphasizes firm-specific assets like IT infrastructure and financial reserves (Christensen, 1992). The DCF sees resilience as an active process of sensing, seizing, and reconfiguring in response to change (Kushida, Murray and Zysman, 2011). Contingency Theory highlights the need to align resilience strategies with regulatory and industry contexts (Kindermann *et al.*, 2021; Klöckner, Schmidt and Wagner, 2023).

The model below distinguishes three core dimensions, *operational*, *technological*, and *strategic-organizational* resilience, with *financial* and *regulatory* resilience as subdimensions. These are grounded in RBV, DCF, and Contingency Theory, respectively. Cloud computing is positioned as a cross-cutting enabler across all categories.

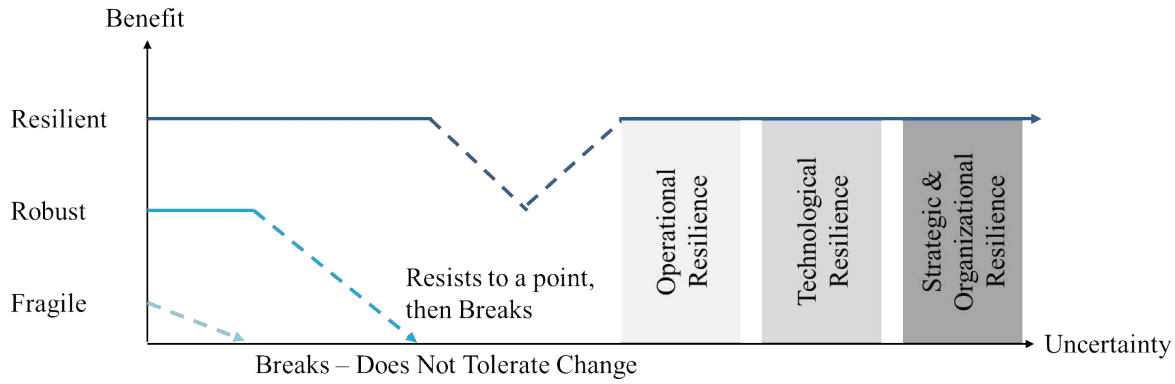

Figure 2: Conceptual framework of resilience as a strategic goal

Source: Own illustration based on (Wandemberg Boschetti, 2019)

2.2.1 Operational Resilience

Operational resilience is the ability to maintain business continuity and recover from disruptions with minimal impact on core functions. It relies on risk management, agile supply chains, and adaptable workforce strategies (Tang, Dong and Zhou, 2025). Organizations that embed resilience into operations can better anticipate risks, respond to crises, and sustain critical activities (Lindgren, 2017).

RBV links operational resilience to firm-specific assets like crisis response systems and workforce agility (Lee and Trimi, 2021). DCF adds that resilience depends on the ability to continuously reconfigure operations (Christensen, Suarez and Utterback, 1998).

Toyota illustrates this: after the 2011 Tōhoku earthquake, the firm expanded its lean model by adding supplier tiers and inventory buffers, enabling faster recovery in later crises (O'Reilly

and Tushman, 2007; Tashiro and Kitago, 2024). This shows how proactive adjustments enhance operational resilience.

2.2.2 Technological Resilience

Technological resilience is an organization's ability to leverage digital infrastructure and IT systems to withstand disruptions, safeguard cybersecurity, and enable adaptive business models (Teece, 2007). Scalable architectures, security, and analytics enhance a firm's ability to manage shocks and system failures (Mell and Grance, 2011).

According to the RBV, proprietary IT systems and security frameworks serve as key resilience assets (Adner and Kapoor, 2010). The DCF emphasizes that resilience grows when firms continually upgrade IT capabilities and integrate automation into decision-making (Gopalakrishnan and Damanpour, 1997).

The role of Regulatory Resilience in Technological Resilience

Technological resilience also depends on regulatory adaptability. In highly regulated industries, compliance with data protection laws (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA)) is critical. Cloud platforms support this through built-in compliance tools, encryption, and real-time monitoring (Wagner, n.d.).

Companies with robust regulatory frameworks were better able to maintain compliance and avoid penalties during rapid, crisis-induced digital shifts (Deloitte, n.d.). Leading cloud providers like AWS, Azure, and GCP support this by embedding real-time compliance monitoring, helping firms adapt quickly to evolving regulations and minimize risk (finreg-e, 2022).

For example, JPMorgan's early investment in scalable cloud systems enabled a fast shift to remote work during COVID-19 while maintaining compliance and continuity, outperforming competitors tied to legacy infrastructure (Groenendaal and Helsloot, 2021). This case illustrates how cloud-enabled technological resilience reinforces agility, security, and regulatory alignment in turbulent environments (Zollo and Winter, 2002).

2.2.3 Strategic & Organizational Resilience

Strategic and organizational resilience is a firm's capacity to anticipate risks, maintain financial stability, and adapt to market shifts through leadership, agility, and financial flexibility (Marston *et al.*, 2010). Resilient organizations invest in dynamic leadership, foster agility, and maintain financial buffers to endure crises without compromising growth (Cheema-Fox *et al.*, 2021).

RBV links this form of resilience to firm-specific capabilities like leadership, decision-making, and financial reserves (Christensen and Bower, 1996). DCF emphasizes continuous learning and strategic reconfiguration (Eisenhardt and Martin, Jeffrey, A., 2000).

Resilience requires proactive preparation. Embedding structured crisis management into strategic planning, through risk monitoring, scenario analysis, and adaptive leadership, enhances a firm's ability to navigate disruptions like COVID-19 (Papadopoulos, Baltas and Balta, 2020). This reflects the DCF's logic of sensing, seizing, and reconfiguring.

By treating crises as catalysts for transformation rather than threats, resilient firms preserve continuity, foster innovation, and strengthen long-term competitiveness.

The role of Financial Resilience in Strategic Resilience

Financial resilience enables firms to maintain liquidity, absorb shocks, and continue investing during crises. Flexible cost structures and contingency planning enhance adaptability in volatile environments. During COVID-19, firms using cloud-based financial models outperformed traditional ones through cost efficiency and scalable resource allocation (Blackrock, 2024).

Starbucks illustrates this: by closing underperforming stores, investing in digital tools, and adopting flexible work models during both the 2008 crisis and COVID-19, the company sustained stability and long-term competitiveness (CIPFA, n.d.; Spender, 2014; Shah *et al.*, 2023).

This chapter has outlined the three core dimensions of corporate resilience – *operational*, *technological*, and *strategic & organizational* – along with key subdimensions such as *regulatory* and *financial* resilience. Together, these factors shape a firm's capacity to endure disruption, recover effectively, and remain competitive.

The theoretical foundations – RBV and DCF – offer complementary lenses to understand how firms build and sustain resilience. Companies that invest proactively in supply chain optimization, IT modernization, and strategic financial planning are better positioned to navigate uncertainty (Teece, 2010).

Following this conceptual foundation, the next chapter examines how cloud computing enables resilience across these dimensions, highlighting the role of digital transformation in organizational adaptability (Garcia-Zambrano, Rodriguez-Castellamos and Garcia-Merino, n.d.).

2.3 Technological Trends – Digitization and Digitalization

Digital technologies have shifted from efficiency tools to strategic assets, playing a critical role in managing crises such as the 2008 financial collapse (Allen and Carletti, 2010), the semiconductor shortage (Wassen, Adel and Laoucine, 2022), supply chain disruptions in the automotive sector (Brandenburg, 2016), and disaster-related logistics failures (Adiguzel, 2019).

A key distinction is between *digitization* – the conversion of analog data into digital formats for incremental gains – and *digitalization*, which embeds digital technologies into core strategies, enhancing adaptability and resilience. Research shows that digitalization is essential for resilience, with 90% of firms now viewing it as a strategic priority (Kindermann *et al.*, 2021). Those aligning digital transformation with broader business goals significantly outperform competitors (Henderson and Venkatraman, 1993).

Cloud computing plays a central role in this shift. No longer just supportive, it now underpins digital transformation by providing scalable infrastructure for rapid crisis response and operational continuity (Yang *et al.*, 2021).

2.3.1 The Acceleration of Digital Transformation

The COVID-19 pandemic drastically accelerated digital transformation, compelling firms to adopt remote work, digital customer channels, and cloud-based supply chains within weeks. What would have taken years happened in months (Blackburn *et al.*, n.d.; McKinsey & Company, 2020). While digitally advanced sectors adapted quickly, physically dependent industries lagged behind (Seetharaman, 2020).

Consumer behavior also shifted rapidly, with a surge in digital usage. Zoom grew from 10 million to 300 million users, and webcam sales rose by 179%, highlighting the urgency and scale of change (Beimborn, Miletzki and Wenzel, 2011; Yang *et al.*, 2021).

This shift broke with traditional S-Curve adoption patterns, as firms accelerated cloud integration to maintain continuity. As shown in Figure 3, early adopters gained lasting advantage through digital lock-in, while late adopters faced competitive disadvantages and strategic inertia (Christensen, 1992; Lee and Trimi, 2021).

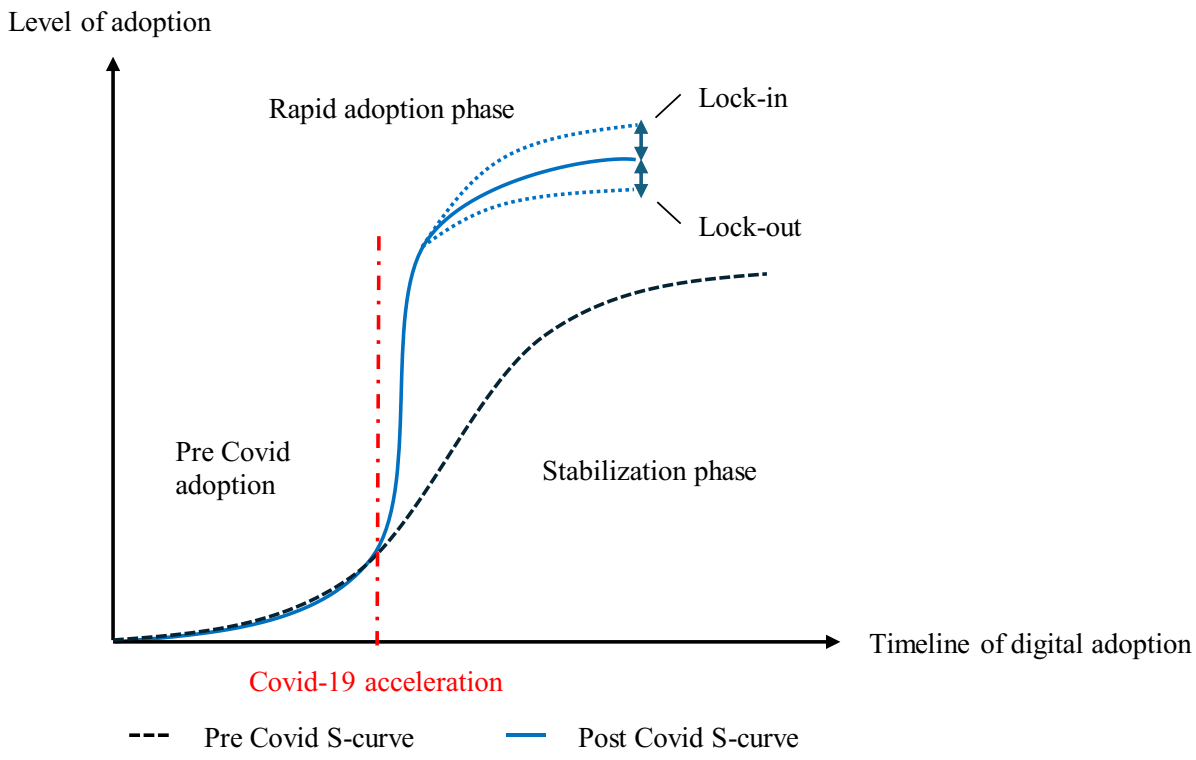

Figure 3: S-Curve shift driven by COVID-19 acceleration

Source: Own illustration

2.3.2 The Role of Emerging Technologies in Crisis Management

The COVID-19 crisis highlighted the critical role of emerging technologies, particularly Cloud Computing and Artificial Intelligence (AI), in effective crisis management. Cloud computing emerged as the foundational platform, especially for Small and Medium-sized Enterprises (SME), offering scalable and flexible infrastructure that enabled rapid response and adaptation (Papadopoulos, Baltas and Balta, 2020).

Strategic, integrated investments in digital ecosystems proved more effective than temporary fixes. (Adner and Kapoor, 2010; Spender, 2014). As illustrated in Figure 4, companies embedding cloud technologies into their core operations achieved greater resilience, revenue stability, and adaptability across sectors such as finance, retail, and education (Yang *et al.*, 2021).

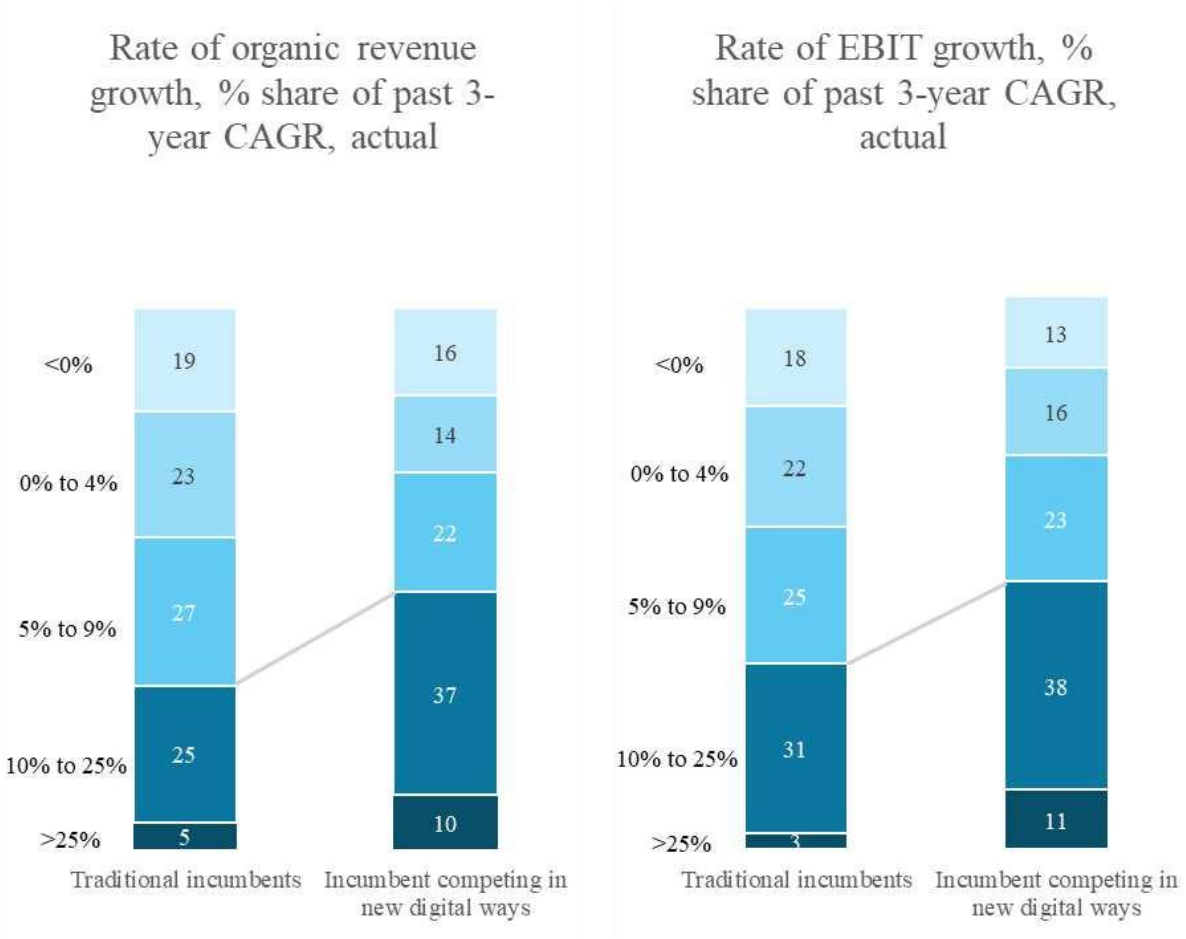

Figure 4: Bold, tightly integrated digital strategies and value creation

Source: Own illustration based on (Blackburn et al., n.d.)

Cloud computing marked a shift from localized IT infrastructure to scalable, internet-based environments. Its elasticity and real-time processing capabilities distinguish it from traditional systems, enabling interoperability and dynamic resource allocation, key for resilience and agility (Kushida, Murray and Zysman, 2011).

Pay-as-you-go Utility Model

Cloud computing differs from traditional utility models like electricity or water through its elasticity, customization, and competitive differentiation. It enables rapid scalability, platform

interoperability, and real-time data processing capabilities essential for digitally driven businesses (Kushida, Murray and Zysman, 2011).

The most cited definition by the National Institute of Standards and Technology describes cloud computing as *"[...] a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell and Grance, 2011, p. 2). The ISO/IEC 17788:2014 standard complements this, emphasizing terminology and interoperability. Both highlight cloud computing's core attributes – scalability, flexibility, and efficient resource use – crucial for strategic agility and regulatory compliance (ISO and ICE, 2023).

2.4 Cloud Computing as a Strategic Enabler of Resilience

As business processes digitalized, cloud computing became a key enabler of resilience. During COVID-19, firms with cloud infrastructures adapted more flexibly to disruptions than those with traditional IT, maintaining continuity through scalability, system stability, and remote productivity (Adner and Kapoor, 2010).

Cloud-based Disaster Recovery

Cloud-based disaster recovery solutions have proven effective in minimizing data loss and system failure, ensuring business continuity amid unexpected disruptions. The widespread use of platforms like Microsoft Teams and Google Workspace during the pandemic further demonstrated the central role of cloud infrastructure in maintaining remote workforce productivity (Adner and Kapoor, 2010; Papagiannidis, Harris and Morton, 2020; Yang *et al.*, 2021).

Resilience as CAPEX or OPEX

Beyond operations, cloud adoption has reshaped financial strategy by shifting IT costs from capital expenditure to operational expenditure. This flexibility empowered firms to respond swiftly to demand fluctuations, scale resources, and align IT spending with strategic growth (Khangha *et al.*, 2013).

The shift to cloud computing represents a strategic choice between short-term continuity and long-term advantage. While temporary solutions helped maintain operations during COVID-

19, sustained investment in technologies like AI, automation, and cloud security offered a lasting competitive edge. The right balance depends on a firm's risk profile, industry dynamics, and digital maturity (Khangha *et al.*, 2013; Papagiannidis, Harris and Morton, 2020).

2.4.1 Infrastructure Decoupling

Cloud computing shifts IT infrastructure from localized systems (e.g., on-premise servers) to shared, scalable environments. This transition enables dynamic reconfiguration and cost efficiency, key for operational resilience in crisis contexts (Kushida, Murray and Zysman, 2011). Technologies like virtualization allow rapid scaling without hardware changes, while data homogenization enables real-time processing and integration, both essential for business continuity and decision-making under pressure (Kindermann *et al.*, 2021).

The cloud ecosystem is shaped by four key stakeholder groups: users, providers, regulators, and infrastructure enablers. Their interaction determines how cloud infrastructure is adopted, governed, and aligned with resilience goals (Marston *et al.*, 2010). Regulatory actors, in particular, play a critical role in defining compliance frameworks that influence architecture choices and operational risk management.

To reduce dependence on non-European providers, the Gaia-X initiative was launched as a European response to vendor lock-in and regulatory fragmentation. By promoting interoperability, modular system design, and data sovereignty, Gaia-X aims to enhance both compliance and technological resilience, especially in highly regulated sectors like healthcare and finance (Yang *et al.*, 2021). The initiative serves as a strategic example of infrastructure decoupling, supporting more flexible, secure, and jurisdiction-aware cloud adoption.

2.4.2 Service Models & Resilience Applications

Cloud computing supports resilience across sectors by enabling technologies like AI or Big Data, fostering continuity, security, and agility (Yang *et al.*, 2021).

Its three core service models, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), contribute differently to operational, technological, and strategic adaptability (Marston *et al.*, 2010).

IaaS delivers configurable computing resources such as storage and virtual machines on a flexible, pay-as-you-go basis (Armbrust *et al.*, 2010). It gives firms full control over infrastructure and security (Bhardwaj, Jain and Jain, 2010; Kushida, Murray and Zysman, 2011). E.g., Netflix leverages AWS to rapidly scale operational resilience, ensuring uninterrupted global streaming (Amazon Web Services, 2016).

PaaS provides a managed development environment that abstracts infrastructure and speeds up deployment (Amazon Web Services, n.d.b; Marston *et al.*, 2010; Beimborn, Miletzki and Wenzel, 2011). Current, a fintech firm used Google Kubernetes Engine to cut time-to-market by 400% and eliminate downtime, enhancing technological agility (Google Cloud, n.d.).

SaaS delivers web-based applications with minimal IT effort (Amazon Web Services, n.d.b; Armbrust *et al.*, 2010; Bhardwaj, Jain and Jain, 2010; Kushida, Murray and Zysman, 2011). OpenTable, for instance, uses Salesforce to optimize customer service, boosting strategic resilience through greater productivity and user engagement (Salesforce, n.d.a).

Each service model supports resilience differently, from infrastructure flexibility to development speed and strategic adaptability.

2.4.3 Challenges of Cloud Computing in Crisis Management

While cloud computing offers strategic advantages during crises, it also presents risks related to security, compliance, and vendor dependency (Papadopoulos, Baltas and Balta, 2020).

Cloud Security & Regulatory Compliance: Risks to Technological & Operational Resilience

The global nature of cloud services complicates data sovereignty and legal compliance. In the UK and Ireland, 30% and 13% of SMEs, respectively, cite security and privacy concerns as barriers to adoption (Papadopoulos, Baltas and Balta, 2020). Navigating frameworks like GDPR, post-Brexit data laws, and the Toronto Declaration adds complexity (Yang *et al.*, 2021). Strong data governance is essential to avoid disruptions, legal penalties, and reputational damage.

Vendor Lock-In & Flexibility Trade-Offs: Risks to Strategic Resilience

Relying on a single cloud provider limits strategic flexibility. Proprietary Application Programming Interfaces and migration costs – up to $2 million for large firms – discourage multi-cloud adoption (Marston *et al.*, 2010; Papadopoulos, Baltas and Balta, 2020). This weakens a firm's ability to adapt under pressure. Cloud-agnostic strategies can mitigate these risks and preserve long-term resilience.

Cloud Security Vulnerabilities: Risks to Technological Resilience

Even with provider protections, 56% of cloud-using firms reported security incidents in 2020, often due to misconfigurations (Papagiannidis, Harris and Morton, 2020) These expose firms to data loss and compliance violations. Strengthening technological resilience requires zero-trust architectures, AI-powered threat detection, and continuous monitoring.

Legal Uncertainties in Multi-Jurisdictional Cloud Operations: Risks to Regulatory Resilience

Operating across jurisdictions introduces legal inconsistencies, such as conflicts between GDPR, the U.S. Patriot Act, and national data policies (Marston *et al.*, 2010). This complicates breach notification protocols, liability terms, and law enforcement access. Firms in regulated sectors must adopt proactive legal risk assessments and regional governance models to reinforce regulatory resilience.

Cloud Computing in Crisis Response

Despite these risks, cloud computing proved vital during the COVID-19 crisis. Companies with established cloud infrastructures adapted quickly, using Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), collaboration tools, and AI to ensure continuity (Kindermann *et al.*, 2021; Yang *et al.*, 2021; Klöckner, Schmidt and Wagner, 2023). In contrast, firms with legacy systems struggled. Cloud-native firms enabled rapid scaling, remote access, and real-time data sharing for ecosystem-wide coordination. Governments also invested in national cloud platforms to improve preparedness (Yang *et al.*, 2021). Integrated, cloud-based crisis frameworks, built on automation, scenario modeling, and scalable infrastructure, enhance organizational performance under uncertainty (O'Reilly and Tushman, 2007).

2.4.4 Cloud Computing and Business Continuity

Business continuity refers to maintaining core operations during disruptions, a challenge cloud computing addresses through scalability, remote access, and integrated disaster recovery (Kushida, Murray and Zysman, 2011; Papadopoulos, Baltas and Balta, 2020). By migrating from on-premise to cloud-based systems, organizations reduce operational risk and ensure efficiency under adverse conditions.

Cloud-native continuity strategies offer failover mechanisms, backups, and cross-regional redundancy, enabling firms to minimize downtime and data loss (Tashiro and Kitago, 2024). For instance, Sunstone Hotel Investors implemented AWS Elastic Disaster Recovery to protect data, lower hardware costs, and adapt faster to changing operational needs (Amazon Web Services, 2024). Similarly, IBM's use of Azure enabled dynamic failover across cloud regions, minimizing downtime and service disruption (Ibrahim, 2024).

These cases illustrate how embedding cloud into continuity planning enhances crisis response. As digital transformation accelerates, cloud-integrated resilience frameworks help firms maintain performance under pressure (Lindgren, 2017; Miceli *et al.*, 2021).

2.4.5 Flexibility and Agility

Strategic agility, the ability to sense, seize, and adapt to shifting conditions, is essential for resilience (Liu *et al.*, 2024). Cloud computing enables this through quick response to external shocks, scaling operations dynamically, and integrating new business models (Kindermann *et al.*, 2021).

The Role of the S-Curve in Cloud Adoption

Timing is critical. Firms that adopted cloud early capitalized on its flexibility before it became essential, while late adopters struggled with implementation and disruption (Christensen, 1992).

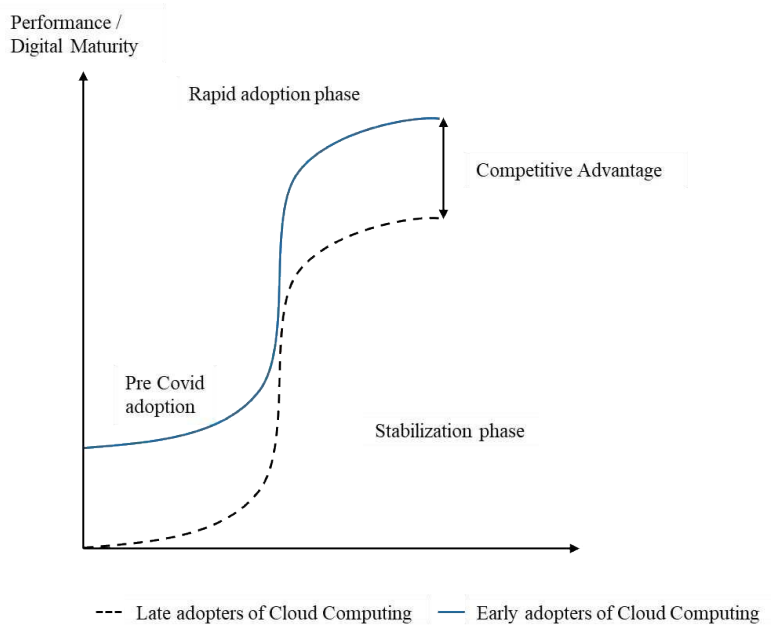

Figure 5: Comparison of firms that proactively and reactively integrated cloud computing

Source: Own illustration

Figure 5 illustrates how early movers gain digital maturity, positioning themselves to scale rapidly and maintain continuity. Digital-native firms like AWS and Zoom outperformed legacy-dependent competitors during the pandemic, gaining a clear resilience advantage (Lee and Trimi, 2021).

Cloud-based analytics and Internet of Things (IoT) enable real-time risk monitoring and supply chain reconfiguration. During COVID-19, Bosch used these tools to dynamically reroute shipments, adjust inventories, and mitigate disruptions, illustrating how digital infrastructure supports operational agility under pressure (Leiting, Cuyper and Kauffmann, 2022; Shah *et al.*, 2023).

Cloud infrastructure also enables rapid business model shifts. Nike's early investment in cloud-based analytics and digital platforms allowed it to pivot quickly during the 2020 lockdown, moving 80% of sales online and maintaining growth despite store closures (Eisenhardt, 1989; Targett, 2024).

These cases show that strategic agility is not just reactive but rooted in proactive digital investment. Cloud computing enables organizations to innovate, pivot, and build a lasting competitive advantage, particularly when embedded in a broader digital strategy.

2.4.6 Strategic Adaptation and Cloud Provider Strategies

Major cloud providers like AWS, GCP, and Azure influence how firms adopt cloud technologies and ensure digital continuity. Each offers distinct strategic advantages, AWS prioritizes operational scalability, GCP emphasizes AI-driven analytics, and Azure focuses on hybrid-cloud solutions for regulated sectors (Khangha *et al.*, 2013).

These strategies directly impacted firms' resilience readiness. Organizations that aligned their digital transformation with these models were better equipped to scale, adapt, and secure operations during crises like COVID-19, gaining a competitive edge (Teece, 2007).

Cloud Adoption in Fast-Changing Industries

Firms in fast-changing industries like fintech and digital media have consistently shown greater agility in adopting disruptive technologies due to rapid innovation cycles and a readiness to pivot (Christensen, Suarez and Utterback, 1998). A comparison with companies that adopted cloud computing during the COVID-19 pandemic reveals similar patterns.

Table 1: Fast-Changing Industries vs. COVID-Driven Transformation

Source: Own illustration based on (Henderson and Venkatraman, 1993; Christensen, Suarez and Utterback, 1998)

Dimensions	Fast-Changing Industries	COVID-19-Driven Digital Transformation
Trigger for change	Rapid technological evolution and competitive pressure force companies to innovate continuously	The external shock (COVID-19) forced businesses to adopt digital-first strategies overnight
Time of adoption	Firms must proactively invest in emerging technologies to stay ahead of the competition	Many businesses adopted Cloud Computing reactively due to crisis-driven urgency
Survival strategies	Early investment in digital infrastructure, organizational agility, and quick adaptation to technological shifts. Leveraging Dynamic Capabilities to remain competitive. Shifting to new business models (e.g., Netflix moving from DVDs to streaming)	Rapid adoption of Cloud Computing, AI, and automation. Shifting to remote work and digital business models (e.g., traditional retailers moving to e-commerce). Government-driven digital investments and funding programs
Resilience factors	Continuous innovation is key to survival. Companies that fail to transition to new technological paradigms (S-Curve shifts) risk becoming obsolete. Strong Dynamic Capabilities are essential for longevity	Firms with pre-existing digital infrastructure were more resilient during crisis. Companies with agile cloud-based models had a competitive advantage. Government policies accelerated digital transformation in regulated industries (e.g., healthcare, finance)

Firms with pre-existing digital capabilities adapted more effectively to external shocks. Their prior investments in innovation, agility, and digital infrastructure gave them a significant advantage during the crisis. In contrast, traditional firms faced steep catch-up pressures. The resilience strategies common in dynamic industries – continuous innovation, early cloud

adoption, and organizational flexibility – offer a model for firms undergoing reactive digital transformation. Those that embraced these approaches were better positioned to mitigate disruptions through cloud computing and dynamic capabilities (Christensen, Suarez and Utterback, 1998). These adoption patterns offer valuable insights into how cloud maturity influenced firms' ability to respond resiliently during the pandemic.

Building on the conceptual and literature-based insights, the next section explores how businesses can further optimize cloud use while mitigating risks tied to third-party provider dependency (Bellini *et al.*, 2018).

3 Methodology

3.1 Research Design

This study investigates how cloud computing has contributed to organizational resilience during the COVID-19 crisis and what strategic insights can be drawn for future disruptions. The research design followed a mixed-methods approach, combining qualitative and quantitative data collection and analysis techniques to triangulate findings (Creswell *et al.*, 2003), described in Figure 6.

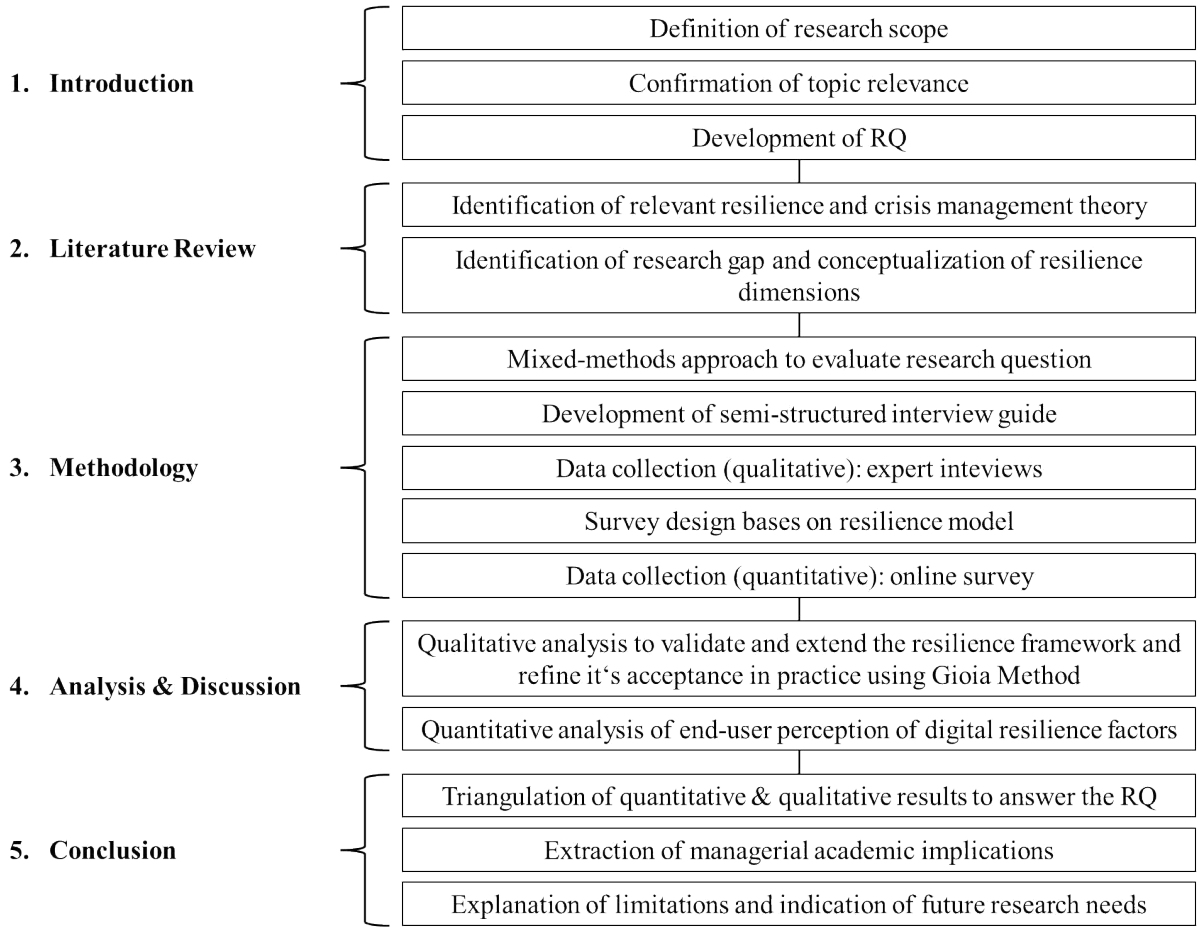

Figure 6: Overview of the research design

Source: Own illustration

A mixed-methods triangulation approach was chosen to answer the research question comprehensively. Triangulation enhanced validity of findings by integrating multiple perspectives and reducing biases inherent to single-method research (Sekaran and Bougie, 2009).

First, semi-structured expert interviews were conducted with industry professionals experienced in cloud computing, corporate resilience, crisis management, and business continuity. Interview data was analyzed using the Gioia Methodology (Gioia, Corley and Hamilton, 2013), enabling inductive coding and theory development across multiple abstraction levels. This interview format was chosen as it allows flexibility and in-depth exploration of complex phenomena, facilitating richer insights by encouraging interviewees to elaborate freely within predefined thematic areas (Qu and Dumay, 2011). The semi-structured approach also enabled systematic comparisons across participants while allowing for emergent, previously unidentified issues to surface, thereby enriching theoretical understanding.

Subsequently, quantitative data were collected through an online survey designed to explore how end-users perceive the resilience dimensions identified in the qualitative study, and to triangulate these perceptions with theoretical and expert insights. Surveys were selected due to their efficiency in capturing individual perceptions, attitudes, and measurable relationships among a broader group of end-users (Hair, Page and Brunsveld, 2019). Given the focus on perceptions rather than managerial decision-making, the sample comprised mainly students, young professionals, and seniors who experienced the COVID-19 disruption from a user perspective within educational or workplace settings.

Finally, the qualitative and quantitative results were triangulated to cross-validate the findings, ensuring robustness and comprehensive insight generation, thus providing clear strategic recommendations for enhancing corporate resilience in future crises.

3.2 Data Collection

The following chapter discusses the data collection methods used in Chapter 4.

3.2.1 Primary Data Collection: Expert Interviews

Semi-structured expert interviews are a common method in business and management research, particularly suitable for exploring complex phenomena through the collection of rich, detailed data (Bansal, Smith and Vaara, 2018). This interview method is ideal for understanding experts' viewpoints, experiences, and strategic decisions related to cloud computing and organizational resilience during crises (Rowley, 2012). A key strength of semi-structured interviews is their flexibility, allowing for the exploration of underlying motivations, beliefs, attitudes, and strategic insights, as experts can freely elaborate on topics raised (Barriball and While, 2013).

In this research, semi-structured expert interviews were chosen due to their suitability in gathering deep insights from individuals possessing extensive practical knowledge and strategic responsibility in crisis management and cloud adoption. The interviews enabled not only structured questioning based on theoretical constructs, but also allowed spontaneous follow-up questions that provided deeper exploration of unexpected, emergent topics (Turner, 2010; Magaldi and Berler, 2020). Furthermore, the format permitted attention to non-verbal cues, enhancing the comprehensiveness and interpretability of the data (Barriball and While, 2013; Seibold, 2020).

An interview guide, developed inductively from the literature review and preliminary identified resilience factors, structured the expert conversations. This guideline was essential for ensuring consistency, comparability, and reliability of the qualitative data (Rowley, 2012; Grossoehme, 2014). While providing a robust framework, the guide allowed flexibility to pursue new relevant insights arising during the discussions (Magaldi and Berler, 2020). As some of the interviews were held in German, those were translated into English.

The interview guide (see Appendix B) comprised approximately ten core questions, covering topics related to technological, operational, and strategic-organizational dimensions of resilience, cloud computing adoption decisions, and experiences during the pandemic. Interviews lasted around 30–45 minutes each, aligning with methodological standards in qualitative management research (Rowley, 2012). To supplement the qualitative findings with quantifiable insights, selected questions included Likert-scale components designed to gauge experts' perceptions quantitatively (Joshi *et al.*, 2015).

The selection of experts ensured representativeness and diversity in perspectives. Participants were identified and recruited through a range of professional channels, including personal networks, LinkedIn, e-mails, and referrals. Invitations were sent to approximately 200 potential participants, from which a final number of 12 experts were interviewed, ensuring data saturation within this methodological context (Guest, Bunce and Johnson, 2006). The experts, described in Table 2, reflect diverse professional backgrounds and roles, including technology executives, cloud transformation specialists, crisis and risk management professionals, strategic advisors, and researchers in innovation and organizational resilience.

Table 2: Overview and coded description of interviewees

Source: Own illustration

Code	Current position and expertise
Interviewee 1	Director at a consulting firm, with expertise in hybrid cloud architecture, enterprise IT modernization, and resilient digital infrastructures.
Interviewee 2	Senior associate in business process consulting at a professional services firm, with experience in enterprise cloud transformation projects and data resilience in retail and regulated industries.
Interviewee 3	Chief Technology Officer at a nonprofit cloud and data governance initiative, with expertise in trust architecture, federated digital ecosystems, and technology strategies for resilient infrastructure.
Interviewee 4	Director-level risk and project governance professional in the financial sector, with expertise in operational resilience, business continuity, and regulatory frameworks such as MaRisk, BAIT, and DORA.
Interviewee 5	Operational risk manager in the fintech sector, with expertise in scalable risk frameworks, crisis response, trading risk analytics, and business continuity planning.
Interviewee 6	Research associate in strategic management and innovation, with expertise in global value chain dynamics and how firms adapt to crises through innovation, outsourcing, and organizational change.
Interviewee 7	Senior crisis management advisor at a global industrial group, with expertise in strategic governance, group-wide coordination, and crisis preparedness at scale, including links to business continuity and situational intelligence.
Interviewee 8	Cloud Transformation Director at a consulting firm with expertise in infrastructure modernization, strategic cloud adoption, and resilience enablement in the German enterprise sector.
Interviewee 9	Distinguished Engineer at a leading cloud provider with expertise in cloud architecture, automation, and resilience engineering.
Interviewee 10	CTO for the automotive sector at a global cloud services provider, with expertise in platform architecture, cloud-native scalability, and enabling organizational resilience through modular infrastructure strategies.
Interviewee 11	Director for Cloud Transformation in the automotive sector at a consulting firm, with prior leadership experience in data and analytics at a major OEM and a strong focus on centralized data governance and cloud strategy execution.
Interviewee 12	Engineering lead at a SaaS company, with expertise in AWS cloud infrastructure, DevOps automation, and building resilient, scalable backend platforms.

Interviews were conducted remotely using the Microsoft Teams platform, facilitating ease of scheduling, effective documentation, and accessibility for geographically dispersed participants.

3.2.2 Primary Data Collection: Consumer Insights Survey

The literature review demonstrated the critical role of cloud computing adoption and user perceptions in enhancing organizational resilience during crises. Therefore, capturing end-users' experiences, perceptions, and acceptance of cloud computing technologies during the pandemic is essential to validate empirically the dimensions of resilience developed through qualitative expert insights and theoretical constructs.

The survey was disseminated online through various platforms (Instagram, WhatsApp, and LinkedIn), ensuring cost-effective data collection and the potential for rapid response rates (Fowler, 2018). The survey outline (see Appendix A) included approximately 18 questions, utilizing a combination of multiple-choice, demographic, 5-point Likert scales, and free text.

The questionnaire was structured into clearly defined sections, reflecting the following areas:

1. Self-assessed technical understanding and digital literacy
2. Experience with organizational crises or disruptions
3. Perception of digital tools as enablers of operational continuity and resilience
4. Evaluation of strategic and technological aspects of cloud computing
5. Perceived impact of cloud solutions on organizational learning and transformation
6. Demographic background for segmentation purposes

The survey conducted online was free from researcher interference and was available in English and German. The Qualtrics platform was utilized due to its robust design capabilities and user-friendly administration. The limitations of this quantitative approach, including possible sampling biases and the representativeness of respondents, will be further discussed in Chapter 5.2.

The survey was initiated by N = 153 participants. To ensure data quality, only respondents who completed all relevant items, including key variables related to cloud computing perception and organizational resilience, as well as demographic information, were retained for analysis. After listwise exclusion of incomplete cases, the final sample consisted of N = 137 valid responses.

Generally, a sample size within this range is deemed appropriate to achieve a margin of error between 5% and 10% at a confidence level of 95% for populations greater than 10,000 (Krejcie and Morgan, 1970; Barlett, Kotrlik and Higgins, 2001). This sample size will allow preliminary

insights into end-users' perceptions, contributing meaningfully to the overall analysis of cloud-enabled resilience. All statistical analyses, including correlation, regression, and scale validation, were conducted using IBM SPSS Statistics to ensure methodological reliability and replicability.

4 Analysis and Discussion

This chapter presents the empirical findings of this study and discusses them in light of the theoretical framework introduced in Chapter 2. The analysis is structured along three core dimensions of organizational resilience – *operational*, *technological*, and *strategic-organizational* – and concludes with an integrative synthesis.

Each dimension directly targets literature gaps identified in the theoretical review, especially regarding cloud-enabled and perception-based resilience. An overview of this mapping is provided in Table 3.

Table 3: Mapping of resilience dimensions to literature gaps
Source: Own illustration

Chapter 4 – Section	Analytical Focus	Addressed Literature Gap
4.1 Operational Resilience	Speed of response, business process continuity, remote readiness	Lack of empirical insight into cloud-based operational flexibility during crises
4.2 Technological Resilience	IT scalability, cloud maturity, infrastructure robustness	Lack of integrative resilience models
4.3 Strategic & Organizational Resilience	Decision-making, crisis leadership, cloud as a strategic enabler	Underexplored strategic role of cloud in navigating uncertainty
4.4 Integration and Synthesis	Interaction of dimensions, emergent capabilities, full model	Combined insights toward theory development

4.1 Qualitative Analysis

This chapter examines how cloud computing influences corporate resilience across *operational*, *technological*, *strategic-organizational*, *regulatory*, and *financial* dimensions, based on insights from twelve expert interviews. Participants ranged from cloud implementation consultants to infrastructure end-users, representing multinationals, SMEs, and start-ups. These contextual differences are considered throughout the analysis to ensure accurate interpretation.

The data was analyzed using the Gioia Methodology (Gioia, Corley and Hamilton, 2013), which supports inductive theory-building through structured coding. First-order concepts were drawn from interview data, grouped into second-order themes, and consolidated into aggregate dimensions (see Appendix B.4 & B.5). This approach ensured transparency between raw data and theoretical insight, strengthening analytical rigor.

4.1.1 Operational Resilience

Operational resilience refers to a firm's ability to maintain and restore core operations during disruptions, relying on business continuity, adaptability, robust processes, and coordinated response mechanisms (Tang, Dong and Zhou, 2025). It requires not only strong infrastructure but also agile processes and prepared personnel.

Interview findings highlighted operational resilience as a critical yet often underdeveloped aspect of cloud transformation. Eight out of twelve interviewees emphasized that cloud-based scalability and modularity allow firms to adapt quickly and reduce downtime during disruptions. Half specifically noted that modular cloud systems outperform traditional infrastructures in reconfiguring operations under pressure.

Proactive crisis preparation also emerged as essential. Interviewees stressed the importance of simulation exercises, strategic Business Continuity Planning (BCP), and real-time data access to ensure functionality of critical areas like finance and supply chain. Agile delivery models, particularly Development and Operations (DevOps), were cited as key enablers of operational adaptability. Real-time risk monitoring and early-warning systems were identified as critical tools (e.g., Key Risk Indicators (KRI)).

Human and cultural factors were repeatedly mentioned as decisive. Interviewees noted that resilience depends on clear ownership, trained crisis teams, and cultures that support fast, informed decision-making. Without these, technical capabilities alone fall short.

A notable example is Edeka, whose cloud-based checkout systems enabled continued operations across thousands of stores during peak pandemic disruptions, illustrating how modular architectures support rapid crisis response.

In sum, cloud computing enhanced operational resilience through scalability, responsiveness, and modular design. However, these benefits only translate into resilience when strategically integrated with organizational processes, cultural readiness, and proactive crisis management. This section directly contributes to the research question by providing empirical evidence of how cloud infrastructures enabled business continuity during COVID-19, addressing a gap in literature on the interaction between technology, planning, and human factors.

4.1.2 Technological Resilience

Technological resilience refers to an organization's ability to maintain core functionalities and adapt its IT infrastructure during disruptions (Teece, 2007). While cloud computing is widely seen as a key enabler, empirical evidence on its crisis-specific role has been limited.

Interview findings strongly supported its importance. In 11 of 12 interviews, cloud-native architectures and decoupled systems were identified as essential for rapid recovery and flexible crisis adaptation. Cloud-native architectures and architectural decoupling were consistently emphasized as key enablers for resilience, allowing faster recovery and more flexible crisis adaptation by 66% of the interviews. Key features cited include scalability, modularity, and real-time redundancy, validating theoretical models and pandemic-era observations (S-Curve model), where cloud-mature firms sustained operations more effectively.

However, three interviewees warned that resilience is not automatic. It requires proactive user-side configuration, encryption, and compliance management. Misunderstandings of the shared responsibility model and weak governance can create vulnerabilities. Security concerns persist in regulated sectors, though certifications like the International Organization for Standardization (ISO) and Security Operations Center (SOC) were seen to reduce audit complexity and enhance trust, especially for SMEs.

Human factors also play a vital role. Risks such as insider threats, lack of governance awareness, and low cloud literacy can undermine even strong technical setups. Thus, resilience depends not just on infrastructure but also on organizational capability and vigilance.

Overall, the findings confirmed that cloud-native systems enhance technological resilience, particularly when supported by strategic configuration, governance, and skilled personnel. This reflects the DCF. Firms that actively reconfigured their architecture and practices under pressure proved more adaptable. Netflix's use of AWS during demand surges exemplifies this, as do interview insights showing that pre-crisis cloud maturity correlated with superior resilience.

Regulatory Resilience

Regulatory resilience refers to an organization's ability to ensure compliance and operational continuity amid evolving legal and governance frameworks (Wagner, n.d.). In cloud

computing, this includes adherence to data protection laws (e.g., GDPR), cross-border governance, and shared responsibility models.

Interview findings highlighted the increasing influence of regulation on cloud resilience strategies. Interviewee 4 warned that misinterpreting shared responsibility often creates compliance risks, with firms wrongly assuming providers handle all legal obligations. Interviewee 5 emphasized tools like the Azure Compliance Center, which automate checks and aid audits, especially useful in sectors like finance. However, jurisdictional complexity and overreliance on technical solutions without internal governance were cited as adoption barriers.

Notably, regulatory mandates can enhance resilience. Interviewee 10 explained how requirements, particularly in banking, drive modular system designs that contain risks and reduce dependencies. Interviewee 3 added that regulations like Gaia-X promote trust through certification frameworks and decentralized architectures, transforming compliance from constraint to strategic enabler.

In summary, regulatory resilience is a key component of technological resilience. While cloud tools support compliance, true resilience depends on legal awareness, sound governance, and strategic system configuration. These findings address a gap in the literature by showing how regulatory standards actively shape resilient cloud strategies, insights directly relevant to navigating future crises.

4.1.3 Strategic & Organizational Resilience

Strategic and organizational resilience refers to a firm's ability to anticipate, adapt, and evolve its strategy, leadership, and culture in response to disruption. It involves aligning technological change with long-term business goals, supported by responsive leadership and adaptive decision-making (Marston *et al.*, 2010; Cheema-Fox *et al.*, 2021).

Interview findings showed that while cloud computing provides critical technical capabilities, it only strengthens resilience when embedded into broader strategic planning. 83% of interviewees noted that cloud transformations were often IT-driven and lacked strategic alignment, leading to missed opportunities during COVID-19. In contrast, firms that integrated cloud adoption into broader transformation efforts achieved stronger resilience outcomes. This reflects the DCF: organizations that sensed disruption early, seized opportunities, and reconfigured leadership and processes fared better.

Leadership understanding and commitment were seen as essential. C-level involvement, especially from CIOs and cross-functional teams, helped overcome resistance and steer strategic adoption. Exercises like tabletop crisis simulations supported organizational readiness. Interviewees also highlighted the role of culture: openness to change, accountability, and continuous learning were key enablers. Barriers included rigid mindsets, security fears, and low digital literacy. Organizational agility, supported by Minimum Viable Product (MVP) approaches and agile leadership, was identified as a success factor.

Effective resilience further required strong collaboration between IT and business units. Siloed initiatives often failed to deliver impact; cross-functional co-ownership proved critical. Vendor lock-in was viewed ambivalently. While it was criticized by some for reducing flexibility, others saw it as a trade-off for scalable redundancy.

The OpenTable case illustrates strategic resilience in action: leveraging cloud platforms, the company quickly adapted its model during the pandemic, supporting restaurants with takeout and real-time booking tools. This alignment of cloud use with broader business strategy underscores the value of strategic integration.

In sum, resilience is not a byproduct of cloud adoption but a strategic and organizational achievement. Leadership engagement, cultural readiness, cross-functional collaboration, and alignment of cloud initiatives with business goals are essential. These findings fill a critical literature gap by showing how strategic intent and cultural factors shape the outcomes of technology-driven transformation.

Financial Resilience

Financial resilience, a key subdimension of strategic resilience, refers to a firm's ability to maintain liquidity, absorb shocks, and sustain investments during crises (Blackrock, 2024). In the context of cloud adoption, it determines whether firms can scale infrastructure, maintain redundancy, and fund resilience-enhancing technologies under economic uncertainty.

Interview findings confirmed that financial resilience significantly influences technological and organizational adaptability. Interviewee 4 noted that frameworks like Basel III strengthen liquidity and risk reporting, supporting continued cloud investments during crises. Interviewee 5 emphasized that only cloud solutions offering clear scalability and strategic value were

retained during the pandemic, while Interviewee 2 pointed to predictable cost structures as a driver behind the shift to SaaS, especially in downturns.

Conversely, financial constraints were a major barrier to implementing redundancy, a critical enabler of technological resilience. As Interviewee 5 observed, budget limitations often delayed essential infrastructure upgrades.

From an RBV perspective, financial flexibility is a key resource enabling cloud-based resilience. Firms with robust financial strategies maintained investments and secured systems, while constrained firms fell behind.

These findings addressed a literature gap by showing how financial resilience shapes cloud-driven adaptability during crises. It ensures survival and creates strategic room to invest and evolve under uncertainty, highlighting its role in enabling resilience strategies.

4.1.4 Integration and Synthesis

This section synthesizes the qualitative findings, identifying key patterns, tensions, and cross-dimensional enablers of resilience in cloud-enabled organizations. It emphasizes the interdependence of resilience dimensions and highlights emergent themes that go beyond existing literature.

The analysis showed that while cloud computing enables *technological*, *strategic*, and *operational* resilience, its full potential depends on proactive strategic alignment, cultural readiness, and thoughtful system design.

Interaction between Resilience Dimensions

This section synthesizes the qualitative findings by highlighting the interconnectedness of technological, operational, strategic, financial, and regulatory resilience. In line with the qualitative research design (Gioia, Corley and Hamilton, 2013) transversal enablers, particularly human and cultural factors, are considered integral to the analysis, as resilience emerges from cross-dimensional interactions rather than isolated efforts.

The findings revealed that resilience dimensions are deeply interlinked and mutually reinforcing. Technological resilience, for instance, enables operational resilience by providing modular and scalable cloud architectures that support rapid adaptation and business continuity.

Several interviewees noted that firms with cloud-native systems were more effective in reconfiguring operations and maintaining critical services under pressure.

Strategic foresight and long-term integration of cloud technologies further amplified technological and operational capabilities. Organizations that embedded cloud adoption into broader transformation strategies demonstrated stronger resilience, while those with reactive, IT-led implementations struggled to fully realize its potential. This contrast was underscored by 25% of interviewees.

Financial and regulatory resilience acted as boundary conditions, defining the scope within which firms could build technological and operational robustness. Liquidity and financial flexibility enabled continued investment in cloud-based redundancy and scaling capacity, even during crises. Likewise, compliance requirements shaped architectural decisions, encouraging modularization and jurisdictional alignment. Interviewees 3, 4, and 5 emphasized that such frameworks indirectly enhanced resilience by enforcing structural safeguards.

Finally, human and cultural factors emerged as the binding force across all dimensions. Organizational culture, leadership commitment, and openness to change played a decisive role in translating technological potential into actual resilience. Without these enablers, strategic cloud adoption efforts often remained isolated within IT departments, limiting their impact. Leadership vision was seen as crucial for driving operational agility and strategic adaptability, whereas risk-averse or rigid mindsets were cited as barriers, especially in larger organizations.

In sum, the findings emphasized that corporate resilience in cloud-enabled environments is not the product of a single dimension, but rather an emergent outcome of the dynamic interplay between technology, strategy, operations, governance, and culture. Resilience requires coordinated action across all these fronts; none of them is sufficient in isolation.

Contrasting Perspectives Identified in the Interviews

While common themes emerged around cloud computing's role in enhancing resilience, several contrasting views revealed key tensions in strategy, technology, and risk perception, highlighting the complexity of cloud-enabled resilience.

A central divergence concerned vendor lock-in. Interviewee 3 saw dependency on a single provider as a strategic risk, advocating for open standards and frameworks like Gaia-X.

Conversely, Interviewee 9 viewed lock-in as a necessary trade-off for operational resilience, offering scalability, redundancy, and recovery "*as a service*." About 25% of interviewees echoed concerns over strategic dependence, while others, especially from tech-driven firms, accepted lock-in pragmatically.

Strategic integration of cloud technologies also varied. Interviewees 10 and 8 described cloud as a core strategic enabler of resilience and competitiveness. In contrast, Interviewees 2 and 7 observed that many organizations approached cloud adoption reactively and without strategic anchoring, depending on leadership priorities and limiting its long-term impact.

Perspectives concerning on-premise systems differed as well. In regulated sectors like banking and healthcare, Interviewees 4 and 5 defended on-premise solutions for data sovereignty and compliance. Others, including Interviewee 3, argued that such reliance limits agility, scalability, and crisis adaptability.

Timing of adoption was another point of contrast. Some firms (Interviewees 10 and 12) proactively invested in cloud infrastructure and showed higher resilience during the pandemic. Others (Interviewees 7 and 8) responded only after disruptions occurred. This reflects the DCF concept of “seizing” opportunities before crises escalate and undermines the S-Curve model (Teece, 2007).

Interviewees also differed in how they viewed the nature of cloud transformation – either as a strategic investment or a reactive update driven by outdated systems and competitive pressure (Interviewees 2, 7). Industry context influenced this as well. Automotive firms preferred phased adoption to manage complexity (Interviewees 10, 11), while tech-driven companies favored rapid transformation to gain early advantages (Interviewees 6, 9).

Finally, views on regulation varied. Interviewee 3 emphasized that compliance should be seen not as a constraint but as a chance to build trusted ecosystems through standardization and certification. Others primarily viewed regulation as a barrier to speed and innovation.

Emergent Themes Beyond the Literature

While existing literature provides a strong foundation for understanding technological, operational, and strategic resilience, the interviews surfaced additional themes that expand and refine these frameworks.

Interviewee 9 emphasized Mean Time to Recovery (MTTR) as a more practical metric than system uptime, reframing resilience as the ability to recover quickly rather than avoid failure. Across interviews, cultural openness, continuous learning, and employee development were repeatedly identified as essential to realizing the full value of technological investments. Without these human enablers, resilience remains limited.

Several interviewees also stressed the importance of modular, decoupled cloud architectures to contain disruptions and increase flexibility, moving away from rigid, monolithic systems.

A nuanced pattern emerged around trust in cloud providers. AWS and Azure were preferred over GCP and especially Chinese providers like Alibaba, with strategic concerns, such as compliance, data sovereignty, and geopolitical stability, shaping decisions. European firms increasingly view regulatory frameworks (e.g., GDPR, the EU Data Act) as active drivers of resilience planning, not just constraints.

Scalability was recognized not only for technical efficiency but also as a strategic asset. Firms with scalable cloud infrastructures adjusted more easily to demand shifts and maintained operations under volatile conditions.

Another key theme was the visibility of organizational dependencies. Interviewee 10 highlighted the challenge of managing complexity in large firms, while Interviewee 7 warned that poor transparency across business units weakens resilience. Modularization helps, but does not fully resolve this issue. Interviewee 3 recommended advanced tools like four-dimensional Digital Twins and unified Trust Frameworks to improve traceability and systemic awareness.

Together, these insights suggested that cloud-enabled resilience requires a holistic strategy, one that integrates technical, organizational, human, and geopolitical factors into a unified approach.

4.2 Quantitative Analysis

To validate the resilience framework and these qualitative insights and test their generalizability, this quantitative study explores how internal stakeholders perceive cloud computing as a driver of organizational resilience, focusing on digital readiness and adaptability across three dimensions: *operational*, *technological*, and *strategic-organizational* resilience.

The analysis is based on 137 complete responses covering cloud usage and resilience perceptions.

Addressing a gap in the literature, typically focused on decision-makers, this study highlights how consumers and technically informed end-users assess cloud technologies during crises. It offers empirical insights into how digital infrastructure supports resilient strategies and operations. By linking RBV and DCF frameworks with real-world data, the survey strengthens the research foundation and offers strategic guidance for future disruptions. The next section outlines the sample's demographic profile.

4.2.1 Demographics and Background

The sample was skewed toward younger respondents, with 67.9% under 35 and the largest group aged 25–34 (47.4%), indicating a potential age bias toward digitally inclined perspectives.

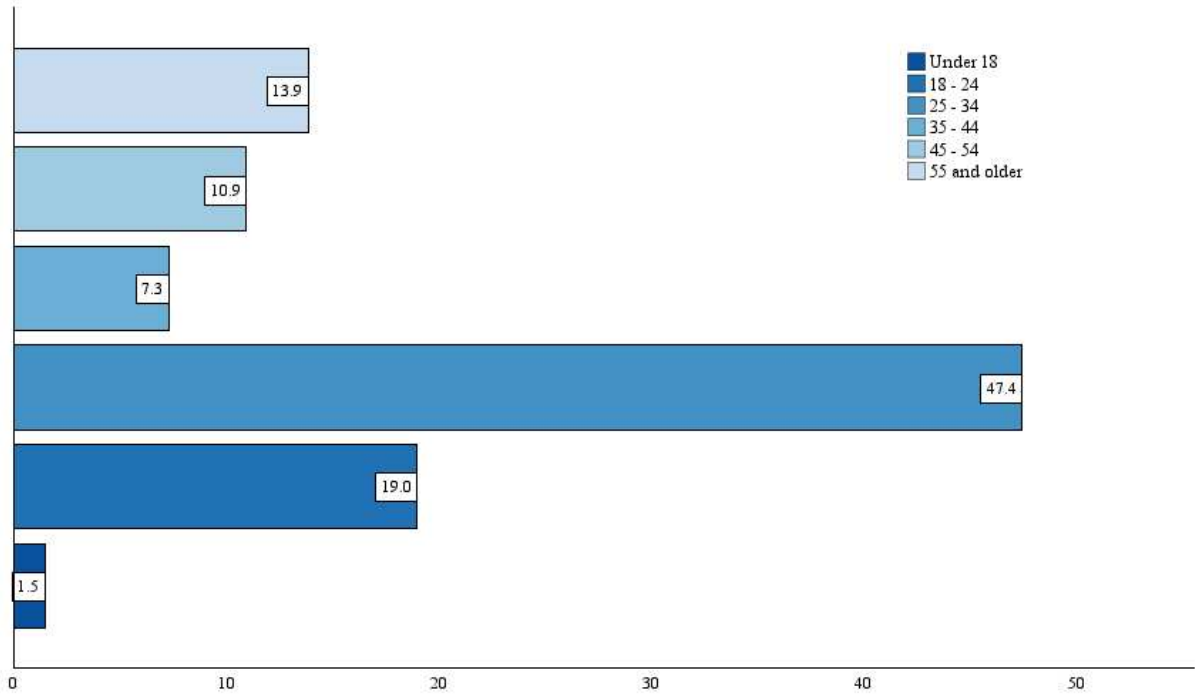

Figure 7: Answer distribution of Q14

Source: Own illustration

Gender distribution showed 62.8% female and 36.5% male, with one participant opting not to disclose. While not fully balanced, gender was not a focus variable and is unlikely to affect the results.

The next question asked respondents about their highest level of education.

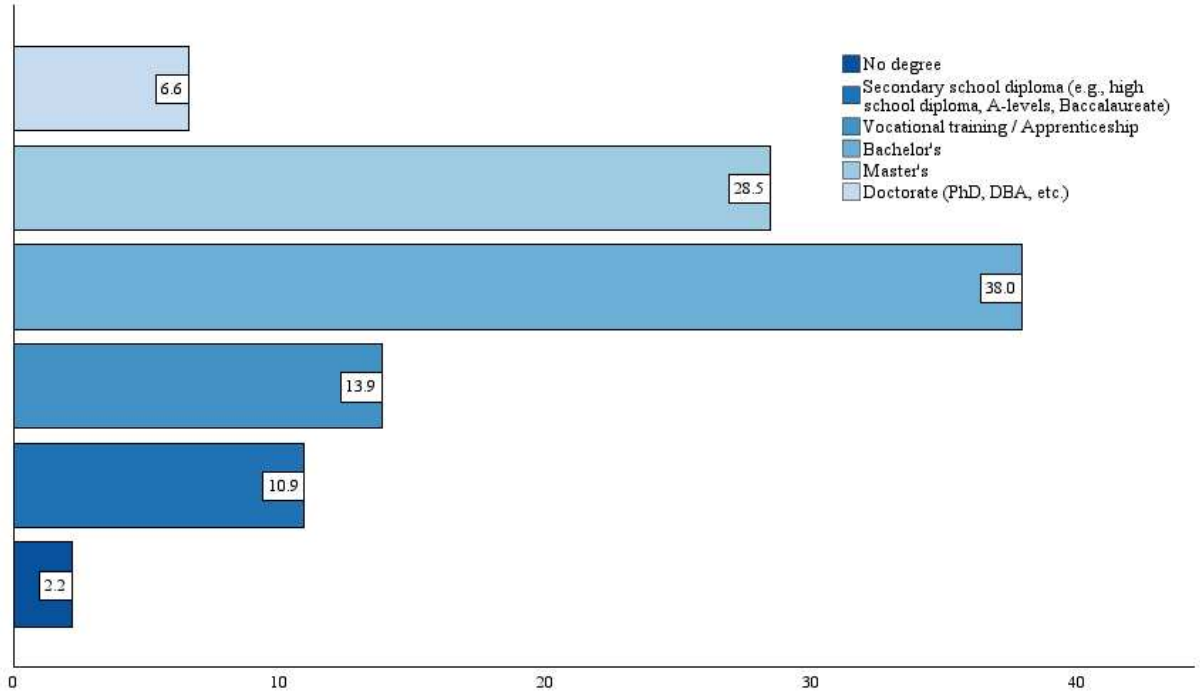

Figure 8: Answer distribution of Q16

Source: Own illustration

Educational attainment was high: 73.1% held at least a bachelor's degree, while only 2.2% had no degree and 10.9% reported secondary education only. This suggests a digitally literate, knowledge-oriented group with greater access to remote work and digital tools than the general population (OECD, 2024).

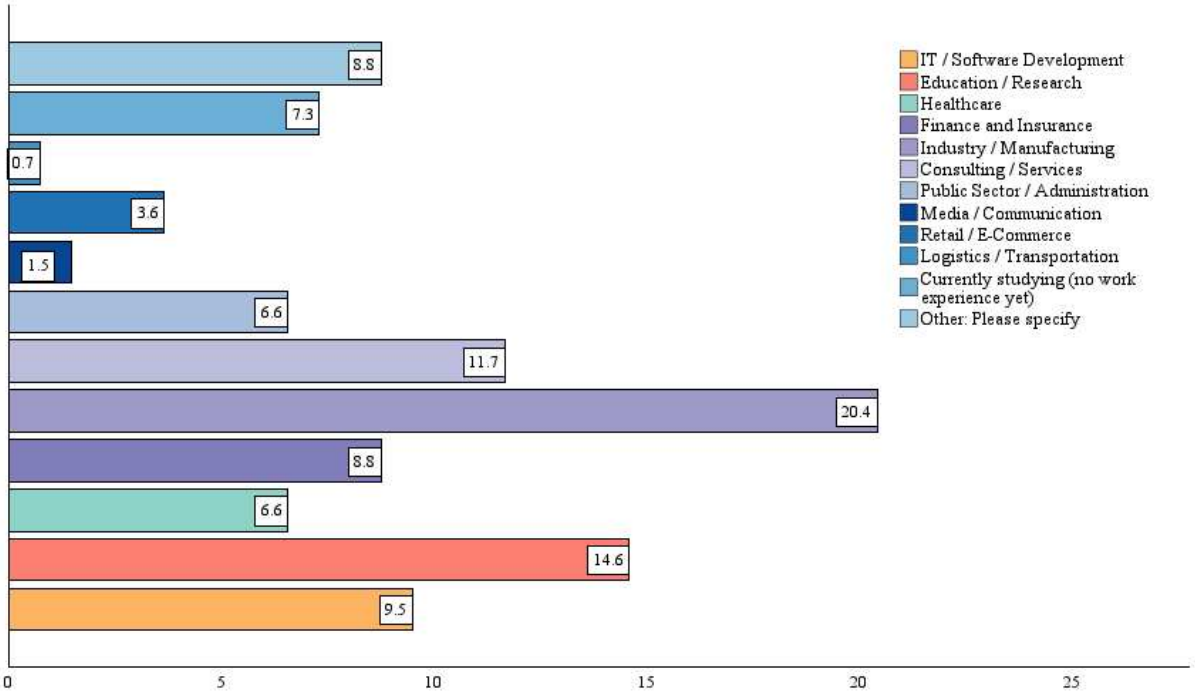

Figure 9: Answer distribution of Q17

Source: Own illustration

Participants represented diverse professions, with the most common sectors being industry/manufacturing (20.4%), education/research (14.6%), and consulting/services (11.7%). Only 9.5% worked directly in IT, indicating the sample was not overly tech-centric. However, many came from digitally progressive sectors, supporting a balanced cross-industry view of resilience.

Finally, 62.8% of respondents lived in cities with over 100,000 inhabitants, suggesting higher exposure to digital infrastructure and remote work factors likely influencing their views on cloud-based resilience.

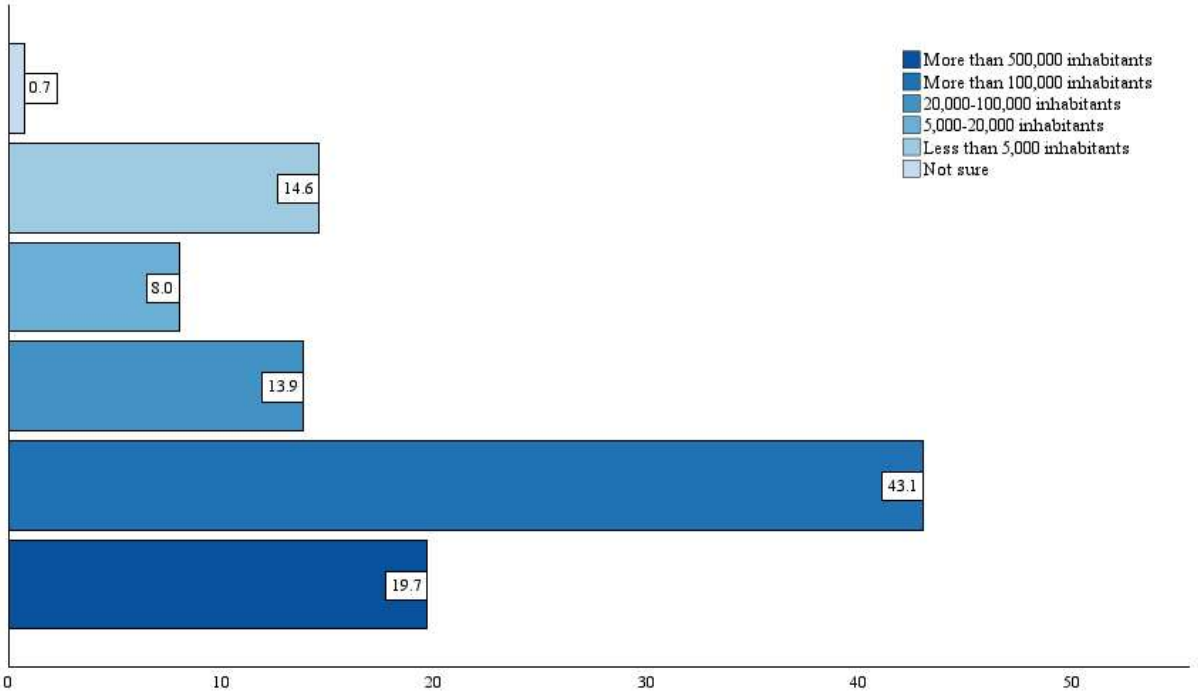

Figure 10: Answer distribution of Q18

Source: Own illustration

4.2.2 Perception of Organizational Resilience and the Role of Digital Tools

To assess the practical experience of respondents with organizational disruptions, participants were asked Q1 whether they had previously witnessed how an organization dealt with a crisis or disruption. A clear majority of 89.8 % (n = 123) answered yes, indicating that they had direct experience with crises in a professional context. This high level of practical exposure suggests that most participants were familiar with real-world organizational responses and challenges. Such experience may shape their perception of resilience-enabling technologies and increase awareness of the value of digital tools in maintaining continuity and adaptability during disruptions.

Participants also assessed their technical understanding and views on digital tools (Q13_1) using a 5-point Likert scale. Agreement with the statement "*[...] digital tools help companies operate during crises*" averaged M = 4.23, while self-rated technical understanding averaged M = 4.17. Both showed low standard deviations, suggesting relatively consistent responses across the sample (Derbyshire, 2017).

Table 4: Belief in digital support and competence

Source: Own illustration

	N	Mean	Std. Deviation
Q13_1	137	4.23	.730
Q13_6	137	4.17	.772

These findings indicated that participants were not only digitally confident but also strongly associated digital tools, particularly cloud services, with organizational resilience. This supported the literature emphasizing the strategic role of digital adaptability in dynamic environments (Hamel and Välikangas, 2003).

4.2.3 Perceived Resilience Dimensions

Building on prior findings, this section introduces four perceived dimensions of organizational resilience derived from theory, expert interviews, and survey data. Three core dimensions – *Operational Resilience*, *Technological Resilience*, and *Strategic & Organizational Resilience* – are based on the theoretical model from the literature. An additional, exploratory dimension, *Culture & Leadership*, emerged from interviews highlighting the role of transparent leadership and adaptive culture. These dimensions guide the subsequent hypothesis development.

Table 5 summarizes the survey items, descriptive statistics, and internal consistency measures assigned to each dimension.

Table 5: Overview of resilience dimensions and assigned survey items

Source: Own illustration

Resilience Dimension	Idem Code	Aggregation	Cronbach's Alpha	Pearson r	Mean (M)	Standard Deviation (SD)
Operational	Q2_1	Single item	n.a.	n.a.	3.10	1.09
Technological	Q13_2 + Q13_3	Yes (with limitations)	0.42	0.27	3.79	0.66
Strategic & Organizational	Q6_1	Single item	n.a.	n.a.	3.66	0.92
Culture & Leadership (Culture)	Q4_1	No (very low correlation)	0.11	0.07	4.47	0.62
Culture & Leadership (Leadership)	Q4_2	No (very low correlation)	0.11	0.07	3.25	1.06

Operational resilience reflects perceived preparedness for disruptions. The mean score of 3.10 suggested moderate agreement, with high variability indicating differing experiences across respondents. The near-symmetrical distribution supported a balanced perception of organizational readiness.

Technological resilience combines perceptions of digital usability and data security. A relatively high mean of 3.79 and low standard deviation (0.66) indicated broad agreement that tools like cloud services are accessible and reliable. Although internal consistency was below standard thresholds, a moderate and significant correlation between the items supported using a composite score for exploratory purposes.

Strategic & Organizational resilience captured strategic learning and post-crisis adaptation. With a mean of 3.66 and moderate variation, the results suggested general agreement that organizations improved preparedness based on prior crises.

Culture & Leadership included two items on cultural openness and internal transparency. Cultural openness received strong consensus, while perceptions of transparency varied more widely. The weak, non-significant correlation indicated that items measured distinct constructs and should not be combined. Culture & Leadership was introduced as an exploratory theme despite conceptual overlaps with Strategic & Organizational Resilience. As such, it was not treated as a standalone outcome in hypothesis testing but analyzed alongside other dimensions to explore links between operational and technological resilience. This approach reflected the embedded nature of culture in broader resilience frameworks.

Methodological Note on Scale Construction and Validity

While multi-item scales are generally preferred for reliability, single- and two-item measures are acceptable in perception-based organizational research when conceptually justified (Fisher, Matthews and Gibbons, 2015). This is particularly relevant in exploratory studies with clearly defined constructs.

For two-item constructs in this study (*Technological and Culture & Leadership*), internal consistency was assessed using both Cronbach's Alpha and Pearson's correlation. Aggregation was applied only when items were conceptually aligned and showed at least a moderate correlation ($r \geq 0.30$), as recommended for short scales (Cohen, 1988).

Given Cronbach's Alpha's sensitivity to item count, Pearson's r offered a more reliable consistency check in such cases (Eisinga, Grotenhuis and Pelzer, 2013). When internal consistency was insufficient, items were analyzed separately within their conceptual dimension.

4.2.4 Drivers of Perceived Resilience

The survey revealed notable differences in how respondents perceive organizational resilience. While adaptive culture was broadly valued, views on preparedness and transparency varied. To explain these differences, four hypotheses were developed based on the conceptual model and literature.

A two-step analysis was used: first, bivariate correlations (Pearson's r) identified significant associations; then, regression models assessed the predictive strength of relevant variables. Linear regression was applied to composite scales (e.g., Technological Resilience), assuming approximate interval-level properties (Carifio and Perla, 2009; Norman, 2010). For single-item variables or ordinal outcomes, ordinal regression and non-parametric tests (Spearman's rho, Kendall's Tau-b) were used as appropriate. This mixed-method approach balances rigor and interpretability in exploratory research.

Table 6 outlines the hypotheses, related survey items, and variables used (single or aggregated).

Table 6: Overview of hypothesis and survey item assignments
Source: Own illustration

Hypothesis	Independent Variable (IV)	IV Question(s)	Dependent Variable (DV)
H1	Adaptation Speed	Q11: Speed of digital adoption during crisis Q12: Speed of digital adaptation today	Operational Resilience
H2	Belief in Digital Tools	Q13_1: Digital tools help companies operate during crises	Technological Resilience
H3	Dependency View	Q6_2: Less dependency enhances resilience	Strategic & Organizational Resilience
H4a1	Adaptive Culture	Q4_1: Open, adaptive culture supports process adaptation	Operational Resilience
H4a2	Transparent Communication	Q4_2: Decisions and information are communicated transparently	Operational Resilience
H4b1	Adaptive Culture	Q4_1: Open, adaptive culture supports process adaptation	Technological Resilience
H4b2	Leadership Communication	Q4_2: Decisions and information are communicated transparently	Technological Resilience

The following section briefly introduces each hypothesis and outlines the rationale behind the expected relationships between variables.

> *H1*: Participants who perceive digital systems as adaptable during crises and in the present day are more likely to rate their organizations as operationally resilient.

H2: Participants who believe that digital tools help companies continue operating during crises are more likely to perceive higher technological resilience.

H3: Participants who believe that organizations are more resilient when they are less dependent on individual systems, people, or service providers are more likely to report that their organization has learned from the COVID-19 crisis and is now better prepared for future disruptions.

H4a1: Participants who perceive their organization as having an open, adaptive culture are more likely to report higher operational resilience.

H4a2: Participants who perceive leadership communication of decisions and information as transparent are more likely to report higher operational resilience.

H4b1: Participants who perceive their organization as having an open, adaptive culture are more likely to report higher technological resilience.

H4b2: Participants who perceive leadership communication of decisions and information as transparent are more likely to report higher technological resilience.

To assess whether the hypothesized relationships were empirically supported, bivariate correlation analyses were conducted. Table 7 summarizes the observed effect sizes, significance levels, and the type of regression applied for each hypothesis.

Table 7: Bivariate correlations and regression type by hypothesis

Source: Own illustration

Hypothesis	Regression	Pearson r	Spearman's ρ	Kendall's τ-b	p-value (nicht Pearson)	N
H1	Ordinal	0.323	0.329	0.270	< .001	103
H2	Linear	0.312	n.a.	n.a.	< .001	137
H3	No	0.121	0.114	0.102	.184 (Spearman)	137
H4a1	Ordinal	0.180	0.212	0.190	.013 (both)	137
H4a2	Ordinal	0.405	0.386	0.332	< .001 (both)	137
H4b1	No	0.073	n.a.	n.a.	.394	137
H4b2	Linear	0.377	n.a.	n.a.	< .001	137

H1 and *H2* were supported: digital adaptability was significantly linked to operational resilience, and belief in digital tools correlated with technological resilience, aligning with both theory and qualitative findings.

H3 was not supported. While the relationship was directionally positive, it lacked statistical significance, suggesting a disconnect between abstract beliefs about structural resilience and perceived organizational learning. This suggests that general beliefs about structural resilience do not automatically translate into perceived learning or preparedness, emphasizing the importance of tangible cloud capabilities over abstract principles.

H4 was assessed through four sub-hypotheses. Transparent leadership communication (Q4_2) showed significant positive associations with both operational (*H4a2*) and technological resilience (*H4b2*). This is illustrated in Figure 11, where higher transparency ratings correspond to higher resilience scores.

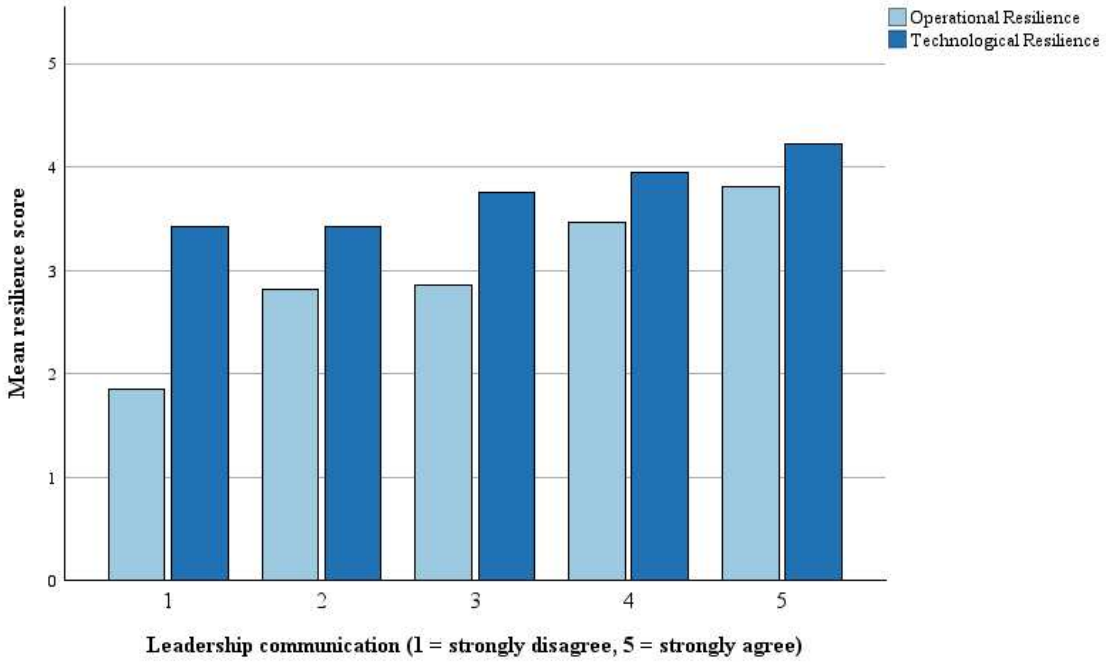

Figure 11: Mean resilience scores by perceived transparency in communication

Source: Own illustration

In contrast, adaptive culture (Q4_1) had only a weak link to operational resilience (*H4a1*) and no significant relationship with technological resilience (*H4b1*), as shown in Figure 12. These findings suggested that transparent communication might play a more decisive role in resilience perceptions than cultural openness, an observation echoed in the interviews.

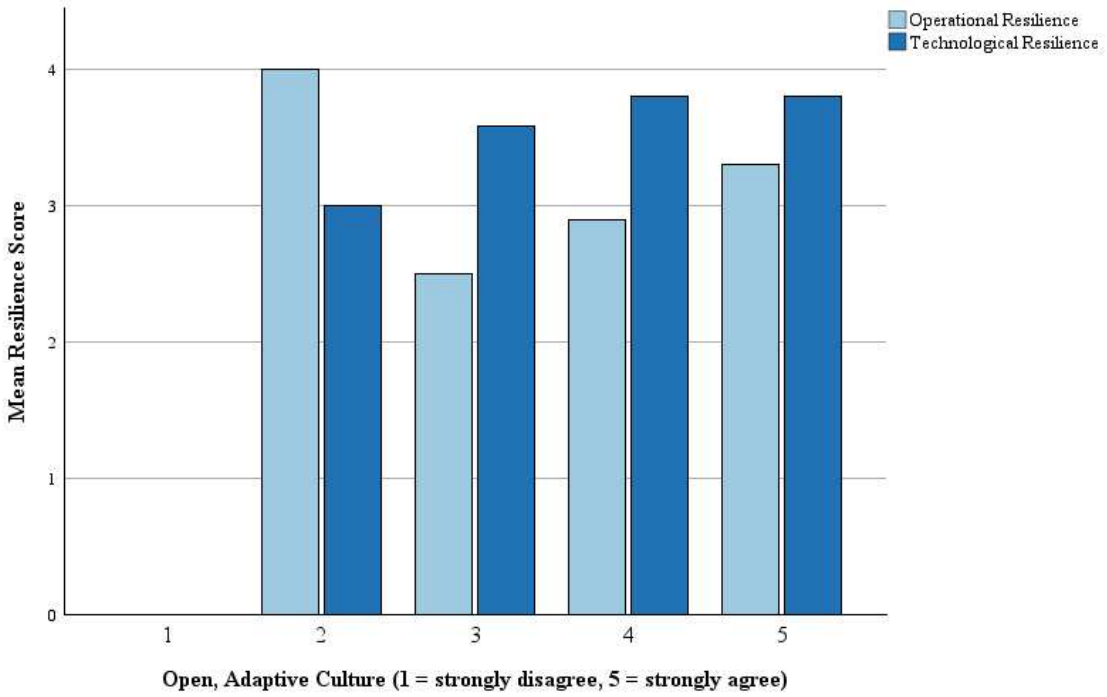

Figure 12: Mean resilience scores by perceived adaptive culture

Source: Own illustration

Regression Analysis and Model Validation

To assess the predictive strength of supported hypotheses, regression models were calculated based on significant bivariate results. All models met the required statistical assumptions, ensuring validity and interpretability. Depending on the dependent variable, either linear or ordinal regression was applied.

Table 8: Summary of assumptions checks for regression models

Source: Own illustration

Model	Linearity	Normality of Residuals	Homoscedasticity	Multicollinearity (VIF)	Proportional Odds (only ordinal)	Model Fit (only ordinal)
H1	n.a.	n.a.	n.a.	n.a.	0.196	Pearson p = .705 Deviance p = .511
H2	✔	✔	✔	n.a. (1 UV)	n.a.	n.a.
H4a1 + H4a2	n.a.	n.a.	n.a.	n.a.	0.266	Pearson p = .620 Deviance p = .478
H4b2	✔	✔	✔	n.a. (1 UV)	n.a.	n.a.
H1 + H4a1 + H4a2 (Combined)	n.a.	n.a.	n.a.	n.a.	0.436	Pearson p = .632 Deviance p = .990
H2 + H4b2 (Combined)	✔	✔	✔	1.132	n.a.	n.a.

Table 8 summarizes the assumption checks; full residual diagnostics are provided in Appendix C.

H1: Adoption Speed and Operational Resilience

To test *H1*, an ordinal logistic regression was conducted with perceived operational resilience as the dependent variable and perceived digital adaptation speed as the predictor (N = 103).

Table 9: Regression results for H1

Source: Own illustration

Predictor	Estimate (B)	SE B	Wald χ^2	p	95 % CI Lower	95 % CI Upper
Adaption_Speed	0.842	0.256	10.792	.001	0.340	1.344
Model Fit & Validity	**Value**					
Model Significance (Chi², df = 1)	11.288, p < .001					
Pearson Goodness-of-Fit (df = 23)	χ^2 =18.928, p = .705					
Deviance Goodness-of-Fit (df = 23)	χ^2 = 22.160, p = .511					
Test of Parallel Lines (df = 3)	χ^2 = 4.693, p = .196					
Pseudo R^2 (Nagelkerke)	.111					

Table 9 shows that the model was statistically significant, indicating that the predictor contributes meaningfully to explaining variance in resilience. Nagelkerke's R^2 was .111, suggesting moderate explanatory power. The coefficient for adoption speed was positive and significant, indicating that faster perceived adaptation increases the likelihood of higher crisis preparedness.

The results suggested that organizations seen as more digitally responsive, during and beyond the COVID-19 crisis, were also perceived as more resilient. This highlights digital agility, especially cloud-enabled responsiveness, as a key factor in maintaining operational continuity and crisis readiness.

H2: Belief in Digital Tools and Technological Resilience

H2 was tested using a simple linear regression with perceived technological resilience as the dependent variable and belief in digital tools (Q13_1) as the predictor (N = 137).

Table 10: Regression results for H2

Source: Own illustration

Variable	B (Unstandard.)	SE B	β (Standard.)	t	p
Constant	2.605	0.315	–	8.266	< .001
Q13_1 (Belief in Digital Tools)	0.280	0.073	0.312	3.810	< .001
Model fit					
R^2 = 097					
Adjusted R^2 = 0.090					
F(1, 135) = 14.519					p < .001
Durbin-Watson = 1.957					

A stronger belief in the usefulness of digital tools is associated with higher levels of perceived technological resilience, suggesting that trust in digital continuity solutions is a relevant factor in shaping resilience perceptions. The model was statistically significant and explained 9.7% of the variance. A one-point increase in belief that digital tools support crisis continuity was associated with a 0.28-point increase in perceived technological resilience.

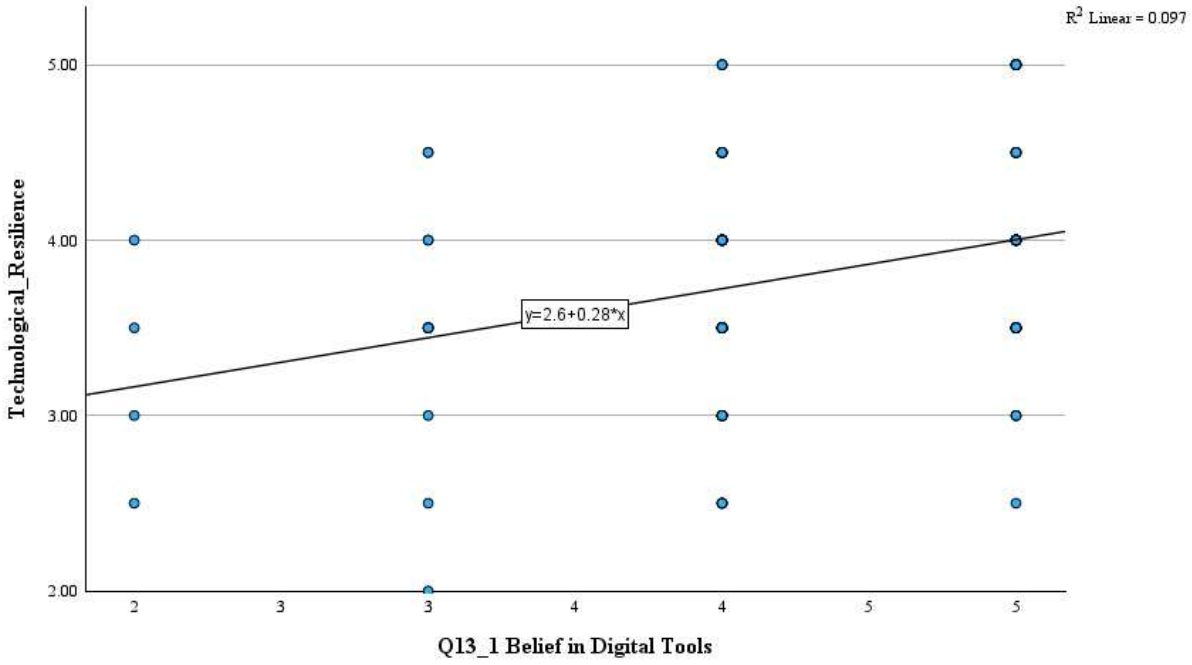

Figure 13: Effect of Belief in Digital Tools on Technological Resilience

Source: Own illustration

The results indicated that trust in digital infrastructure, especially cloud-based solutions, not only reflected usage but also reinforced perceptions of technological reliability. Confidence in digital tools, therefore, played a key role in shaping resilience perceptions.

H4a1 and H4a2: Leadership Communication and Culture on Operational Resilience

An ordinal logistic regression was conducted to test whether adaptive culture (Q4_1) and leadership communication (Q4_2) influence perceived operational resilience (Q2_1).

Table 11: Regression results for H4a1 and H4a2

Source: Own illustration

Predictor	Estimate (B)	SE B	Wald χ^2	p	95 % CI Lower	95 % CI Upper
Q4_1 (Adaptive Culture)	0.464	0.259	3.198	.074	–0.045	0.972
Q4_2 (Leadership Communication)	0.758	0.162	21.924	< .001	0.441	1.076
Model Fit & Validity	**Value**					
Model Significance (Chi², df = 2)	27.243, p < .001					
Pearson Goodness-of-Fit (df = 54)	χ^2 = 50.258, p = .620					
Deviance Goodness-of-Fit (df = 54)	χ^2 = 53.899, p = .478					
Test of Parallel Lines (df = 6)	χ^2 = 7.639, p = .266					
Pseudo R^2 (Nagelkerke)	.192					

These results suggested that leadership communication was a more consistent and influential factor than general cultural openness when it comes to perceptions of operational crisis preparedness. This aligned with previous bivariate results and reinforced the importance of communicative clarity in building resilience. As shown in Table 11, the model was statistically significant and met all assumptions, with a Nagelkerke of .192 indicating moderate explanatory power. Leadership communication had a significant positive effect, suggesting that transparent communication strongly shapes perceptions of crisis preparedness. Adaptive culture showed a positive trend but did not reach significance.

These findings confirm that while cultural openness alone offered limited predictive value, transparent communication played a more decisive role in operational resilience, highlighting the importance of clarity and coordination during disruptions.

H4b2: Leadership Communication and Technological Resilience

A simple linear regression tested the relationship between leadership communication (Q4_2) and perceived technological resilience (N = 137).

Table 12: Regression results for H4b2

Source: Own illustration

Variable	B (Unstandard.)	SE B	β (Standard.)	t	p
Constant	3.033	0.168	–	18.067	< .001
Q4_2: Leadership Communication	0.232	0.049	0.377	4.730	< .001
Model fit					
$R^2 = 0.142$					
Adjusted $R^2 = 0.136$					
$F(1, 135) = 22.377$					$p < .001$
Durbin-Watson = 2.061					

The model was statistically significant and explained 14.2% of the variance, reinforcing the relevance of communicative clarity in digitally resilient environments. A one-point increase in perceived communication transparency was associated with a 0.232-point increase in technological resilience.

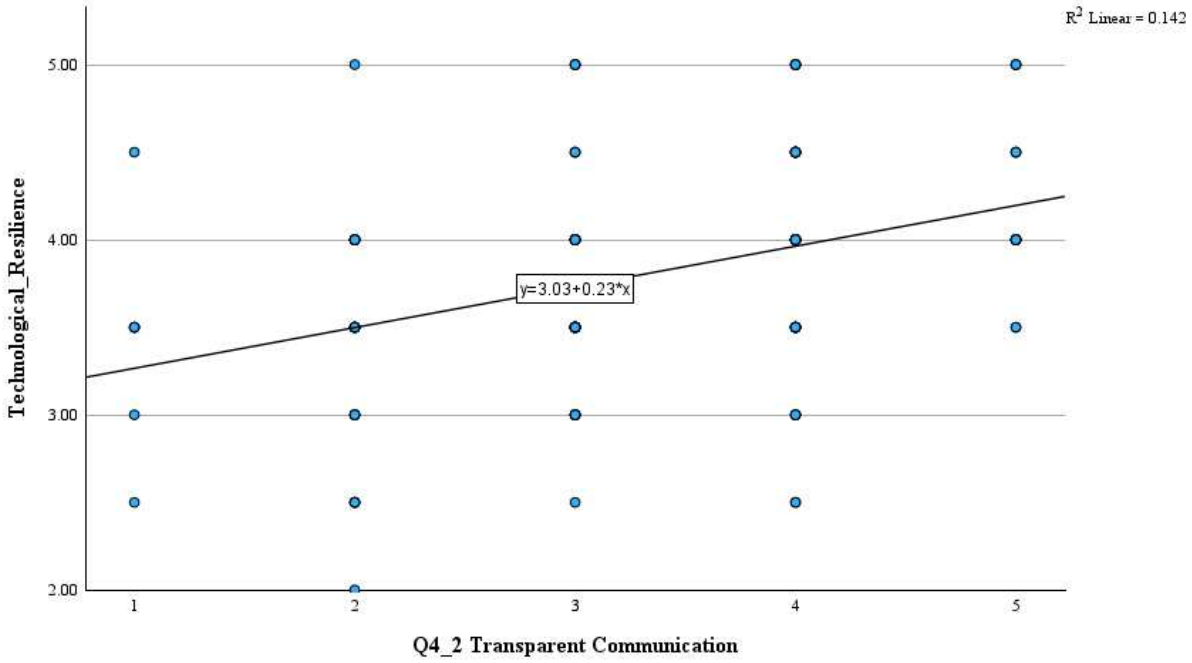

Figure 14: Effect of Leadership Communication on Technological Resilience

Source: Own illustration

Figure 19 illustrates this relationship. The findings supported *H4b2*, showing that transparent leadership communication strengthened perceptions of digital robustness. This suggested that internal communication not only influenced culture but also shaped trust in digital systems during crises.

H1 + H4a1 + H4a2: Impact of Adoption Speed, Adaptive Culture, and Leadership Communication on Operational Resilience

An ordinal logistic regression tested the combined impact of digital adaptation speed (*H1*), adaptive culture (*H4a1*), and leadership communication (*H4a2*) on perceived operational resilience (Q2_1).

Table 13: Regression results for H1, H4a1, and H4a2

Source: Own illustration

Predictor	Estimate (B)	SE B	Wald χ^2	p	95 % CI Lower	95 % CI Upper
Q4_1 (Adaptive Culture)	0.444	0.328	1.837	.175	–0.198	1.087
Q4_2 (Leadership Communication)	0.726	0.189	14.778	< .001	0.356	1.096
Adoption_Speed	0.739	0.261	8.024	.005	0.228	1.251
Model Fit & Validity	**Value**					
Model Significance (Chi², df = 3)	29.087, p < .001					
Pearson Goodness-of-Fit (df = 185)	χ^2 = 177.952, p = .632					
Deviance Goodness-of-Fit (df = 185)	χ^2 = 143.074, p = .990					
Test of Parallel Lines (df = 9)	χ^2 = 9.018, p = .436					
Pseudo R^2 (Nagelkerke)	.262					

As shown in Table 13, the model was statistically significant and met all assumptions. The Nagelkerke was .262, offering moderate-to-strong explanatory value and greater explanatory power than the individual models. Adoption speed and leadership communication had significant positive effects, while adaptive culture did not reach significance when other factors were controlled.

These findings suggested that specific capabilities, namely digital responsiveness and transparent communication, were more influential for perceived crisis preparedness than general cultural openness. The results emphasized that resilience stemmed from a combination of technical agility and communicative clarity, rather than infrastructure alone.

This supports the DCF (Teece, 2007, Barreto 2010), illustrating that sensing, seizing, and reconfiguring, in this case through rapid adaptation and leadership behavior, are central to effective crisis response.

H2 + H4b2: Impact of Digital Tools and Leadership Communication on Technological Resilience

A multiple linear regression tested the combined effects of belief in digital tools (Q13_1) and leadership communication (Q4_2) on perceived technological resilience (N = 137).

Table 14: Regression results for H2 and H4b2

Source: Own illustration

Variable	B (Unstandard.)	SE B	β (Standard.)	t	p
Constant	2.389	0.307	–	7.779	< .001
Q13_1 (Belief in Digital Tools)	0.186	0.075	0.207	2.486	.014
Q4_2: Leadership Communication	0.189	0.051	0.306	3.681	< .001
Model fit					
$R^2 = 0.180$					
Adjusted $R^2 = 0.168$					
$F(2, 134) = 14.708$					$p < .001$
Durbin-Watson = 2.053					

As shown in Table 14, the model was statistically significant and explained 18% of the variance, more than either predictor alone (*H2*: 9.7%; *H4b2*: 14.2%). Both variables remained significant and complemented each other, with leadership transparency slightly outweighing belief in digital tools. A one-point increase in perceived leadership transparency was associated with an average increase of 0.189 points in technological resilience, while a one-point increase in belief in digital tools corresponded to an increase of 0.186 points.

These results showed that digital trust and transparent leadership each strengthened and together amplified perceptions of technological resilience. The findings highlighted that resilience depended not only on digital functionality but also on leadership behavior, underscoring the importance of combining technical robustness with communicative governance.

4.2.5 Expanding the View: Additional Patterns in Perceived Resilience

Beyond hypothesis testing, this section explores broader patterns in perceived resilience across sectors, barriers, and open-ended responses, extending the quantitative findings and setting the stage for triangulation with qualitative insights.

Open-ended responses (Figure 15) emphasize communication, leadership, and structure as key resilience enablers, more so than technology.

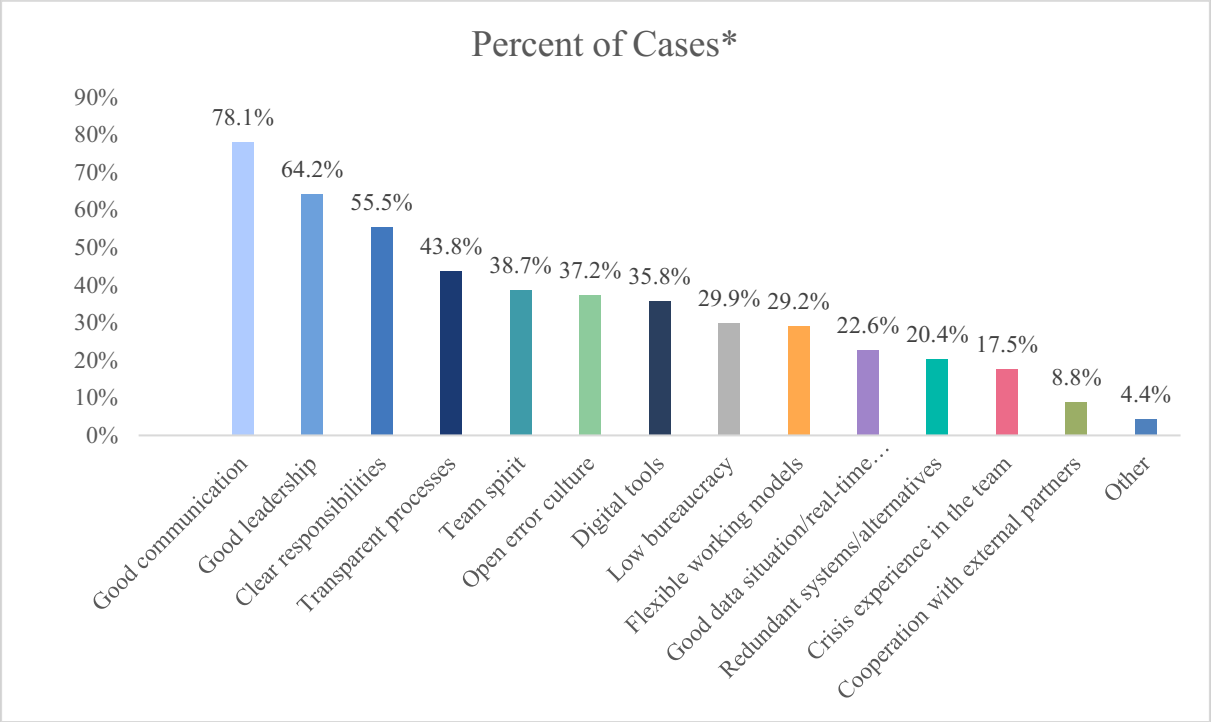

Figure 15: Perceived drivers of crisis preparedness (Q3)

Source: Own illustration

**"Percent of cases" refers to the percentage of all valid participants (N = 137) who selected each option. Multiple responses were possible per participant.*

Grouped thematically (Figure 16), flexibility, transparent communication, and personal responsibility emerged as dominant enablers, reinforcing earlier findings that resilience is behavior and structure-driven, not technology alone.

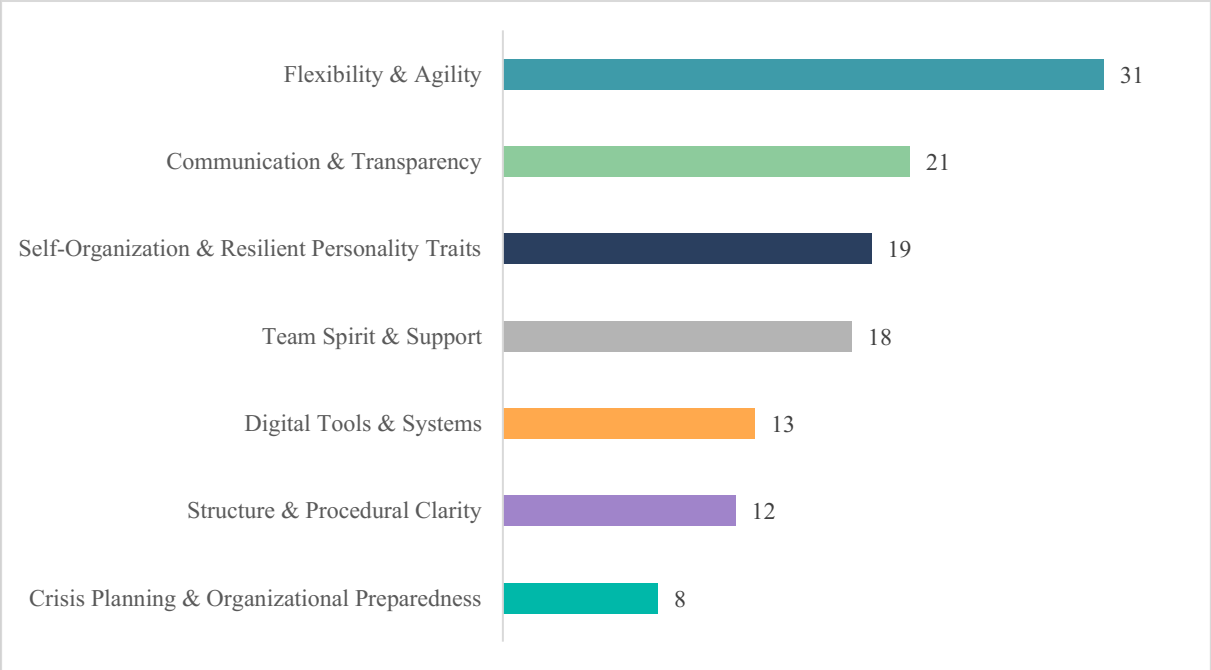

Figure 16: Open-ended themes on organizational resilience (Q7)

Source: Own illustration

Two themes stood out: "*adaptation"* was the most cited term across responses, particularly within "*Flexibility & Agility*", and "*leadership communication"* was frequently criticized for being unclear or low in decision-making, supporting the statistical and qualitative emphasis on communication as a resilience factor.

Figure 17 shows that perceived barriers are primarily organizational, bureaucratic, slow decisions, and unclear responsibilities. Despite being critical, these issues are rarely addressed proactively, suggesting a gap between perceived and implemented resilience strategies. Technological barriers ranked lower, indicating that core challenges lie in governance, not tools.

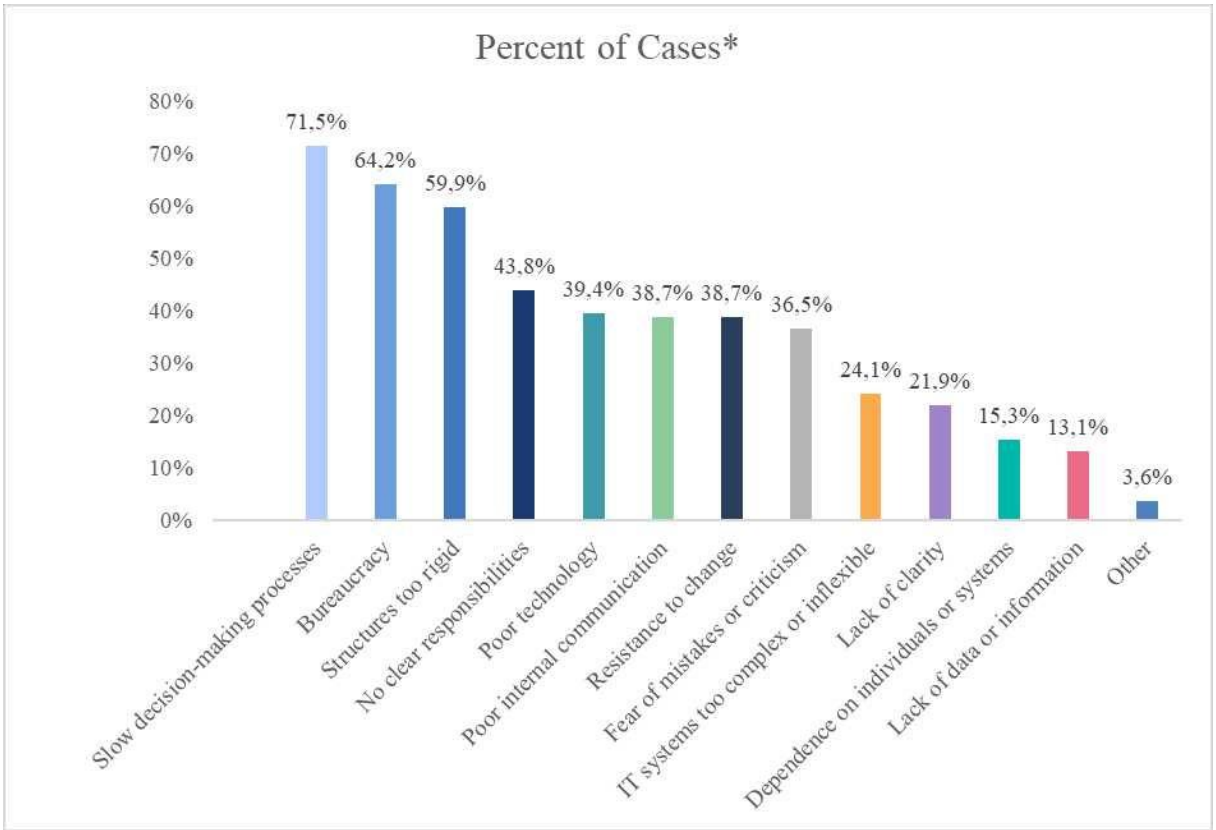

Figure 17: Perceived barriers of crisis preparedness (Q5)

Source: Own illustration

Figure 18 confirms high usage of communication tools like *Microsoft 365*, *Teams*, and messengers, trusted for integration and usability. AI was rarely mentioned but shows potential, aligning with high agreement in Q13_5 that it will support future adaptability (M = 3.88).

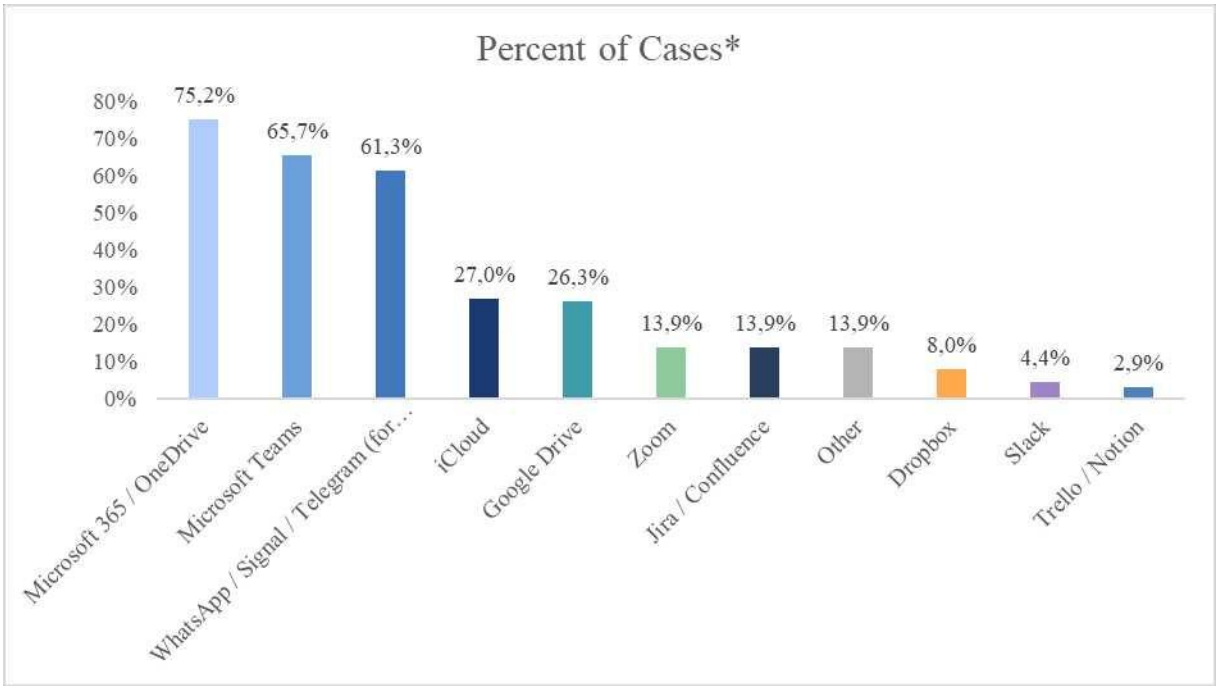

Figure 18: Weekly used tools (Q8)

Source: Own illustration

Figure 19 reveals that "*Flexibility*", "*Efficiency*", and "*Collaboration*" are the most valued aspects of digital tools, especially for remote work and coordination. These findings support *H2* and Q4_2 results, linking digital trust and communication to resilience. When linked with Q8, the pattern becomes even clearer: frequently used tools like *Microsoft 365*, *Teams*, and *WhatsApp* directly correspond to the functions rated as most helpful, supporting the idea that familiar, integrated tools contribute to perceived resilience. Features like scalability and security ranked low, suggesting they are either taken for granted or less visible to end users.

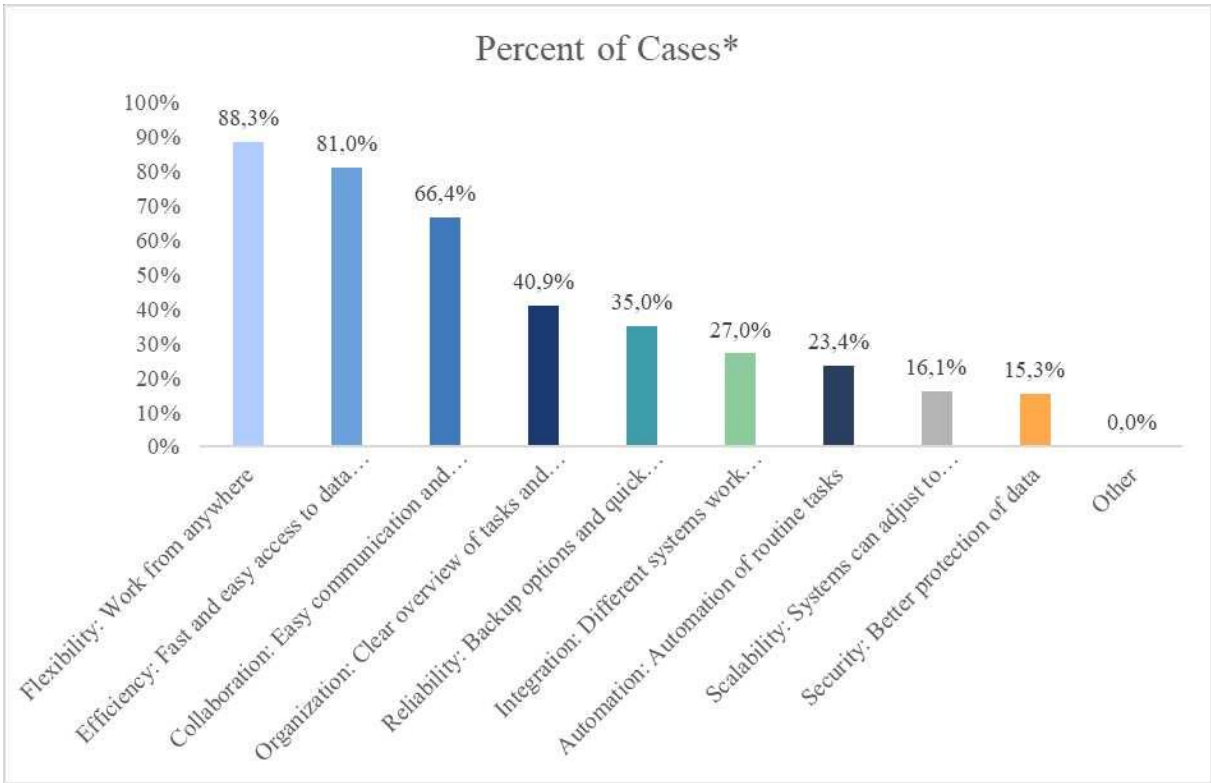

Figure 19: Helpful aspects about tools (Q9)

Source: Own illustration

By contrast, Figure 20 highlights challenges such as internet dependency, tool overload, and instability. These contrast with the helpfulness ratings (Q9), showing that while tools enable flexibility, they also introduce risks, especially around integration and reliability.

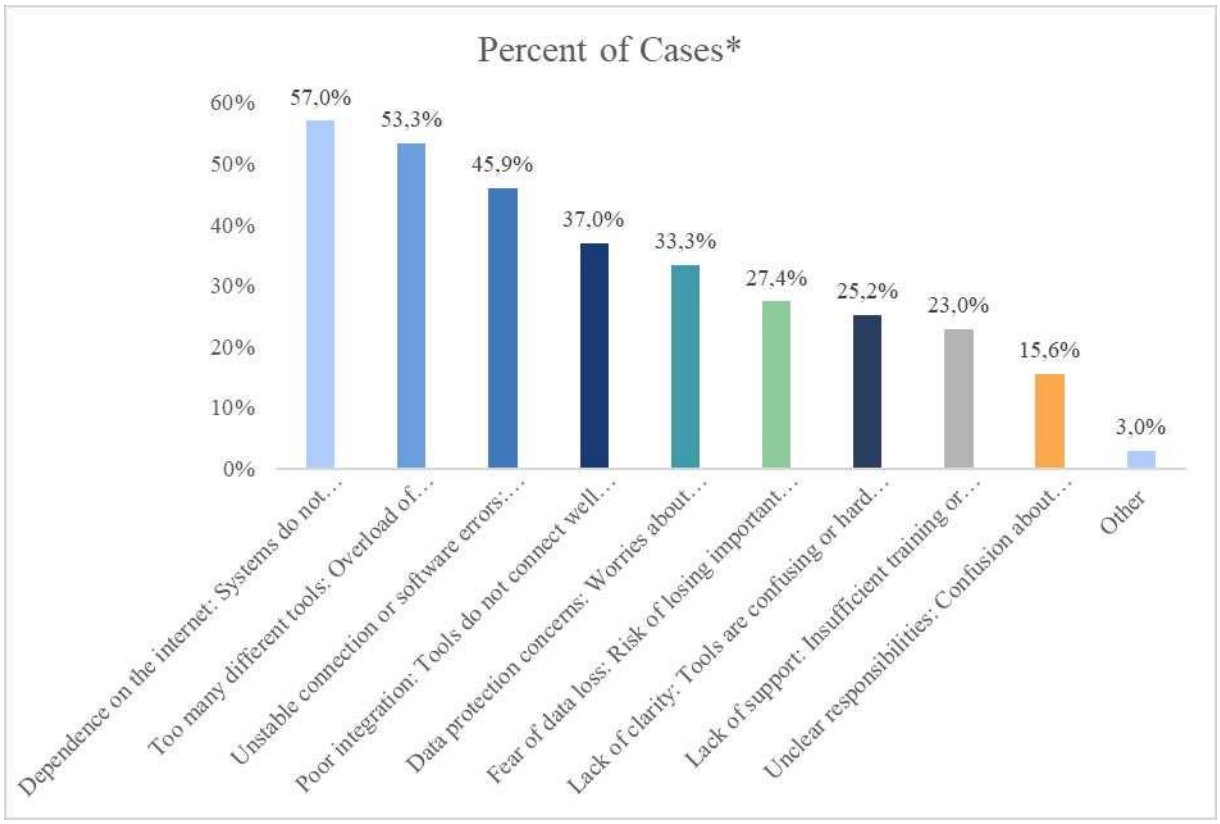

Figure 20: Bothering aspects about tools (Q10)

Source: Own illustration

Sectoral analysis (Figure 21) supports *H1* but adds nuance: Consulting, IT, and E-Commerce show high adaptation and resilience, while Public Sector and Healthcare lag, likely due to regulatory or structural limits.

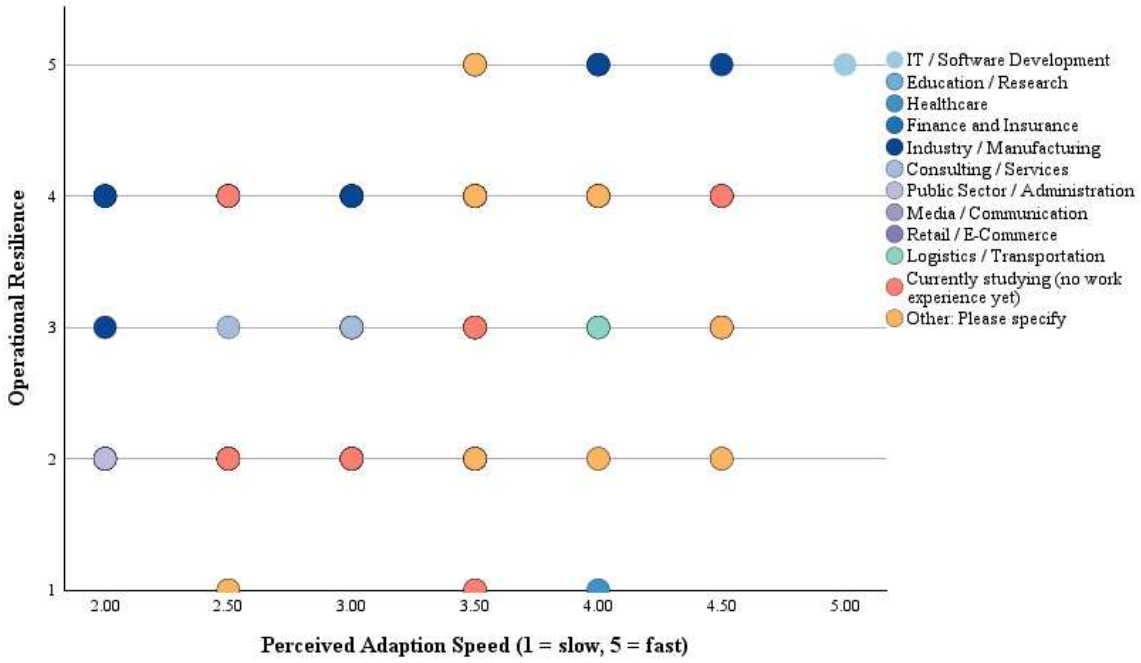

Figure 21: Sectoral patterns of adaptation and resilience

Source: Own illustration

Post-crisis adaptation (Figure 22) also varied; Logistics and Retail improved most, driven by digital upgrades, while Healthcare and Finance showed smaller shifts.

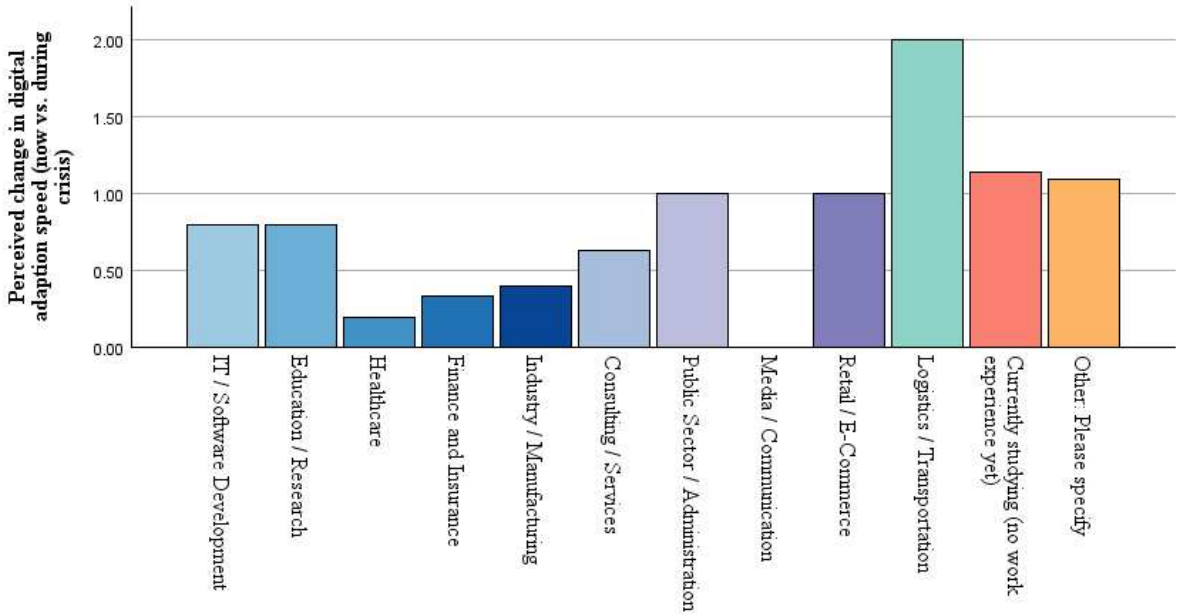

Figure 22: Perceived post-crisis change in digital adaptation speed by sector

Source: Own illustration

Finally, Figure 23 shows that sectors like Finance, IT, and Consulting report higher and more consistent operational resilience, while Healthcare, Retail, and Public Administration show more variation, indicating uneven experiences and structural constraints.

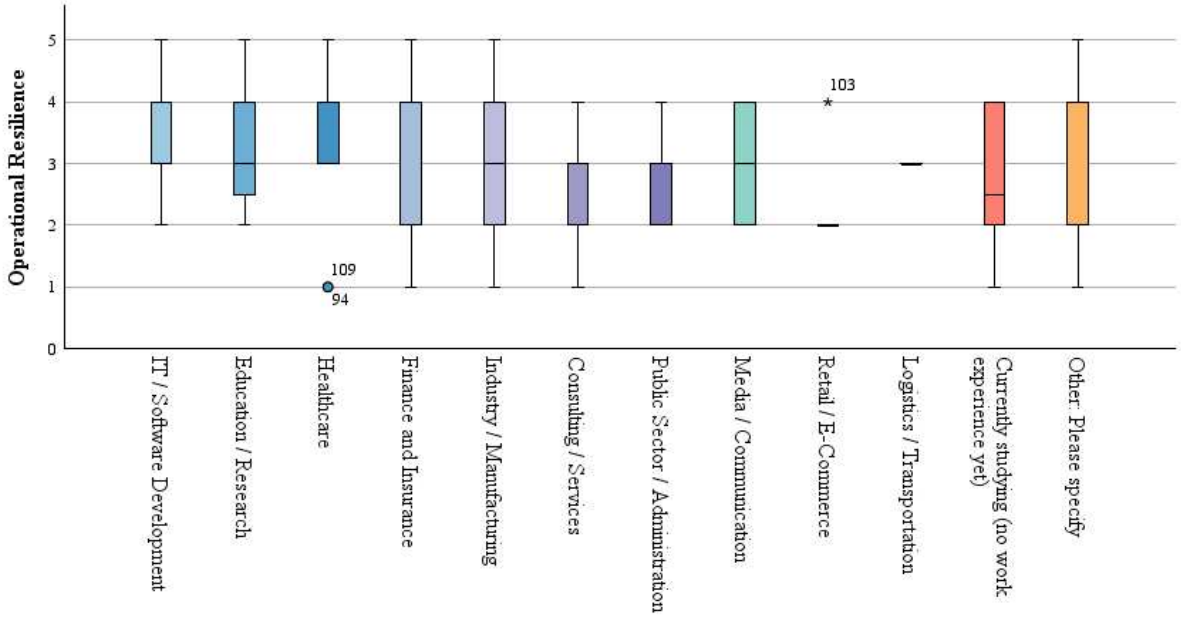

Figure 23: Distribution of perceived operational resilience by industry

Source: Own illustration

5. Conclusion

The conclusion brings together the empirical and theoretical findings to answer the RQ and reflect on broader strategic implications.

5.1 Main Findings – Triangulation

To understand how organizations navigate disruption effectively, this chapter synthesizes insights from literature, expert interviews, and survey data into an integrated resilience perspective. This synthesis underscored the crucial role of culture and leadership in building corporate resilience. Theoretically, these elements represent intangible, firm-specific resources (RBV) and act as key enablers of DCF. Expert interviews, especially Interviewee 5, highlighted the need for distributed ownership, adaptive mindsets, and transparent leadership as core components of crisis preparedness.

Survey responses (Figures 20 and 21) confirmed this relevance, with "*adaptation*," "*responsibility*," and "*leadership*" frequently cited as resilience enablers. However, the quantitative analysis revealed a gap: while transparent leadership communication (Q4_2) was significantly linked to operational and technological resilience, adaptive culture (Q4_1) was not. This indicates a common implementation gap; cultural values are recognized but lack impact without structural support.

Contingency Theory supported this view, suggesting that culture unfolds its full effect only when embedded in a supportive context. Developing a resilient culture, therefore, requires deliberate leadership, clear communication, and integration into organizational routines, insights that directly inform the final framework's cultural and leadership dimension.

This study bridged a gap in resilience research, demonstrating how cloud infrastructure, embedded in cultural and strategic frameworks, enables technical and perceived resilience. It expands classical models by empirically validating digital resilience as a multidimensional construct.

Organizational Barriers & Gaps

A recurring theme across the data was the limiting effect of structural deficiencies on resilience. Figure 22 highlights bureaucracy, unclear responsibilities, and lack of transparency as key

barriers, an observation echoed by Interviewees 4 and 5, who emphasized governance gaps and missing role clarity in practice.

Theoretically, such barriers hinder core dynamic capabilities. Organizations struggle to seize and reconfigure without clear responsibilities and decision structures. Similarly, RBV suggests that even valuable resources like cloud tools remain underutilized if structural conditions prevent their deployment.

This gap is reflected in the survey. While digital tools were rated as helpful (*H2*), structural inertia weakened overall resilience perceptions. The results underline that tools alone are not enough; supportive systems are essential.

To strengthen resilience, organizations must modernize structurally. Clear governance, defined priorities, and integrated processes are prerequisites for leveraging digital solutions effectively in times of crisis.

Technology vs. Structure: Misalignment and Complementarity

The findings highlighted a complex interplay between digital tools and resilience. Regression results (*H2*, *H4b2*) showed that trust in tools and transparent communication boosted technological resilience. Yet, Figures 24 and 25 revealed usability strengths (e.g., flexibility, efficiency) alongside frustrations with fragmented systems, tool overload, and instability.

Expert interviews confirmed that tools alone don't create resilience. Their impact depends on governance, user training, and integration into routines, core elements of DCF, like seizing and reconfiguring.

Contingency Theory reinforces this: tools must fit with workflows, communication patterns, and culture. Misalignment, e.g., redundant tools or poor integration, turns technology from an enabler into a constraint. Digital tools require strategic alignment and process maturity. Without structural fit, even strong technologies fall short in fostering resilient behavior.

Sectoral Differences & Adoption Speed

Sectoral comparisons revealed clear differences in resilience and digital adaptability (Figures 26–28). Retail, e-commerce, IT, and consulting scored higher on both dimensions, while healthcare and public administration lagged. Interviewee 10 linked this to proactive adaptation

in retail (echoing the S-Curve), whereas Interviewee 4 pointed to regulatory constraints and rigidity in the public sector.

These differences supported Contingency Theory: resilience depends on sector-specific conditions. DCF explains why dynamic industries build routines for ongoing reconfiguration, enabling stronger crisis responses. Industry inertia limits the impact of digital tools. However, slower sectors can enhance resilience by learning from fast-moving peers, e.g., through cloud-based pilots, hybrid IT strategies, or targeted tech scouting, without undermining their compliance needs.

5.1.1 Theoretical Implications

This study extended classical resilience theory by empirically confirming the relevance of culture and leadership as distinct, yet underrepresented, enablers of crisis adaptability. While traditional RBV emphasizes tangible and firm-specific assets, the findings demonstrated that intangible capabilities, such as communication, governance, and organizational learning, are equally vital. Cloud infrastructure, often seen as commoditized, gains strategic relevance only when embedded into a broader configuration of DCF.

From a DCF perspective, the study illustrates that sensing, seizing, and reconfiguring depend not merely on access to digital tools but on the structural and cultural routines that activate them. Contingency Theory is also reinforced, showing that resilience cannot follow a one-size-fits-all formula. Its effectiveness depends on structural alignment, sectoral context, and organizational maturity.

Together, these insights culminate in a four-dimensional resilience model that *integrates culture and leadership* alongside *operational*, *technological*, and *strategic-organizational* components, offering theoretical refinement and a pragmatic framework for resilience-building.

5.1.2 Practical Implications

The results of this study offer actionable insights for firms seeking to enhance crisis preparedness through cloud-enabled resilience. The research confirmed that cloud computing contributed to corporate resilience during the COVID-19 pandemic, primarily by supporting process continuity, digital collaboration, and rapid scalability. Widely used tools such as Microsoft Teams and OneDrive enabled organizations to maintain operational and

technological functions under extreme pressure. These findings, supported by *H1* and *H2*, item evaluations, and expert interviews, demonstrate that cloud infrastructure acts as an amplifier of resilience rather than an automatic guarantee.

At the same time, the study underscored a critical insight: cloud technology requires strategic and organizational embedding to unfold its full resilience potential. As shown in the regression models and triangulated with qualitative data, cultural and leadership-related factors play a central role in enabling digital adaptability. Fast-changing industries such as retail and IT, which were early adopters of cloud-based systems, emerged as sectoral frontrunners in perceived resilience (see Figures 26–28). This supported the theoretical proposition that timing (S-Curve logic) and contextual fit significantly influence resilience outcomes.

To translate these findings into practice, the study proposes a resilience model structured along four integrated dimensions, each associated with specific strategic levers. The matrix below summarizes these dimensions and their corresponding implications for firms.

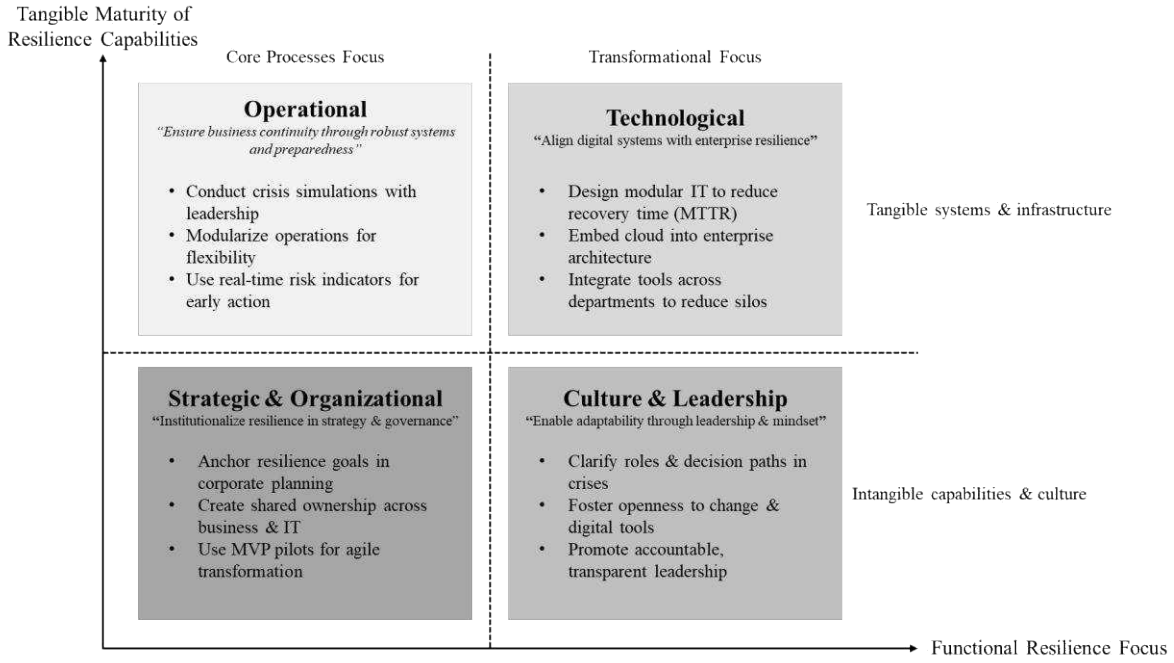

Figure 24: Strategic Resilience Matrix – action areas across four dimensions

Source: Own illustration

This matrix provides a practical roadmap for companies aiming to build organizational resilience in volatile environments and serves as a decision-support tool for strategic resilience planning. It also reflects the core conclusion of this research: technology alone is not enough.

Resilience emerges from the interplay of people, systems, and strategy, with cloud computing acting as a catalyst when embedded into cohesive transformation efforts.

5.2 Limitations

This thesis was conducted over a limited timeframe of approximately four months, restricting the ability to observe long-term resilience outcomes or changes over time. Data obtained from a self-reported survey. The exclusive focus on cloud computing may have underrepresented the role of other enabling technologies (e.g., AI, IoT, or Blockchain) in crisis contexts. Additionally, the COVID-19 pandemic served as a specific case for crisis-driven resilience, limiting the generalizability of the findings to other types of disruption, such as geopolitical or environmental crises.

5.2.1 Expert Interviews

The qualitative component included twelve semi-structured interviews, with most participants representing large corporations in cloud-intensive industries. This may have led to a bias toward specific governance structures and digital maturity levels (Houghton *et al.*, 2013). The reliance on voluntary expert availability limited the diversity of perspectives, particularly from SMEs or public institutions. The inductive interview guide and the Gioia methodology added transparency, but may still reflect selective researcher interpretation (Makwana *et al.*, 2023). The geographical scope was mainly European, which limits global generalizability.

5.2.2 Survey

The online survey employed a non-random sample, with a concentration of young, highly educated respondents. Self-reported survey data may involve biases or inaccuracies due to subjective interpretation and response behavior (Bryman, 2016). This limits demographic and professional diversity and may affect generalizability. Sectoral representation was uneven, with strong participation from students and tech-related fields. Resilience was assessed from a user perspective rather than a management viewpoint, which may affect perceived relevance. Some constructs relied on single- or two-item scales, which are acceptable in exploratory research but limit statistical robustness (Fisher, Matthews and Gibbons, 2015). Furthermore, the study design did not allow for causal inferences or validation through confirmatory factor analysis. The number of responses declined toward the end of the survey, suggesting potential fatigue effects. For example, open-ended questions early in the survey (e.g., Q3, Q5) received

significantly more answers than later ones (e.g., Q8–Q10). Moreover, the highest agreement levels were found in questions about positive drivers of resilience, while negative aspects showed more distributed and less dominant responses. This suggests that criticism of digital tools is more fragmented and less salient, although still relevant for interpretation.

Overall, while the mixed-method approach offers valuable triangulated insights, these limitations underscore the importance of cautious interpretation and contextual sensitivity.

5.3 Future Research

This study highlighted how cloud computing strengthens corporate resilience across four dimensions. Future research could build on these findings in several ways.

First, emerging technologies like AI-as-a-Service or edge computing may enable new forms of resilience. Their impact on adaptability and crisis response should be further explored, especially in dynamic environments.

Second, sectoral differences have suggested that resilience is context-dependent. Comparative and longitudinal studies could examine how organizational conditions, regulation, or maturity shape resilience trajectories across industries.

Third, future research should include managerial perspectives. Case studies or expert interviews could offer deeper insight into governance, alignment, and the strategic framing of digital tools.

Fourth, the proposed four-dimensional resilience framework warrants empirical validation across technologies and contexts. In particular, the distinct role of culture and leadership warrants further investigation.

Lastly, future studies should increase methodological diversity, e.g., broader sampling, longitudinal designs, and standardized resilience metrics, to enhance robustness and generalizability.

Reference list

Adiguzel, S. (2019) ‘Logistics management in disaster’, *Journal of Management, Marketing and Logistics (JMML)*, 6(4), pp. 212–224. doi: 10.17261/Pressacademia.2019.1173

Adner, R. and Kapoor, R. (2010) ‘Value creation in innovation ecosystems: how the structure of technological interdependence affects firm performance in new technology generations’, *Strategic Management Journal*.

Allen, F. and Carletti, E. (2010) ‘An Overview of the Crisis: Causes, Consequences, and Solutions’, *International Review of Finance*. Available at: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1468-2443.2009.01103.x.

Amazon Web Services (n.d.a) *Cloud-Computing with AWS: The leading Cloud*. Available at: https://aws.amazon.com/de/what-is-aws/ (Accessed: 9 May 2024).

Amazon Web Services (n.d.b) *Was ist Software as a Service (SaaS)?* Available at: https://aws.amazon.com/what-is/saas/ (Accessed: 4 April 2025).

Amazon Web Services (2016) *Netflix Case Study*. Available at: https://aws.amazon.com/de/solutions/case-studies/netflix-case-study/ (Accessed: 5 April 2025).

Amazon Web Services (2024) *Sunstone Hotel Investors Facilitates Business Continuity with AWS Elastic Disaster Recovery: Implementing AWS Elastic Disaster Recovery for Business Continuity*. Available at: https://aws.amazon.com/de/partners/success/sunstone-rednight/ (Accessed: 5 April 2025).

Armbrust, M. *et al.* (2010) ‘A view of cloud computing’, *Communications of the ACM*, 53(4), pp. 50–58. doi: 10.1145/1721654.1721672

Bansal, A. (2016) ‘Employee trust dynamics during organizational change: A context of mergers and acquisitions’, *Asia-Pacific Journal of Business Administration*, 8, pp. 55–69. doi: 10.1108/APJBA-08-2015-0075

Bansal, P., Smith, W. and Vaara, E. (2018) 'New Ways of Seeing through Qualitative Research', *Academy of Management Journal*, 61, pp. 1189–1195. doi: 10.5465/amj.2018.4004

Barlett, J.E., Kotrlik, J. and Higgins, C. (2001) 'Organizational Research: Determining Appropriate Sample Size in Survey Research', *Information Technology, Learning, and Performance Journal*, 19.

Barney, J., Wright, M. and Ketchen, D.J. (2001) 'The resource-based view of the firm: Ten years after 1991', *Journal of Management*, pp. 625–641.

Barreto, I. (2010) 'Dynamic Capabilities: A Review of Past Research and an Agenda for the Future', *Journal of Management*, 36(1), pp. 256–280. doi: 10.1177/0149206309350776

Barriball, K.L. and While, A. (2013) 'Collecting data using a semi-structured interview: A discussion paper.', *Journal of Advanced Nursing*, 19. doi: 10.1111/j.1365-2648.1994.tb01088.x

Beimborn, D., Miletzki, T. and Wenzel, S. (2011) 'Platform as a Service (PaaS)', *WIRTSCHAFTSINFORMATIK*, 53(6), pp. 371–375. doi: 10.1007/s11576-011-0294-y

Bellini, H. *et al.* (2018) 'The Cutting "Edge" of Computing: How edge computing will augment the cloud & unlock real-time, big data applications', *Equity Research Goldman Sachs*.

Bhardwaj, S., Jain, L. and Jain, S. (2010) 'CLOUD COMPUTING: A STUDY OF INFRASTRUCTURE AS A SERVICE (IAAS)', *I nternational Journal of Engineering and Information Technology* (2), pp. 60–63.

Blackburn, S. *et al.* (n.d.) *Digital Strategy during the corona virus*. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-strategy-in-a-time-of-crisis#/ (Accessed: 4 April 2025).

Blackrock (2024) *Financial resilience in a new economic regime*. Available at: https://www.blackrock.com/corporate/about-us/investment-stewardship/insights/financial-resilience-in-new-economic-regime (Accessed: 4 April 2025).

Brandenburg, M. (2016) ‘Supply chain efficiency, value creation and the economic crisis – An empirical assessment of the European automotive industry 2002–2010’, *International Journal of Production Economics*, 171, pp. 321–335. doi: 10.1016/j.ijpe.2015.07.039

Bryman, A. (2016) ‘Social Research Methods’, *Oxford University Press*.

Carifio, J. and Perla, R. (2009) ‘Resolving the 50-year Debate Around using and Misusing Likert Scales’, *Medical education*, 42, pp. 1150–1152. doi: 10.1111/j.1365-2923.2008.03172.x

Chartered Institute of Public Finance and Accountancy (CIPFA) (n.d.) *Financial Resilience Index: What is the Financial Resilience Index?* Available at: https://www.cipfa.org/services/financial-resilience-index (Accessed: 4 April 2025).

Cheema-Fox, A. *et al.* (2021) ‘Corporate Resilience and Response to COVID-19’, *Journal of Applied Corporate Finance*, 33(2), pp. 24–40. doi: 10.1111/jacf.12457

Christensen, C.M. (1992) ‘Exploring the Limits of the Technology S-Curve. Part I: Component Technologies’, *Production and Operations Management*.

Christensen, C.M. and Bower, J.L. (1996) ‘Customer Power, Strategic Investment, and the Failure of Leading Firms’, *Strategic Management Journal*.

Christensen, C.M., Suarez, F.F. and Utterback, J.M. (1998) ‘Strategies for Survival in Fast-Changing Industries’, *Management Science*.

Cohen, J. (1988) ‘Statistical Power Analysis for the Behavioral Sciences’.

Creswell, J. *et al.* (2003) ‘Advance Mixed methods Research Designs’, in *Handbook of mixed methods in social and behavioral research*, pp. 209–240.

Deloitte (n.d.) *Resilience by design: Financial services operating models and operational resilience*. Available at: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-resilience-by-design-en.pdf (Accessed: 4 April 2025).

Derbyshire, J. (2017) ‘Potential surprise theory as a theoretical foundation for scenario planning’, *Technological Forecasting and Social Change*, 124, pp. 77–87. doi: 10.1016/j.techfore.2016.05.008

Duchek, S. (2020) ‘Organizational resilience: a capability-based conceptualization’, *Business Research*, 13(1), pp. 215–246. doi: 10.1007/s40685-019-0085-7

Eisenhardt, K.M. (1989) ‘Making Fast Strategic Decisions in High-Velocity Environments’, *The Academy of Management Journal*.

Eisenhardt, K.M. and Martin, Jeffrey, A. (2000) ‘Dynamic Capabilities: What Are They?’ *Strategic Management Journal*.

Eisinga, R., Grotenhuis, M. and Pelzer, B. (2013) ‘The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown?’ *International journal of public health*, 58, pp. 637–642. doi: 10.1007/s00038-012-0416-3

finreg-e (2022) *Building resilience into compliance management programs with regulatory frameworks*. Available at: https://www.finreg-e.com/building-resilience-into-compliance-management-programs-with-regulatory-frameworks/ (Accessed: 4 April 2025).

Fisher, G., Matthews, R. and Gibbons, A. (2015) ‘Developing and Investigating the Use of Single-Item Measures in Organizational Research’, *Journal of occupational health psychology*, 21. doi: 10.1037/a0039139

Fowler, F. (2018) *Survey Research Methods (5th edition)*.

Garcia-Zambrano, L., Rodriguez-Castellamos, A. and Garcia-Merino, J.D. (n.d.) ‘Does Proactive Management of Core Competencies Improve Performance?’ *Proceedings of the European Conference on Intellectual Capital*.

Garcie-Valenzuela, V.M., Jacob-Hernandez, C.A. and Flores-Lopez, J.G. (2023) ‘Dynamic Capabilities and Their Effect on Organizational Resilience in Small and Medium-Sized Commercial Enterprises’, *Management & Marketing*, pp. 496–514.

Gioia, D., Corley, K. and Hamilton, A. (2013) 'Seeking Qualitative Rigor in Inductive Research', *Organizational Research Methods*, 16, pp. 15–31. doi: 10.1177/1094428112452151

Google Cloud (n.d.) *Current: Preparing teenagers for financial responsibility*. Available at: https://cloud.google.com/customers/current (Accessed: 5 April 2025).

Gopalakrishnan, S. and Damanpour, F. (1997) 'A Review of Innovation Research in Economics, Sociology and Technology Management', *Omega, International Journal of Management Science*.

Groenendaal, J. and Helsloot, I. (2021) 'Cyber resilience during the COVID-19 pandemic crisis: A case study', *Journal of Contingencies and Crisis Management*, 29. doi: 10.1111/1468-5973.12360

Grossoehme, D. (2014) 'Overview of Qualitative Research', *Journal of health care chaplaincy*, 20, pp. 109–122. doi: 10.1080/08854726.2014.925660

Guest, G., Bunce, A. and Johnson, L. (2006) 'How Many Interviews Are Enough?' *Field Methods - FIELD METHOD*, 18, pp. 59–82. doi: 10.1177/1525822X05279903

Hair, J., Page, M. and Brunsveld, N. (2019) *Essentials of Business Research Methods*.

Hamel, G. and Välikangas, L. (2003) 'The Quest for Resilience', *Harvard business review*, 81, 52-63, 131.

Helfat, C.E. *et al.* (2023) 'Renewing the resource-based view: New contexts, new concepts, and new methods', *Strategic Management Journal*.

Henderson, J.C. and Venkatraman, N. (1993) 'Strategic alignment: Leveraging information technology for transforming organizations', *IBM Systems Journal*.

Houghton, C. *et al.* (2013) 'Rigour in qualitative case-study research', *Nurse researcher*, 20, pp. 12–17. doi: 10.7748/nr2013.03.20.4.12.e326

Ibrahim, O. (2024) ‘Impact of Cloud Computing on Business Continuity and Disaster Recovery’, *Journal of Technology and Systems*, 6, pp. 16–28. doi: 10.47941/jts.2146

International Organization for Standardization (ISO) and International Electrotechnical Commission (ICE) (2023) *ISO/IEC 22123-1:2023(en): Information technology — Cloud computing — Part 1: Vocabulary*. Available at: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:22123:-1:ed-2:v1:en (Accessed: 5 April 2025).

Joshi, A. *et al.* (2015) ‘Likert Scale: Explored and Explained’, *British Journal of Applied Science & Technology*, 7, pp. 396–403. doi: 10.9734/BJAST/2015/14975

Khangha, S. *et al.* (2013) ‘Management Innovation and Adoption of Emerging Technologies: The Case of Cloud Computing’, *European Management Review*.

Kindermann, B. *et al.* (2021) ‘Digital orientation: Conceptualization and operationalization of a new strategic orientation’, *European Management Journal*, 39(5), pp. 645–657. doi: 10.1016/j.emj.2020.10.009

Klöckner, M., Schmidt, C.G. and Wagner, S.M. (2023) ‘The COVID-19 pandemic and shareholder value: impact and mitigation’, *International Journal of Product Research*.

Krejcie, R.V. and Morgan, D.W. (1970) ‘Determining Sample Size for Research Activities’, *Educational and Psychological Measurement*, 30(3), pp. 607–610. doi: 10.1177/001316447003000308

Kushida, K.E., Murray, J. and Zysman, J. (2011) ‘Diffusing the Cloud: Cloud Computing and Implications for Public Policy’, *Journal of Industry, Competition and Trade*, 11(3), pp. 209–237. doi: 10.1007/s10842-011-0106-5

Lee, S.M. and Trimi, S. (2021) ‘Convergence innovation in the digital age and in the COVID-19 pandemic crisis’, *Journal of Business Research*, 123, pp. 14–22. doi: 10.1016/j.jbusres.2020.09.041

Leiting, A.-K., Cuyper, L. de and Kauffmann, C. (2022) ‘The Internet of Things and the case of Bosch: Changing business models while staying true to yourself’, *Technovation*, 118, pp. 102–497. doi: 10.1016/j.technovation.2022.102497

Lengnick-Hall, C.A., Beck, T.E. and Lengnick-Hall, M.L. (2011) 'Developing a capacity for organizational resilience through strategic human resource management', *Human Resource Management Review*, 21(3), pp. 243–255. doi: 10.1016/j.hrmr.2010.07.001

Lindgren, P. (2017) 'Advanced Business Model Innovation', *Wireless Personal Communications*.

Liu, Y. *et al.* (2024) 'Effects of digital orientation on organizational resilience: a dynamic capabilities perspective', *Journal of Manufacturing Technology Management*, 35(2), pp. 268–290. doi: 10.1108/JMTM-06-2023-0224

Magaldi, D. and Berler, M. (2020) 'Semi-structured Interviews', in Zeigler-Hill, V. and Shackelford, T.K. (eds.) *Encyclopedia of Personality and Individual Differences.* Cham: Springer International Publishing, pp. 4825–4830.

Makwana, D. *et al.* (2023) 'Sampling Methods in Research: A Review', 7, pp. 762–768.

Marston, S. *et al.* (2010) 'Cloud Computing – The Business Perspective', *Decision Support Systems*. Available at: https://www.sciencedirect.com/science/article/pii/S0167923610002393.

McKinsey & Company (2020) 'How COVID-19 has pushed companies over the technology tipping point—and transformed business forever'.

Mell, P. and Grance, T. (2011) 'The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology', *National Institute of Standards and Technology*.

Miceli, A. *et al.* (2021) 'Thriving, Not Just Surviving in Changing Times: How Sustainability, Agility and Digitalization Intertwine with Organizational Resilience', *Sustainability*.

Microsoft Azure (n.d.) *What is Azure: What is Mircosoft Azure*. Available at: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/ (Accessed: 9 May 2024).

Mitra, A., O'Regan, N. and Sarpong, D. (2018) 'Cloud resource adaptation_A resource based perspective on value creation for corporate growth', *Technological Forecasting & Social Change*. Available at: https://doi.org/10.1016/j.techfore.2017.08.012.

Mitroff, I.I. (1988) 'CRISIS MANAGEMENT: CUTTING THROUGH THE CONFUSION', *Sloan Management Review*, 29(2), p. 15. Available at: https://www.proquest.com/scholarly-journals/crisis-management-cutting-through-confusion/docview/224966854/se-2?accountid=28899.

Norman, G. (2010) 'LIkert scales, levels of measurement adn the "laws" of statistics', *Advances in health sciences education : theory and practice*, 15, pp. 625–632. doi: 10.1007/s10459-010-9222-y

Oesterle, S. *et al.* (2020) 'A contingency lens on cloud provider management processes', *Business Research*, 13(3), pp. 1451–1489. doi: 10.1007/s40685-020-00128-8

O'Reilly, C.A. and Tushman, M.L. (2007) 'Ambidexterity as a Dynamic Capability: Resolving the Innovator's Dilemma', *Research Paper Series*.

Organisation for Economic Co-operation and Development (OECD) (2024) *Education at a Glance 2024*. Available at: https://www.oecd.org/en/publications/education-at-a-glance-2024_c00cad36-en.htmlhttps://www.oecd.org/en/topics/sub-issues/education-attainment.html? (Accessed: 9 May 2025).

Papadopoulos, T., Baltas, K.N. and Balta, M.E. (2020) 'The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice', *International Journal of Information Management*, 55 (4pp). doi: 10.1016/j.ijinfomgt.2020.102192

Papagiannidis, S., Harris, J. and Morton, D. (2020) 'WHO led the digital transformation of your company? A reflection of IT related challenges during the pandemic', *International Journal of Information Management*, 55 (5pp). doi: 10.1016/j.ijinfomgt.2020.102166

Porter, M.E. (1985) 'The Competitive Advantage: Creating and Sustaining Superior Performance', *Harvard business review*, pp. 82–84. doi: 10.1590/S0034-75901985000200009

Qu, S. and Dumay, J. (2011) 'The qualitative research interview', *Qualitative Research in Accounting & Management*, 8, pp. 238–264. doi: 10.1108/11766091111162070

Rajagopal (2015) 'Chaos in Markets', in Rajagopal (ed.) *The Butterfly Effect in Competitive Markets: Driving Small Changes for Large Differences.* London: Palgrave Macmillan UK, pp. 3–29.

Rowley, J. (2012) 'Conducting research interviews', *Management Research Review*, 35, pp. 260–271. doi: 10.1108/01409171211210154

Salesforce (n.d.a) *OpenTable boosts customer service with Agentforce: How Salesforce Helps OpenTable*. Available at: https://www.salesforce.com/customer-stories/opentable/ (Accessed: 5 April 2025).

Salesforce (n.d.b) *Salesforce develops the technology, the partnerships, and the communities that help companies connect with customers*. Available at: https://www.salesforce.com/de/company/our-story/ (Accessed: 9 May 2024).

Seetharaman, P. (2020) 'Business models shifts: Impact of Covid-19', *International Journal of Information Management*, 54 (4pp). doi: 10.1016/j.ijinfomgt.2020.102173

Seibold, L.K.C. (2020) 'Methodology', in Seibold, L.K. (ed.) *Family Businesses' Growth: Unpacking the Black Box.* Wiesbaden: Springer Fachmedien Wiesbaden, pp. 167–212.

Sekaran, U. and Bougie, R. (2009) 'Research Methods for Business: A Skill Building Approach (5th Edition)', *International Journal of Information Technology and Management - IJITM*.

Shah, H.M. *et al.* (2023) 'The contemporary state of big data analytics and artificial intelligence towards intelligent supply chain risk management: a comprehensive review', *Kybernetes*.

Sheffi, Y. (2013) *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*.

Spender, J.-C. (2014) *Business strategy: Managing uncertainty, opportunity, and enterprise*. Oxford: Oxford University Press.

Taleb, N. (2010) 'The Black Swan The Impact of the Highly Improbable', *London: Penguin*, 36.

Tang, C., Dong, S. and Zhou, R. (2025) 'The impact of digitalization on corporate resilience', *International Review of Economics & Finance*, 97 (14pp). doi: 10.1016/j.iref.2024.103834

Targett, E. (2024) *Did a digital obsession 'Just Do It' in for Nike's John Donahoe?* Available at: https://www.thestack.technology/did-a-digital-obsession-just-do-it-in-for-nikes-john-donahoe/ (Accessed: 5 April 2025).

Tashiro, K. and Kitago, Y. (2024) 'Development of a Model for Comprehensive Evaluation of Corporate Resilience Against Disasters (1)—An Examination Based on Indicators Developed by "Resilient Organisations"', *Journal of Disaster Research*.

Teece, D.J. (2007) 'Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance', *Strategic Management Journal*.

Teece, D.J. (2010) 'Business Models, Business Strategy and Innovation', *Long Range Planning*.

Teece, D.J., Pisano, G. and Shuen, A. (1997) 'Dynamic Capabilities and strategic Management_Teece, Pisano and Shuen (1997)', *Strategic Management Journal*, pp. 509–533.

Turner, D. (2010) 'Qualitative Interview Design: A Practical Guide for Novice Investigators', *Qualitative Report*, 15. doi: 10.46743/2160-3715/2010.1178

Vailshery, L.S. (2024) *Public cloud services end-user spending worldwide from 2017 to 2025 (in billion U.S. dollars)*. Available at: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/ (Accessed: 9 May 2025).

Wagner, D. (n.d.) *Embracing regulatory resilience*. Available at: https://www.everbridge.com/blog/embracing-regulatory-resilience/ (Accessed: 4 April 2025).

Wandemberg Boschetti, J.C. (2019) *Processes Need To Be Managed, People Need To Be Led!* Available at: https://jcwandemberg.medium.com/a-tropophilic-workforce-59bbd2707327 (Accessed: 4 April 2025).

Wassen, M., Adel, E. and Laoucine, K. (2022) 'The Global Semiconductor Chip Shortage: Causes, Implications, and Potential Remedies', *IFAC PapersOnLine*.

Weick, K. and Sutcliffe, K. (2007) 'Managing the Unexpected Resilient Performance in an Age of Uncertainty', 8. Available at: https://www.researchgate.net/publication/265106124_Managing_the_Unexpected_Resilient_Performance_in_an_Age_of_Uncertainty?enrichId=rgreq-51c6a75ed0992a2906eb06d575462a8e-XXX&enrichSource=Y292ZXJQYWdlOzI2NTEwNjEyNDtBUzoyNjk1NzMwMzExOTg3MjRAMTQ0MTI4MjYyNzY3Nw%3D%3D&el=1_x_3&_esc=publicationCoverPdf.

Yang, L. *et al.* (2021) 'Europe's digital economy at a tipping point', *Equity Research Goldman Sachs*.

Zollo, M. and Winter, S.G. (2002) 'Deliberate Learning and the Evolution of Dynamic Capabilities', *Organization Science*.

Appendix A: Outline of survey questions

Table 15: Survey questions outline

Source: Own illustration

Q No.	Question	Question Type	Answer Options
General Familiarity and Perception of Resilience, Cultural & Leadership aspects, and individual experience			
Q1	Have you ever experienced how an organization dealt with a crisis or disruption?	Single Choice	Yes; No
Q2_1	In your experience, how much do you agree with the following statement? Companies I have worked for are well-prepared for crises or disruptions.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Q3	In your opinion, what are the most important factors to help companies be well prepared for crises? Please select up to 5 aspects you consider particularly important.	Multiple choice	Good communication; Digital tools; Transparent processes; Team spirit; Good leadership; Clear responsibilities; Crisis experience in the team; Flexible working models; Open error culture; Low bureaucracy; Redundant systems/alternatives; Good data situation/real-time information; Cooperation with external partners; Other
Q4_1	In your experience, how much do you agree with the following statement? An open, adaptive corporate culture helps companies to quickly adapt processes, decisions, and priorities in times of crisis. Means flexibility	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Q4_2	In your experience, how much do you agree with the following statement? Decisions and important information are communicated transparently in my company.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)

Q5	In your opinion, what factors make it difficult for organizations to respond effectively to challenges? Please select up to 5 aspects you consider particularly obstructive.	Multiple choice	Bureaucracy; Poor technology; Lack of clarity; Structures too rigid; Slow decision-making processes; No clear responsibilities; Fear of mistakes or criticism; Dependence on individuals or systems; Poor internal communication; Resistance to change; Lack of data or information; IT systems too complex or inflexible; Other
Q6_1	In your experience, how much do you agree with the following statement? My organization has learned from the COVID-19 crisis and is now better prepared for future crises or disruptions.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Q6_2	In your experience, how much do you agree with the following statement? Companies are more resilient in crises if they are less dependent on individual systems, people, or external service providers.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Q7	When you think of a difficult work- or study-related situation (e.g., pandemics, supply chain problems, economic crises, or major operational disruptions like production delays, logistics bottlenecks, staff shortages), what actions or characteristics in yourself or your environment helped you personally to remain capable of taking action?	Open Field	Free text
General Familiarity with Digitalization and Digital Tools			

Q8	Which digital tools or platforms do you use regularly (at least once a week)?	Multiple Choice	Google Drive; Microsoft 365 / OneDrive; Microsoft Teams; Zoom; Dropbox; iCloud; Slack; Trello / Notion; WhatsApp / Signal / Telegram (for communication in work or study contexts only); Jira / Confluence; Other
Q9	What do you find helpful about digital tools? Please select up to 5 aspects that you find particularly helpful.	Multiple Choice	Efficiency: Fast and easy access to data and tools; Flexibility: Work from anywhere; Collaboration: Easy communication and teamwork; Organization: Clear overview of tasks and projects; Scalability: Systems can adjust to changing needs; Reliability: Backup options and quick recovery; Automation: Automation of routine tasks; Integration: Different systems work together easily; Security: Better protection of data; Other
Q10	What bothers you about digital tools? Please select up to 5 aspects that you find particularly bothering.	Multiple Choice	Lack of clarity: Tools are confusing or hard to navigate; Data protection concerns: Worries about data privacy and security; Unstable connection or software errors: Frequent technical issues; Too many different tools: Overload of different systems and platforms; Dependence on the internet: Systems do not work offline; Unclear responsibilities: Confusion about who uses which tool or how; Lack of support: Insufficient training or assistance when using tools; Poor integration: Tools do not connect well with each other; Fear of data loss: Risk of losing important information; Other
Q11	Based on your experience, how quickly were digital systems adapted or expanded during times of crisis?	Single Choice	Within 1 day; Within 1 week; Within 1 month; Longer than 1 month; No adjustment made; I cannot judge
Q12	Based on your experience, how quickly can digital systems be adapted or expanded today during times of crisis?	Single Choice	Within 1 day; Within 1 week; Within 1 month; Longer than 1 month; No adjustment made; I cannot judge

Perceptions of Digital Tools and Technology Trust			
Q13_1	In your experience, how much do you agree with the following statement. I believe that digital tools (e.g., cloud services, shared files, online access, etc.) can help companies continue operating even during disruptions or crises.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Q13_2	In your experience, how much do you agree with the following statement? The digital tools I use regularly are clear, intuitive, and easy to use.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Q13_3	In your experience, how much do you agree with the following statement. I have the impression that data security in digital tools (e.g., cloud services, online platforms like Microsoft 365, Google Drive, etc.) has improved in recent years.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Q13_4	In your experience, how much do you agree with the following statement. I would have more trust in a company that uses modern digital technologies – e.g., as an employer, service provider, or business partner.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Belief in AI as a Driver of Adaptability			
Q13_5	In your experience, how much do you agree with the following statement. Artificial intelligence will help organizations become more adaptable in the future.	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)

O

Familiarity with digital Tools and technical understanding			
Q13_6	In your experience, how much do you agree with the following statement. I have a good technical understanding when using digital devices and applications (e.g., computers, internet services, software, apps).	5-point Likert scale	Strongly disagree (1) - Strongly agree (5)
Demographic and Background Questions			
Q14	How old are you?	Single Choice	Under 18; 18–24; 25–34; 35–44; 45–54; 55 or older
Q15	What gender do you identify with?	Single Choice	Female; Male; Non-binary; Prefer not to say
Q16	What is your highest level of education completed?	Single Choice	No degree; Secondary school diploma (e.g., high school diploma, A-levels, Baccalaureate); Vocational training / Apprenticeship; Bachelor's; Master's; Doctorate (e.g. PhD, DBA)
Q17	Which of the following best describes the area where you currently live most of the time?	Single Choice	A large city (more than 100,000 inhabitants); A medium-sized city (20,000–100,000 inhabitants); A small town or large village (5,000–20,000 inhabitants); A rural area (less than 5,000 inhabitants); Not sure / Prefer not to say
Q18	Which field or industry best describes your current professional background, previous experience, or intended career path?	Dropdown / Open field	IT / Software Development; Education / Research; Healthcare; Finance and Insurance; Industry / Manufacturing; Consulting / Services; Public Sector / Administration; Media / Communication; Retail / E-Commerce; Logistics / Transportation; Currently studying (no work experience yet); Other

Appendix B: Expert Interviews

To capture the diversity of backgrounds of the interviewees, interviews were done semi-structured, specific to each expert's area and experience. The central themes were universal across all conversations, but the specific questions were customized according to the area of expertise of the participant and the direction of the discussion. For analytical simplicity, experts were divided into three wide categories.

B.1: Technology & Cloud Transformation Experts

Experts with deep technical expertise, typically responsible for cloud architecture, platform scalability, DevOps practices, and infrastructure automation (Interviewees 3, 8, 9, 10, 12).

1. What does resilience mean from a technical or architectural standpoint in your work?
2. How do modular architectures or microservices help organizations respond to disruptions?
3. In your experience, how important is automation in enabling resilience and recovery?
4. How do you balance scalability with reliability in cloud-native systems?
5. What role do monitoring and observability play in maintaining operational stability?
6. Have you encountered challenges in achieving resilience across multiple cloud providers or regions?
7. In your view, how does platform complexity affect resilience?
8. To what extent do you consider cost-efficiency a constraint on designing resilient systems?
9. How do you approach dependency management or avoid vendor lock-in?
10. What best practices have you established for minimizing downtime or accelerating recovery?

Interview summary – Interviewee 3

The expert is involved in a European technology and standardization project that supports federated cloud and data infrastructures. His work focuses on building a trustworthy digital ecosystem that is supported by a technical and organizational trust framework. The aim is to enable redundancy, interoperability, and sovereign data processing in cloud infrastructures - particularly concerning European values, security, and sustainability. A key message was that resilience can arise not only from individual IT optimization but also from the structure of entire ecosystems. This is less about completely eliminating dependencies and more about making

them transparent and controllable. Resilience is thus understood as an emergent property of a system that consists of open standards, mutual trust, and shared infrastructure. Particular attention was paid to the distinction between IaaS as a technical component and PaaS/SaaS as a strategic enabler - for example for process automation, reporting, or regulatory compliance. The expert emphasized that the actual added value of cloud computing often lies not in the infrastructure, but in the higher-value platform services.

In the context of vendor lock-in, the expert explained how an interoperable cloud ecosystem (e.g. based on Gaia-X) can help to reduce vendor dependencies. Thanks to open standards and certifications, a switch to alternative providers can be made more quickly and confidently if necessary - provided a common understanding of trust and data quality is established. This common basis is created by a trust framework that serves as a “common language” for trust. Each participant can decide independently whether and to what extent they want to engage with the framework, whereby the underlying mechanism is standardized. This enables a high degree of freedom with simultaneous structural connectivity. The concept of digital twins to make systemic dependencies visible was also discussed - for example in the aviation industry. Even if this visibility alone does not guarantee resilience, it is an important prerequisite for this. In combination with compute-to-data approaches, in which data is no longer moved but processed locally, new resilient data spaces can also be created - especially for highly sensitive information.

Cloud computing was described as a strategic resilience factor, particularly due to its short-term scalability, elasticity, and access to resources that would not be available internally. This flexibility is seen as a fall-back option in crises but is associated with high costs. At the same time, the cloud could bring regulatory advantages through certifications and infrastructure standards. Looking ahead, the expert sees regulatory impetus e.g. through the digital product passport as an opportunity to reduce administrative effort, increase transparency, and build new resilient supply and production networks through standardized data spaces. Overall, resilience is not understood here as a purely technical concept, but as a system property of networked players, technologies, and governance structures, supported by standardization, trust, and decentralized control mechanisms.

Interview summary – Interviewee 8

The interviewee is an experienced IT consultant specializing in cloud infrastructure and strategic cloud transformation. His experience during the pandemic showed that the majority of organizations approached cloud strategies reactively rather than proactively. Organizations that had invested in cloud technologies ahead of time, before the crisis, particularly in adaptive sectors such as e-commerce, were significantly more resilient. Businesses in legacy sectors, however, lacked the strategic vision to leverage the cloud technologies in an optimal manner.

The specialist pointed out that, in most instances, cloud transformation programs were primarily confined to IT departments and not integrated strategically at the executive level. Consequently, the potential of cloud computing as an organizational and strategic enabler of resilience was typically underleveraged. He pinpointed that cultural adaptability and change willingness were essential success determinants. Organisations that had conservative mindsets, risk aversion, and low international exposure were much behind in embracing new technological needs. Geopolitical considerations have increasingly influenced cloud computing strategies. The analyst suggested that data sovereignty concerns, GDPR compliance, and the advent of legislation such as the EU Data Act compelled a rethink among many organizations regarding their selection of service providers and cloud architectures. The evolution of multi-cloud approaches and sovereign cloud offerings was characterized as a reaction to these obstacles to balance operational flexibility, regulatory compliance, and strategic autonomy.

A prevalent pattern that was discovered was the disconnect between technical cloud migration processes and realization of actual resilience improvements. Most organizations carried out basic lift-and-shift migrations without re-architecting applications or streamlining processes, thereby capping the potential resilience benefits that could be derived from cloud adoption. The subject matter expert also highlighted the dangers of inadequate project management and the absence of well-defined resilience objectives throughout transformation programs.

Looking to future developments, the expert highlighted the keen strategic significance of new trends like edge computing, multicloud infrastructures, and the use of artificial intelligence in cloud environments. He considers cloud computing not merely as a means of reducing costs, but as a strategic platform that allows for quicker responses to crises, better data-based decision-making, and the creation of more flexible and resilient organizational structures. But he

emphasized that genuine resilience demands not only technological readiness but also a revolutionary cultural change on every level of the organization.

Interview summary – Interviewee 9

The expert was a former principal engineer with extensive experience in cloud architecture, infrastructure automation, and other distributed systems at one of the three big cloud providers. His observations reinforced the idea that hardware structures and architectural redundancy alone will not provide resiliency; it is fundamentally about minimizing MTTR, not getting a theoretical high availability level. He asserts that while it may be appealing to deploy your application in multiple regions and have a level of redundancy in your architecture, this leads to an enormous increase in costs and operational complexity, making it unrealistic for most companies. This leads to the conclusion that prioritizing speedy recovery processes – consistent backups, automation of recovery process, and well-documented run-books – is more practical and realistic for companies trying to achieve resiliency.

The expert pointed out that cloud infrastructures, although marketed as resilient, don't make systems resilient in a vacuum. Resiliency is dependent on how companies architect their applications, maintain data consistency, and prepare for failure. He noted that many enterprises probably don't have the architectural patterns to survive latency, regional failure, or failure of great magnitude. This is because many applications were built under the assumption they will never be distributed. He pointed out that resiliency requires planning around caching, fail-over, and gradual degradation, along with a strong operational culture. With respect to vendor lock-in, the expert offered a nuanced view. He indicated that generally higher resilience is even more closely associated with higher vendor lock-in because the enterprise virtually has the dimension of complexity, redundancy, and mean time to recovery, in effect, outsourced to hyperscalers. As with many of the existing infrastructure industries, such as grid power or payments, systemic resilience comes with trade-offs that are realized when organizations agree to depend on a service supplier. He reiterated that while vendor lock-in can increase risks, it can simultaneously facilitate greater access and democratization, for customers and organizations seeking to bridge a personal gap to resilience (providing resilient services and infrastructure on a budget for small businesses builds resilience overall in society).

Where cloud computing substantially intersects with organizational resilience is that often technical decisions are enmeshed within business promises you take into account for your customers. Each company's level of resilience, logically, is distinct according to business model and customer expectations. A company in e-commerce may require continuity of service provision, where companies in other industries could have significantly diminished expectations or tolerances for downtime, even if temporary. The expert indicated that strategic resilience does not lie strictly with tolerable decision-making based on technical choices (i.e., lowest cost or risk). Rather, strategic resilience requires cloud architects to examine how cloud architectures align with risk appetites, customer contract obligations, etc.

In terms of future developments, the expert was skeptical about the role of AI in deterministic recovery processes, arguing that resilience needs predictability, not probability. He sees resilience enhancement through classical automation, infrastructure design, and operational discipline rather than speculative AI-driven mechanisms. Finally, he pointed out that physical capacity constraints and economic realities would continue to shape cloud resilience strategies, with independent data centers and spillover models complementing hyperscaler ecosystems when capacity limits are reached.

Interview summary – Interviewee 10

The expert engages in cloud consulting and infrastructure management for top German companies. His extensive experience with diverse projects determined that the initial adoption of cloud computing was mainly reactive, undertaken because of emergencies like the pandemic. However, it progressively became a strategic enabler of operational and organizational resilience. He drove home the fact that cloud infrastructures provide required architectural flexibility, enabling companies to disaggregate IT components, minimize internal dependencies, and scale rapidly in the face of crises. The ability to virtualize major operations, such as retail checkout processes, came particularly handy amidst pandemic-driven shortages in labor and demonstrated how up-front cloud investments yielded returns through agility and scalability in delivering resiliency. The author further highlighted that real resilience depends not just on the potential of technology but also on strategic thinking and cultural adaptability. Without leadership engagement and a dynamic IT strategy, cloud adoption may be an exclusively technical modernization effort without strategic returns. He posited that effective cloud transformations in the form of resilience necessitate a top-down process, with strategic-

level concepts of flexibility and modularization carried through to technical execution. Those organizations that had independent development environments and reduced interdependencies among teams exhibited a better capacity for responding flexibly and quickly in periods of crisis.

Human factors were pinpointed as a key area in developing resilience. The expert pointed out that even the best cloud plans fared poorly where employees were unable or unwilling to embrace new technology. Organizational change management, continuous learning programs, and a culture open to technological change were seen to be considered imperative prerequisites. Employee resistance in various large-scale companies significantly influenced cloud technology adoption rates, where supporting mechanisms such as minimum viable products, hackathons, and adaptive training methods had to be introduced. On regulatory resilience, the expert said that physical control over data infrastructure may provide a sense of security, but such resilience lies in the quality of governance and trust in expert cloud providers. Certifications, compliance frameworks, and shared responsibility models were highlighted as being critical in managing regulatory complexity across global operations. At the same time, geopolitical risks such as arguments over data sovereignty and evolving global relationships increasingly influence provider decisions and architecture design, with an accelerated trend towards multi-cloud approaches and regional diversification.

Looking ahead, the specialist thinks that the cloud ecosystem will still evolve further, and multicloud setups, modular architectures, and local sovereign cloud platforms will gain more attention. He emphasized the necessity for organizations to develop IT infrastructures that are both technically scalable and organizationally modular, thereby reducing systemic risks by establishing clearly defined boundaries and specialized platforms for regulated workloads. He defined resilience as a product of dynamic strategic alignment, technological flexibility, and cultural adaptability, with cloud computing acting as an amplifier but not a guarantee of corporate resilience.

Interview summary – Interviewee 12

This expert is the Head of Engineering and Cloud Infrastructure Architect at a technology startup where he plans and builds high-reliability, scalable cloud systems primarily on AWS. His experience taught him that cloud computing offers startups a necessary platform for expansion through scalable resources, elastic costs, and global access without having to bear

huge capital costs upfront. The deployment of cloud technology was more of a proactive strategic choice taken to facilitate accelerated organizational expansion, and not merely a reaction to external pressures. However, he added that certain changes, such as scaling up cost savings and improving system designs, automatically became essential as operational demands changed. The expert added that merely adopting cloud technology does not in itself ensure resiliency; rather, architectural modularity, adherence to best practices, and a foresight strategy are important factors.

Scalability, multi-region presence, and quick adjustment of infrastructures were highlighted as main advantages realized through cloud-based solutions. Particular focus was put on the use of multi-availability zones and global content delivery, enabling near-continuous uptime and fault-tolerant service delivery. Security improvements were also pointed out, mainly through standardized managed services and infrastructure-as-code approaches, reducing operational complexity and vulnerability exposure. On the topic of risks, the expert discussed the trade-offs involved in vendor lock-in. While admitting that a certain amount of lock-in is unavoidable, he asserted that careful design decisions and the utilization of containerized platforms such as Kubernetes can effectively minimize the risk of dependence without compromising flexibility. Multicloud approaches were viewed as a nascent but complicated answer that involves weighing their advantages and operational intricacies carefully. Financial aspects continue to drive cloud strategies. The expert noted that for some workloads, most notably resource-hungry applications like video rendering, cloud expenses can become financially unsustainable in the long term. He anticipates an increasing trend towards partial cloud repatriation, where businesses have hybrid architectures by hosting particular, cost-sensitive workloads on alternative infrastructures selectively and keeping the cloud for scalability and flexibility benefits. Cloud will remain a fundamental building block, but hybrid will be an even more dominant approach for companies seeking to balance performance and cost.

Looking ahead, the specialist envisioned AI integration into cloud operations as a central transformational driver. Since AI-driven infrastructure management is not yet fully mature, he anticipated that in the future, AI would be instrumental in streamlining the processes of cloud monitoring, troubleshooting, and automation. To him, resilience will come to rely not only on technology decisions but also on the strategic capacity to dynamically integrate cloud services, edge computing, and domain-specific infrastructures with workload-specific requirements.

B.2: Strategic & Organizational Resilience Experts

Executives focusing on cloud technology alignment with business strategy, managing digital transformation, and embedding resilience in organizational structures and decision-making (Interviewee 1, 2, 6, 11).

1. From a strategic perspective, how does cloud contribute to business resilience?
2. What organizational capabilities are needed to support adaptive technology use during disruption?
3. How does leadership influence the success of cloud-enabled transformation during crises?
4. What barriers do companies typically face when aligning IT with resilience goals?
5. Can you describe the role of governance and decision-making in a resilient organization?
6. How do you see resilience evolve from operational reliability to strategic adaptability?
7. Have you observed differences in cloud maturity levels across industries or regions?
8. What role does cross-functional collaboration play in building resilience?
9. How should organizations prioritize between agility, scalability, and resilience?
10. Are there any lessons from past crises that have changed how you approach digital transformation?

Interview summary – Interviewee 1

The expert works on the strategic and architectural level of cloud transformation and advises organizations from the administration, pharmaceutical, and retail sectors. In his role, he combines technical understanding with transformation and organizational consulting. His perspective on resilience in the cloud is strongly characterized by business orientation, cultural influencing factors, and a differentiated view of the beneficial use of the cloud.

His central point is that cloud resilience is not only created through backups or technical redundancies but above all through automatable, resilient architectures that are deliberately designed and equipped with the right platform services (PaaS, SaaS). Cloud resilience is not only evident at the IaaS level, but also through the functionality of the higher service models - according to the expert, this is where the real potential for relieving employees and automating critical functions lies. A common misunderstanding in previous cloud adoption projects was to

use the cloud as a purely technological “lift-and-shift” solution. This led to higher operating costs, a lack of flexibility, and lower resilience gains. It is only thanks to increased market expertise and the growing maturity of user companies that more strategic transformation is now taking place. As a striking example, the expert cites the shift from CAPEX to OPEX models and thus also a change in the understanding of IT usage and cost responsibility.

According to the expert, it is important that technical resilience measures are only effective if the business logic has been defined in advance. The specialist department must formulate clear requirements and priorities - for example: Which processes must always be available? Which ones can fail? These questions are often unresolved as there is no clear communication or governance structure between business and IT. IT often anticipates requirements without these having been explicitly expressed. During the COVID-19 pandemic, it became clear how important scalability and agility through the cloud can be - but only if they are used correctly. The expert describes cases in which digitized administrations were virtualized within a few weeks, while other organizations took months. The speed of response is directly linked to the degree of cloud usage and organizational adaptability. Hybrid architectures that rely on redundancy, scaling mechanisms, and local fallback levels are described as promoting resilience. Especially in geopolitical crises - such as those caused by tariffs on US cloud services - it is important to retain strategic alternatives. Completely abandoning on-premise structures is therefore risky. The expert does not see the cloud as the sole answer, but rather as a strategic addition that can offer considerable added value in the right context - both in terms of resilience and innovative capacity.

In conclusion, the expert emphasizes that resilience is the ability to react to unforeseen events in a confident and structured manner - with clear communication, functional systems, suitable architectures, and coordinated interaction between IT, organization, and culture.

Interview summary – Interviewee 2

The expert deals with cloud transformation projects, particularly in the area of data infrastructure, backup solutions, and Azure architectures. The technical perspective was at the forefront but was closely linked to strategic, regulatory, and cultural issues.

A central theme was the observation that although cloud transformations have an organization-wide impact, they are almost exclusively initiated and implemented by the IT department. Other departments benefit passively but are rarely actively involved - which can harm integration and process adaptation. This disconnect is particularly evident in conservative industries such as mechanical engineering, pharmaceuticals, or banking. Here, the cloud is often introduced reactively, for example when legacy systems reach the end of their technical life. By contrast, the retail sector is considered to be particularly progressive - it was already investing in cloud-based backup and data storage systems before the pandemic, partly to stabilize the high data loads caused by online business. Companies often implement the cloud for cost reasons, although the return on investment only becomes apparent after several years. A transformation back to on-premise is considered almost impossible, which underlines the strategic importance of the initial decision. At the same time, projects were often initiated without sufficiently assessing the organizational maturity for this - in one case, for example, no one voluntarily took on a key role in the cloud strategy, which noticeably slowed down the transformation. The expert repeatedly emphasized that a lack of change management is one of the main reasons for the failure of transformation projects. The benefits for employees are often not immediately noticeable, while the costs increase directly - which leads to resistance.

In terms of technology, it was highlighted that companies only benefit from the cloud if there is a certain degree of standardization. Highly individualized IT structures are difficult to transfer and hinder efficiency. At the same time, the cloud is seen as an enabler for operational resilience: It enables automation, error prevention, scalability, and access to technologies such as Big Data and AI. However, the expert believes that there is a lot of uncertainty surrounding the latter in particular the practical benefits are still often unclear. With regard to security concerns, it was emphasized that cloud solutions often meet significantly higher compliance standards than internal data centers. According to the expert, standards and certifications at cloud providers offer a regulatory advantage - concerns about data protection (e.g. GDPR) are widespread but often exaggerated from a technical perspective.

In the expert's overall view, resilience is understood as a technological, strategic, and organizational capability that cannot be achieved without cultural openness and a willingness to change. Transformation is ultimately not a purely technical issue, but a human one that requires holistic preparation and internal communication.

Interview summary – Interviewee 6

The expert is a researcher and analyst with considerable experience studying global value chains and the semiconductor industry. Although outside of his area of specialization, he was able to provide useful analogies in relation to the concepts of resilience mechanisms in the chip industry. In particular, he mentioned that a major construct of resilience was collective roadmapping: firms came together to envision advances in technology, and the investments of industry participants were coordinated, a development which dissolved as the number of manufacturers dwindled. The larger conclusion was that thinking collectively about potential risks and opportunities and making plans to deal with them proactively - rather than only reacting to a crisis - is essential for resilience over the long term. Additionally, the expert explained that successful strategic moves within organizations tend to emerge from a combination of identifying movements in the environment early and having the capability to make decisions for action quickly. He talked about Intel making the first move from being a memory chip company to becoming a microprocessor company due to organizational sensing and a decision to act. This way of thinking parallels some concepts related to DCF because perceiving and acting quickly is a key activity in sustaining competitive advantage when uncertainty exists.

About outsourcing and firm boundaries, the expert believed that decisions about strategy were driven by considerations that were not only cost-related but also the fact that the firm wanted to retain control over key intellectual property and core competencies. Trust in external partners was also critical in determining which functions firms were willing to outsource, e.g., TSMC taking on sensitive designs had meaning, just as today in cloud computing concerns regarding data sovereignty, trust frameworks, and control of expensive/valuable technical functions.

During the Cold War, the expert wondered whether the geopolitical landscape was less complicated, but the external political and regulatory pressures facing industries dependent on technology today pose a basic challenge for resilience. The expert emphasized that in terms of dynamic capabilities, timing of strategic investments/repurposing, organizational learning, and adaptation would determine whether they would be resilient or go out of business when faced with technological or market disruption. The expert also advised that organizations must stay cognizant of up-and-coming technologies, such as AI, where fear of missing out (FOMO) could cause irrational investing and expenditure without distinct strategic benefits. He asserted that

authentic strategic resilience cannot be an organization simply following technology trends but requires aligning investments with its fundamental assets and long-term value-generating strategies.

Interview summary – Interviewee 11

This interviewee serves as a manager in cloud transformation consulting for the automotive industry, following stints in cloud strategy development and data analytics with an OEM in the automotive sector. His main takeaway was that having a strong business case was paramount to OEM cloud adoption. He explained that the drivers for cloud usage initially were not strategic agility or resilience, but rather cost, modernization of systems, and the rationalization of obsolete platforms and fragmented legacy robust infrastructures. He noted that many of the legacy systems, especially at established OEMs, relied on mainframe architecture that was developed in the 1960s, which introduced operational risks and inefficiencies, and the cloud provided expedient solutions. However, while a cloud migration may help meet technical benefits, like scalability and potential for cost management, true organizational resilience leverages several other factors, such as strong strategic anchoring, cultural tendencies, and proactive investment in cloud governance. He did mention in his experience that the pandemic had little to no direct effect on the acceleration of cloud transformation, and most cloud initiatives were either already underway or had become independent of COVID-19.

From a regulatory and legal perspective, the expert highlighted that data sovereignty, contract design, and compliance remained critical hurdles in cloud strategies, particularly when customer data was involved. Although regulatory barriers could delay migration projects, he observed that legal departments in large firms typically solved such challenges effectively once initial agreements with cloud providers were in place. Strategic trust decisions — for example, the lower preference for GCP among automotive firms due to competitive concerns — were considered integral to selecting appropriate providers.

In the broader strategic context, the expert explained that companies that tackled technological debt early through cloud transformation placed themselves in a much stronger competitive position. Those that delayed modernization faced mounting risks from fragmented data landscapes and operational inefficiencies. Cloud-enabled centralization and advanced analytics capabilities were seen as crucial for future-proofing production, logistics, and sales processes.

He also pointed to a shift in IT organizational structures: cloud adoption was not merely a technological change but a catalyst for developing more agile, DevOps-oriented approaches across enterprises, enabling faster and more flexible reactions to external market dynamics.

In the future, the expert recognized that concerns over dependency on US based hyperscalers could lead to European cloud strategies being reshaped over the longer term given also the evolution of regulations such as the EU Data Act. While alternatives such as sovereign cloud initiatives were in existence, he did not view any type of shift from dominant providers as yet realised in practical terms. In the end, he described cloud computing as a multiplier for corporate resilience but only for those companies that were willing to marry new technology with future strategic horizon scanning, corporate culture open to re-configuration and brand new levels of organisational agility.

B.3: Crisis & Risk Management Professionals

Risk governance, operational resilience, and major crises experts. These experts had experience in resilience from highly regulated or crisis environments (Interviewee 4, 5, 7).

1. How do you define organizational resilience from a crisis management perspective?
2. What are key components of effective crisis planning and response in large organizations?
3. How do you ensure continuity of operations during unexpected disruptions?
4. What role does communication play in crisis situations, both internally and externally?
5. How do you assess and reduce dependencies on specific systems or service providers?
6. Can you describe how business continuity is integrated into day-to-day operations?
7. What frameworks or standards (e.g., ISO 22301, Mindestanforderung an das Risikomanagement (MaRisk; lit. Minimum Risk Management Requirements), Digital Operational Resilience Act (DORA)) guide your resilience planning?
8. How do you train or prepare teams for incident handling and escalation?
9. What are common weaknesses or blind spots in crisis preparedness that you've observed?
10. How do you balance between technical, organizational, and human factors in resilience management?

Interview summary – Interviewee 4

The expert works for an international financial institution in the area of non-financial risks and resilience, with a focus on regulatory frameworks such as MaRisk, Bankaufsichtliche Anforderung an die IT (BAIT; lit. Supervisory Requirements for IT in Financial Institutions), and the implementation of the new European directive DORA (Digital Operational Resilience Act). His areas of responsibility include business continuity management (BCM), outsourcing management, information security, and the governance of new products.

The description of a paradigm shift was central whereas previously many of the functions mentioned existed in organizational silos, DORA requires a holistic approach to resilience. The aim is to unite all critical areas such as BCM, information security, and third-party management under a coherent governance framework. This would enable the systematic recording of interdependencies and support coordinated crisis preparation. With regard to measuring the success of such frameworks, the expert referred to established instruments such as key risk indicators (KRIs) and key performance indicators (KPI) to continuously monitor risks, test cycles, plans, and adaptation requirements. Resilience is strongly defined here by process quality and compliance with rules, a view that is strongly influenced by the regulatory environment of banks.

A central point of discussion was the critical view of cloud technologies. The expert described how there is currently increasing skepticism among information security experts towards public cloud solutions, especially in comparison to well-maintained on-premise infrastructures. According to his observations, the trend is partly moving back towards local data centers, as these are seen as more controllable and potentially more secure. The often-cited advantage of cloud providers providing security expertise “out of the box” only applies to a limited extent, as in models such as “shared responsibility”, key tasks, e.g. configuration, and encryption remain with the customer. He made a clear distinction according to company size. For small and medium-sized companies, the cloud is a sensible way to achieve rapid digitalization, e.g. for CRM or front-end systems. For large, regulated organizations such as banks, however, the requirements are so high that a complete cloud transformation is hardly realistic from a security and control perspective. Private cloud solutions come very close to on-premise logic but are often complex and expensive.

DD

The expert does not see people as a resilience factor but as the biggest risk factor. Systems are controllable, whereas people are unpredictable. This assessment underlines the regulatory perspective, which focuses on standardization, compliance with guidelines, and technical security. In the expert's view, AI is currently tending to reduce resilience, as new attack vectors (e.g. deepfakes, new forms of malware) are emerging for which banks are not yet prepared. Protection solutions based on AI are still in the development stage and have hardly been implemented to date.

In conclusion, the expert emphasized that regulatory requirements in the financial industry are often “must-haves” unlike in less regulated industries, where many resilience measures tend to be “nice-to-haves”. This results in a particularly high level of structural and procedural resilience in specific sectors, which is, however, strongly based on compliance and control rather than flexibility or technological progress.

Interview summary – Interviewee 5

The expert works in the field of operational risk management, with direct responsibility for business continuity management (BCM), crisis response, and process monitoring. His perspective on resilience is strongly influenced by practice, systems thinking, and human behavior. At the heart of this is the conviction that resilience is not created by technology alone, but by culture, responsibility, and critical thinking.

The dual role of people in resilience processes was particularly emphasized. On the one hand, people are the most vulnerable link in any system, susceptible to routine, stress, and a lack of mindfulness. On the other hand, they can use creativity, personal responsibility, and situational intelligence to save critical situations in which technical systems would fail. The expert therefore calls for the human factor to be explicitly anchored as a component in resilience models, not as a disruptive factor, but as a potential strength. Operational resilience can be considered in three stages: (1) cultural attitude, (2) structural framework conditions, and (3) data-driven management. In many companies, however, this sequence is reversed or incomplete. A resilient organization recognizes that knowledge of consequences often achieves more than mere regulation. Education, context, and understanding are the real levers, including the acceptance of new technologies such as cloud computing.

In the technological area, it was emphasized that although systems such as cloud platforms offer a high degree of technical redundancy and scalability, they can never be completely fail-safe. The final percentage points of resilience always depend on people, their attentiveness, decision-making ability, and ability to act. According to the expert, external factors such as appreciation, freedom to make decisions, and visibility also influence the willingness to take responsibility in crises. He is also critical of the widespread reactive organizational logic ("Why change something that works?"). Many employees develop a "learned helplessness" in the face of disruptions due to a lack of training or cultural drive. This results in workarounds that later manifest themselves as safety gaps or inefficiencies. To counter this, it is important to identify key people in the company at an early stage, regardless of hierarchy - often it is not managers, but inconspicuous but committed players who keep operations running. Looking back on the COVID-19 pandemic, the expert describes how working from home and digital collaboration increased availability, but at the same time led to mental stress, role conflicts, and reduced vigilance. Some people evolved, and others fell back into ineffective patterns. Resilience varies greatly depending on the environment, role, and individual attitude, a further argument for taking the human factor into account in resilience models in a differentiated way.

Finally, the expert draws an analogy from road traffic: no matter how safe a system may be, if an unforeseen external variable (e.g. another driver) intervenes, it is not the model that decides, but the preparation for the unexpected. Responsiveness and training then determine how severe the damage will be. Resilience must be understood in the same way, as active, human-based protection against the unplannable.

Interview summary – Interviewee 7

The expert leads corporate security intelligence and crisis management coordination in a large industrial group with more than one thousand companies. The expert said that resilience is moving away from the reactive crisis management process to a more proactive function with a strategic orientation. The pandemic and subsequent geopolitical crises, such as the Ukraine war and the energy market disruptions, acted as important catalysts that exposed the weaknesses of obsolete Business Continuity Management systems, which had not been appropriately maintained. The expert indicated that the recognition of these weaknesses initiated a larger organizational transformation that enabled resilience to become a strategic priority and incorporated into different areas of the organization, such as logistics and procurement.

The expert explained that crisis management has traditionally meant being responsive to acute crises, but the escalating complexity of crises, now typically termed "polycrisis" (where many risks have overlapping impacts), will require the organization to identify and evaluate risk earlier and create system-wide anticipation capabilities. The business functions need to not only have their own individual resilience measures, but they must also be cognizant of interdependencies across the organization. The expert mentioned easy recurring helixes where the disruptive effect of the initial issue escalates because the cascade of impacts was unclear across the business units. He said an overall systems-level mapping of their processes, interdependencies within organizational units, and potential chain of impacts must be updated regularly and used to strengthen an organization's resilience, but he also acknowledged that these models mean nothing when being used at the corporate level and remain a significant challenge. The expert shared the governance of corporate crisis management structures. He explained that there are crisis units under major business functions, but a corporate crisis team is only called on once cross-functional or system risk has emerged. He believed that a pragmatic, modular way was necessary due to the nature of the size and complexity of the organization. He stressed that resilience initiatives must be economically viable, applying the Pareto principle: not all theoretical risk can or should be contained entirely, resulting in trade-offs between increased investment for risk and less risk coverage within the organization.

Regarding human factors, the expert confirmed that organizational resilience is fundamentally constrained by human behavior. While training programs and awareness campaigns are regularly conducted, particularly in areas like IT security and social engineering, he emphasized that human error, negligence, or non-compliance cannot be eliminated. The organizational culture was described as relatively strong in promoting responsibility, vigilance, and a proactive attitude toward crisis preparedness at all employee levels, supported by regular internal communications and awareness initiatives.

Finally, the expert underscored that resilience cannot be understood as a purely technical or procedural feature but must be seen as an emergent property of the entire organization, encompassing leadership commitment, cultural readiness, technological flexibility, and cross-functional collaboration. He suggested that while the need for resilience is widely acknowledged, consistent strategic implementation and prioritization are still in progress, requiring further integration into decision-making structures at the highest management levels.

B.4: Individual Evaluation using Gioia Method

Table 16: Individual aggregated Gioia Analysis

Source: Own illustration

Aggregate Dimension	Second-Order Themes (Clustered)	Interviewees	Identification of first patterns and similarities	First Emerging Core Findings	Summary
Interviewee 2, 3, 4					
Technological Resilience	- Architectural flexibility through cloud - Modularization as a resilience strategy - Standardized failure resilience through cloud - Risks of overcentralization - Cloud may mitigate IT security risk	2, 3, 4	Technological Resilience is the strongest theme: - All three interviews emphasize that cloud adoption improves resilience primarily through better architecture (flexibility, modularization, failure recovery). Organizational and strategic barriers are frequently cited: - Cloud transformation often remains IT-led and disconnected from broader business strategy. - Cross-functional integration is missing → resilience benefits are not fully realized. Trust issues with major cloud providers are present: - Interviewee 3 explicitly highlights trust and dependency risks (vendor lock-in concerns). - Interviewee 2 hints at provider preferences (AWS/Azure vs. others). Regulatory caution slows down adoption in traditional industries: - Especially visible in Interviewee 2's perspective on private cloud preference in heavily regulated sectors.	Technological modularization is viewed as essential for building resilient IT architectures. Strategic integration of cloud initiatives remains underdeveloped, limiting full resilience potential. Vendor lock-in and trust concerns are emerging barriers to cloud-driven resilience. Traditional industries show higher regulatory caution, influencing their cloud adoption pace.	The first set of interviews highlights cloud computing primarily as a technological resilience enabler through architectural modularity and flexibility. However, strategic underutilization and emerging trust concerns towards hyperscalers suggest that resilience gains are limited unless cloud adoption is embedded more broadly across business functions.
Strategic & Organizational Resilience	- Cloud transformation led by IT departments - Low cross-functional cloud integration - Lack of strategic use of cloud - Vendor lock-in and sovereignty concerns	2, 3			
Regulatory Resilience	- Regulatory caution and adoption reluctance	2			
Trust Factors	- Perception of loss of control and dependency - Distrust towards hyperscalers	3			
Interviewee 1, 5, 6					
Technological Resilience	- Cloud-native design as a stability factor - Robust cloud architecture and automation - Flexibility through modular systems - Scalability as a key resilience advantage	1, 5, 6	Cloud-native architectures and automation are key to technological resilience: - Multiple interviewees emphasize that resilience stems from how cloud systems are designed and automated, not just from using cloud per se. Strategic cloud adoption is essential: - Using cloud consciously and aligning it with business goals is seen as crucial for resilience gains. Organizational gaps limit resilience benefits: - Misalignment between IT and business units, and failure to critically evaluate processes, were mentioned as major barriers. Human factors (mindset and culture) are critical: - Resilience cannot be achieved without a cultural shift towards more openness, flexibility, and continuous learning.	Technological resilience depends heavily on cloud-native architectural design and automation capabilities. Strategic intent and business alignment are critical prerequisites for realizing resilience benefits from cloud adoption. Organizational silos and lack of cross-functional process evaluations severely hinder resilience efforts. Cultural readiness and an openness to continuous learning are necessary to fully leverage cloud resilience potentials.	The interviews confirm that technological resilience through cloud adoption is not automatic but depends on conscious design choices, strategic alignment, and cultural adaptation. Organizational structures and human factors emerge as significant barriers if not addressed properly.
Strategic & Organizational Resilience	- Strategic and conscious cloud use - Resilience enabled through purposeful technology use - Vendor lock-in and strategic autonomy considerations - Responsibility splits between IT and Business	1, 5, 6			
Organizational Resilience	- Lack of evaluation of critical processes - Business-IT misalignment	1, 5			
Human Factors	- Cultural learning curve and mindset shift needed for cloud maturity - Change resistance limits resilience gains	1, 6			
Interviewee 7, 8, 9					
Strategic & Organizational Resilience	- Shift in crisis management approach - Reactivity trap and strategic deficits - Decentralized resilience responsibility - Cloud transformation as a long-term strategic investment - Slow transition due to corporate culture barriers	7, 8	Strategic deficits are widespread: - Resilience is often addressed reactively rather than proactively. - True resilience would require integrating strategic thinking and crisis readiness early. Cloud's potential for resilience is underused: - Cloud architectures enable fast recovery (Mean Time to Recovery as a KPI), but companies often neglect strategic cloud-based resilience design. Human factors and culture heavily slow down resilience transitions: - Corporate mindsets and resistance to technological change delay cloud benefits and resilience improvements. Vendor lock-in as a resilience paradox: - Greater resilience (faster recovery, better automation) often comes with deeper dependency on specific cloud providers.	Strategic resilience efforts remain largely reactive rather than proactive across industries. Cloud-native architectures and automation significantly enhance technological resilience but remain underutilized. Organizational cultures and mindsets are critical bottlenecks in achieving full resilience potential through cloud transformation. Vendor lock-in is increasingly seen as a necessary trade-off for gaining operational resilience capabilities.	These interviews illustrate that while cloud technologies provide unmatched opportunities for building resilience, organizational barriers, reactive mindsets, and strategic neglect severely limit their effective use. Resilience must therefore be actively integrated into both technological and organizational strategies.
Technological Resilience	- Untapped technological potential of cloud for resilience - Cloud-native recovery architectures (Mean Time to Recovery focus) - Automation as key to faster recovery - Cloud capacity and redundancy as resilience mechanisms	7, 9			
Operational Resilience	- Structural intransparency and unclear dependencies hamper crisis response - Rapid switch and modularity as crisis strategies	7, 8			
Vendor Lock-In (Cross-theme)	- Higher resilience often correlates with stronger lock-in	9			
Human Factors	- Organizational mindset limits speed of cloud adoption - Resistance to technological change	8			
Interviewee 10, 11, 12					
Technological Resilience	- Architectural decoupling through cloud - Overcoming interdependent IT architectures - Cloud-native system design for resilience - Automation as a means of minimizing Mean Time to Recovery - Flexibility and redundancy through cloud design	10, 11, 12	Cloud enables both technological and strategic resilience: - Cloud is consistently seen as a tool to decouple IT architectures and create strategic flexibility. Cloud-native architectures and automation reduce vulnerability: - Faster recovery times (MTTR reduction) and flexible scaling are seen as critical resilience factors. Organizational and cultural readiness determine success: - A strong emphasis is placed on mindset shifts, continuous learning, and early strategic investment to fully leverage cloud advantages. Crisis response benefits from cloud: - Examples like Edeka show how cloud allowed companies to quickly adapt during crises.	Technological resilience is significantly enhanced by architectural decoupling and cloud-native system design. Strategic resilience requires proactive cloud adoption and leadership-driven commitment to flexibility. Cultural factors such as mindset change and lifelong learning are essential for sustaining resilience gains. Operational resilience is amplified by cloud's scalability and its ability to support rapid crisis response.	The last interviews reinforce that cloud computing must be strategically embedded and culturally supported to unlock its full resilience potential. Architectural flexibility, operational scalability, and human adaptability emerge as crucial components across all sectors.
Strategic & Organizational Resilience	- Cloud as a strategic enabler - Strategic room for maneuver through cloud flexibility - Early investment in cloud to achieve strategic advantage - Cloud transformation linked to mindset and leadership commitment	10, 11, 12			
Operational Resilience	- Use of cloud platforms to react quickly during crises (e.g., Edeka checkout example) - Cloud scalability for handling peak loads and operational disruptions	10, 11			
Human Factors	- Mindset change as prerequisite for resilience - Need for lifelong learning and cultural openness to technology shifts	10, 12			

B.5: Total Evaluation using Gioia Method

Table 17: Total Gioia Analysis

Source: Own illustration

Aggregate Dimension	Recurring Second-Order Themes (compressed)	Frequency	Cross-Interview Patterns	Overarching Core Findings	Summary
Technological Resilience	Architectural decoupling	11/12 Interviewees	- Cloud-native architecture is critical for technological resilience - Across nearly all interviews, technological decoupling, modularization, and cloud-native designs are highlighted as key enablers for faster recovery and flexible responses to crises. - Strategic alignment is missing but critical - loud adoption is often still IT-led and lacks broad strategic embedding. Companies that aligned cloud transformation with their business strategy saw significantly better resilience gains. - Vendor lock-in seen both as a risk and as necessary trade-off - Most interviewees recognize that vendor lock-in can undermine strategic resilience, but also accept that it is often inevitable when seeking high operational resilience (speed, automation, redundancy). - Mindset and cultural change are non-negotiable for resilience - Organizational culture, openness to change, and leadership-driven transformations were repeatedly cited as the main barriers—or enablers—for achieving resilience through cloud. - Regulatory factors increasingly influence resilience strategies - Especially in European contexts, concerns about data sovereignty, GDPR, and the upcoming EU Data Act influence how companies plan cloud architectures for resilience.	Technological resilience is predominantly achieved through cloud-native design, architectural decoupling, and automation aimed at minimizing recovery times. Strategic resilience requires not only adopting cloud technologies but embedding them proactively into broader business strategies to ensure organizational flexibility and competitive advantage. Operational resilience is significantly enhanced by the scalability and modularity that cloud infrastructures offer, enabling rapid responses to crises. Human and cultural factors are decisive in determining the success of cloud-based resilience initiatives; mindset shifts, leadership engagement, and lifelong learning emerge as critical enablers. While vendor lock-in is recognized as a resilience risk, it is often accepted pragmatically as the cost for achieving superior operational robustness. Regulatory resilience is becoming a strategic priority, driven by geopolitical shifts and evolving legal frameworks like GDPR and the EU Data Act.	Cloud computing offers powerful tools for enhancing corporate resilience, but its success depends not only on technological implementation. Strategic foresight, cultural transformation, operational modularity, and regulatory adaptability are equally critical for building truly resilient organizations.
	Cloud-native design and automation				
	Scalability and redundancy				
	MTTR (Mean Time to Recovery) focus				
Strategic & Organizational Resilience	Cloud as a strategic enabler	10/12 Interviewees			
	Need for proactive strategic cloud adoption				
	Cloud adoption still too IT-driven				
	Vendor lock-in as a strategic dilemma				
Operational Resilience	Crisis adaptation through cloud scalability	8/12 Interviewees			
	Modular systems enable rapid reconfiguration				
Regulatory Resilience	Regulatory compliance and sovereignty concerns	5/12 Interviewees			
	Role of EU Data Acts and geopolitical factors				
Human Factors	Cultural mindset shift essential	9/12 Interviewees			
	Resistance to change as resilience bottleneck				
	Importance of lifelong learning				

Appendix C: Regression Diagnostics

C.1: Linearity and Homoscedasticity Checks

C.1.1: H2

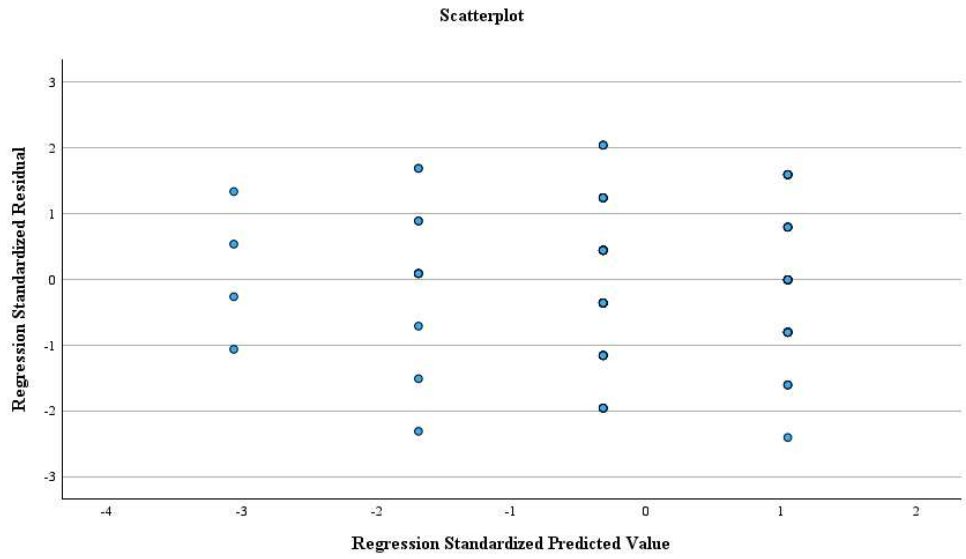

Figure 25: Scatterplot of Standardized Residuals vs. Predicted Values – H2

Source: Own illustration

C.1.2: H4b2

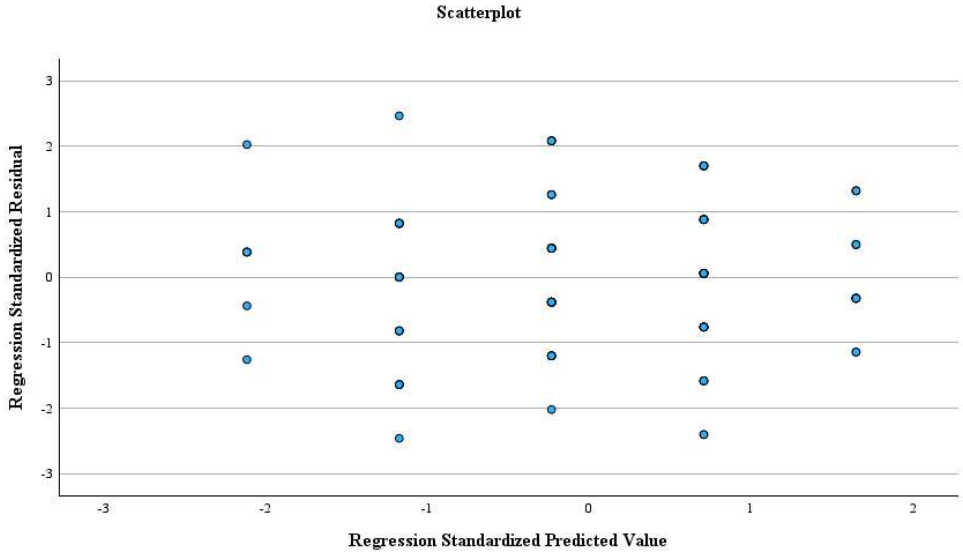

Figure 26: Scatterplot of Standardized Residuals vs. Predicted Values – H42b

Source: Own illustration

C.1.3: H2 and H4b2

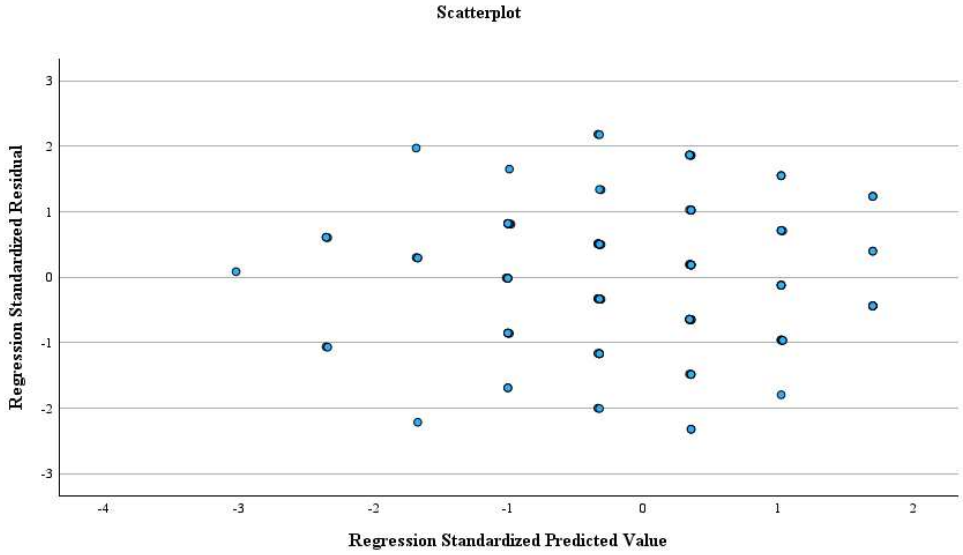

Figure 27: Scatterplot of Standardized Residuals vs. Predicted Values – H2 and H42b

Source: Own illustration

C.2: Normality of Residuals

C.2.1: H2

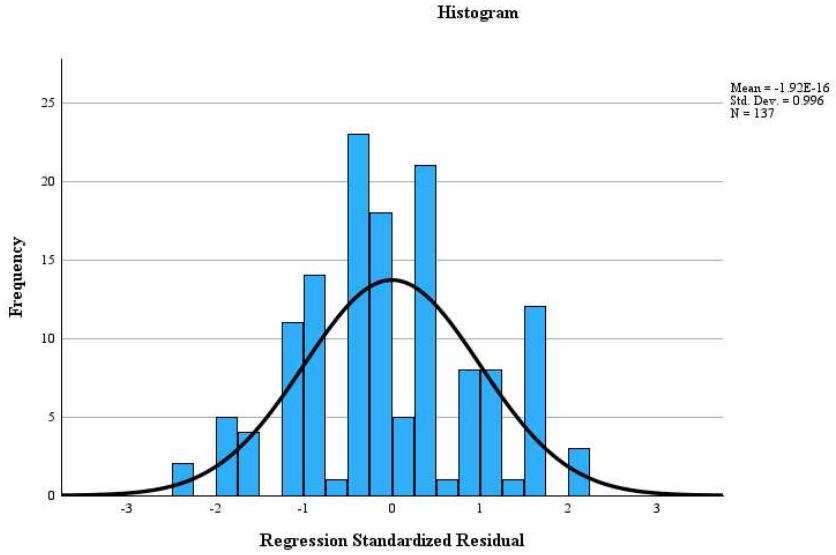

Figure 28: Histogram of Standardized Residuals – H2

Source: Own illustration

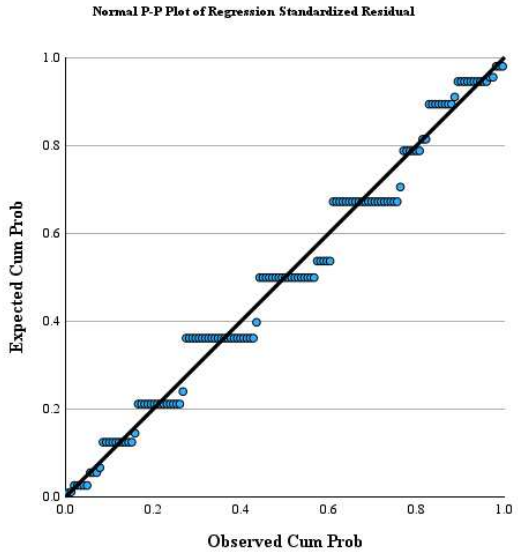

Figure 29: Normal P-P Plot of Standardized Residuals – H2

Source: Own illustration

C.2.2: H4b2

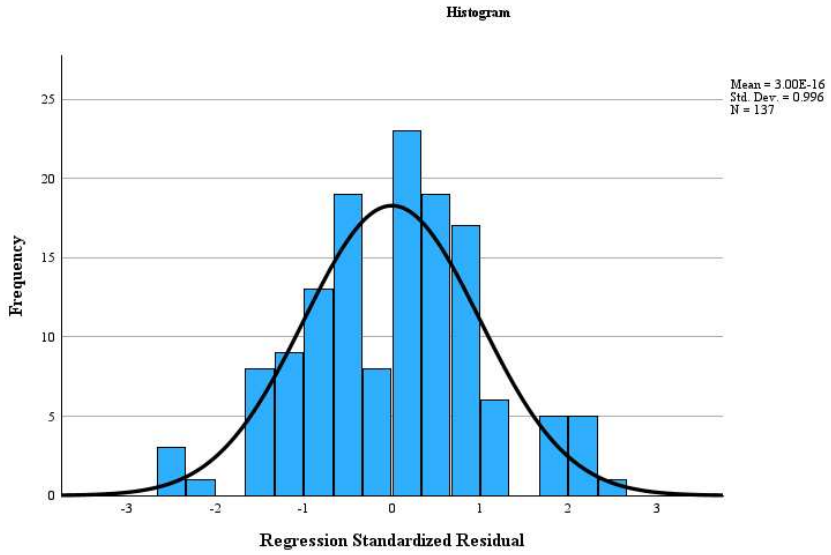

Figure 30: Histogram of Standardized Residuals – H42b

Source: Own illustration

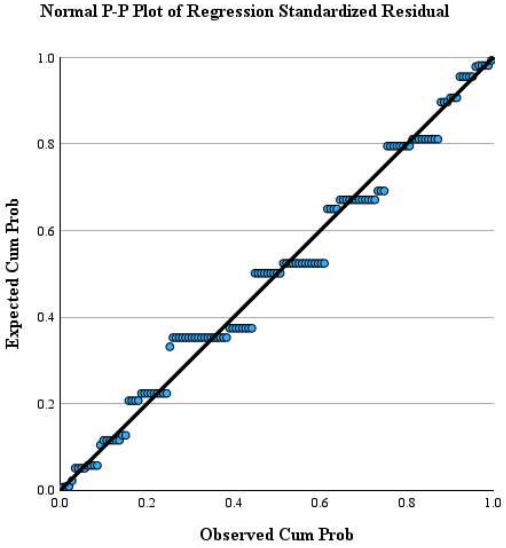

Figure 31: Normal P-P Plot of Standardized Residuals – H42b

Source: Own illustration

C.2.3: H2 and H4b2

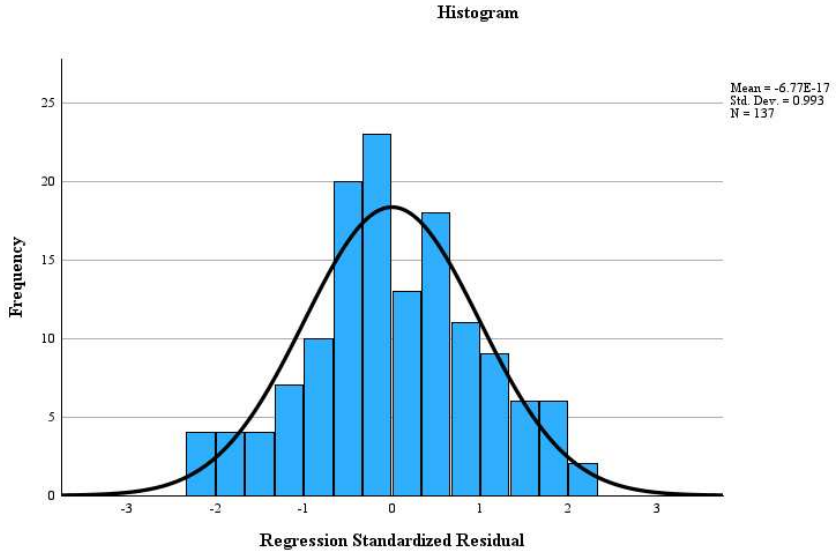

Figure 32: Histogram of Standardized Residuals – H2 and H42b

Source: Own illustration

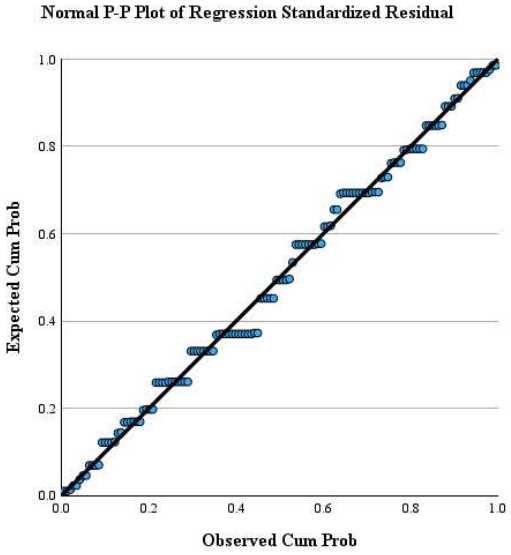

Figure 33: Normal P-P Plot of Standardized Residuals – H2 and H42b

Source: Own illustration