Scientia Moralitas International Journal of Multidisciplinary Research
ISSN 2472-5331 (Print) | ISSN 2472-5358 (Online) | Vol. 9, No. 1, 2024
DOI: 10.5281/zenodo.12801187

Data Strategy of Banks in a Platform Ecosystem Environment – Evaluation of Opportunities and Risks from the Perspective of Different Role Holders

Sebastian Voigt[1], Alexander Holland[2]
[1]UCAM Universidad Católica San Antonio de Murcia, Murcia, Spain,
sgvoigt@alu.ucam.edu
[2]FOM University of Applied Sciences, Essen, Germany,
alexander.holland@fom.de

ABSTRACT: Banking today is increasingly taking place in platform ecosystem environments. Many new players are conquering the market and offering compelling banking products that provide added value and user experience. This trend drives banks to participate in this ecosystem, develop new business models, and provide sustainable solutions to their customers according to the holistic approach. However, these far-reaching decisions imply a comprehensive data strategy for banks. This paper evaluated opportunities and risks from the perspective of different role-holders. For this purpose, this paper applied a purely deductive research approach based on previous assumptions. It has a qualitative exploratory design based on structured interviews followed by Qualitative Data Analysis (QDA). The categories and coding used within the QDA were generated through an interview guide. Esteemed experts from the banking, consulting, IT provider, software development, and startup industries were assigned to the three role groups of banks, IT providers, and regulators and interviewed to provide insights and new findings on various issues of data strategy, data exchange, interaction, and data governance frameworks. The research findings shed light on how banks strategically use and deal with data within platform ecosystems to improve the customer experience and create value for different stakeholders, as well as the associated potential risks with banks' data strategy, its categorization, and IT alignment with their business strategy. Understanding how these risks can be effectively managed and mitigated is crucial. Finally, it looked at how banks work with other ecosystem players to create frameworks and standards for data governance that ensure data security, interoperability, and trust within platform ecosystems.

KEYWORDS: banking, platform ecosystem, data strategy, data governance

Introduction

Banks are increasingly immersed within platform ecosystems in today's rapidly evolving financial landscape, where data reigns supreme as the currency of value

creation. As these ecosystems continue to expand and intertwine with various stakeholders, understanding the intricacies of data strategy becomes paramount (Rufo 2023, 165–178). This paper delves into the nuanced evaluation of opportunities and risks inherent in the data strategies of banks operating within platform ecosystems. From the vantage points of different role holders, including banks themselves, regulators, and technology partners, this paper explores how data strategies shape the dynamics of these ecosystems. By shedding light on the multifaceted perspectives surrounding data utilization, this article aims to provide valuable insights for stakeholders navigating the complex terrain of modern banking.

Problem definition

The topic of data and the associated control of this data and, above all, the extraction and acquisition of insights that imply corporate value must be managed professionally (Boso et al. 2022, 1218–1230). In conjunction with the exponential increase in data volumes (Langer & Mukherjee 2023, 100) and professional analysis to gain insights, companies are facing significant challenges (Choi & Park 2022, 1-2). Customer data is the gold of the 21st century (Giebe 2022, 350-355) and can be aggregated into an overall profile of a customer if individual data components are adequately analyzed and, above all, correctly linked. This overall picture of a customer is completed when external data from various data sources and third-party partners is brought together. This is referred to as a holistic customer approach (Bellos & Kavadias 2021, 1719-1722), meaning that products and services are developed in a customer-centric way, i.e., offered from the customer's perspective and for the customer (Fader 2020, 19-22).

However, due to the nature of their industry, banks face particular circumstances and challenges, such as outdated legacy IT structures (Lipton et al. 2016, 4-5) and, in particular, German banks with regulatory and data protection issues (Wendlinger 2022, 26-31) on the one hand. The Payment Services Directive 2 (PSD2) (European Union 2015, 30) opens the market to new participants. Banks can no longer use their customer data exclusively if the customer wants their data to be passed on by the third-party provider. However, banks can benefit from this opening and develop new revenue streams. Sub-processes, products, or services that would not be economically viable to develop themselves can be produced by creating new collaborations with new providers or FinTechs that specialize in specific services and have market expertise in their field and, where applicable, already have a successful or positive reputation and customer experience (Brodsky & Oakes 2017, 4-8). For these reasons, a bank cannot offer all services alone to satisfy customer's needs. With the help of partners and the further expansion of a bank's services, customer satisfaction and, thus, customer loyalty and retention can be increased (Omarini 2023, 75–113). This creates an environment of a platform ecosystem or a banking-as-a-platform that unites a wide variety of players alongside the bank around

the customer as a holistic starting point and exchanges data streams with each other (Cummins et al. 2020, 319–334).

A data strategy provides the guidelines for an organization's long-term decisions on how it uses data to fulfill its mission and organizational values (Grossman 2018, 45-51). The data strategy should be closely interlinked with IT (Legner & Pentek 2020, 11). In contrast to the data strategy, which is aimed at the data monetization strategy, the IT strategy creates the basis for all data-related activities in the company by aligning the application and system landscape. The IT strategy is not dealt with here in this paper, but how the data strategy can, among other things, align the IT strategy. A data strategy is essential for banks (Karkošková 2023, 7-9) to ensure a coordinated approach as a platform ecosystem player and establish a framework for handling data and exchanging it with other partners while weighing up opportunities and risks. The first frameworks for data ecosystem business models have already been published or are available (Ballon 2022, 4-13). However, the main question is whether banking sector experts know these governance frameworks and standards for creating holistic data management or are already using them within the company. After a thorough literature review, there are several definitions of data governance. According to Abraham et al. and the paper's research design, data governance is a cross-functional framework for managing data as an asset, formalizing data policies, standards, and procedures, and monitoring compliance (Abraham et al. 2019, 426).

Methodology

To evaluate a possible data strategy of banks in the environment of a platform ecosystem concerning two essential prerequisites, i.e., to generate data activities from data assets and data infrastructures (Bonvino & Giorgino 2024, 8-9) and to guarantee applicable EU data protection law (Coche et al. 2024, 3-7) and to analyze the opportunities and risks from the perspective of various role owners, a suitable scientific methodology must be selected. Standardized expert interviews (Hopf 2004, 203-207), which directly illuminate the views of various role holders in banks and collect sufficient primary data, are suitable for this purpose (Anjum et al. 2021, 6-10). This type of methodology is attributed to qualitative content analysis. Mayring says, "Qualitative content analysis wants to preserve the advantages of quantitative content analysis for a more qualitative text interpretation" (Mayring 2004, 161). The advantages, according to Mayring (Mayring 2004, 161), are:

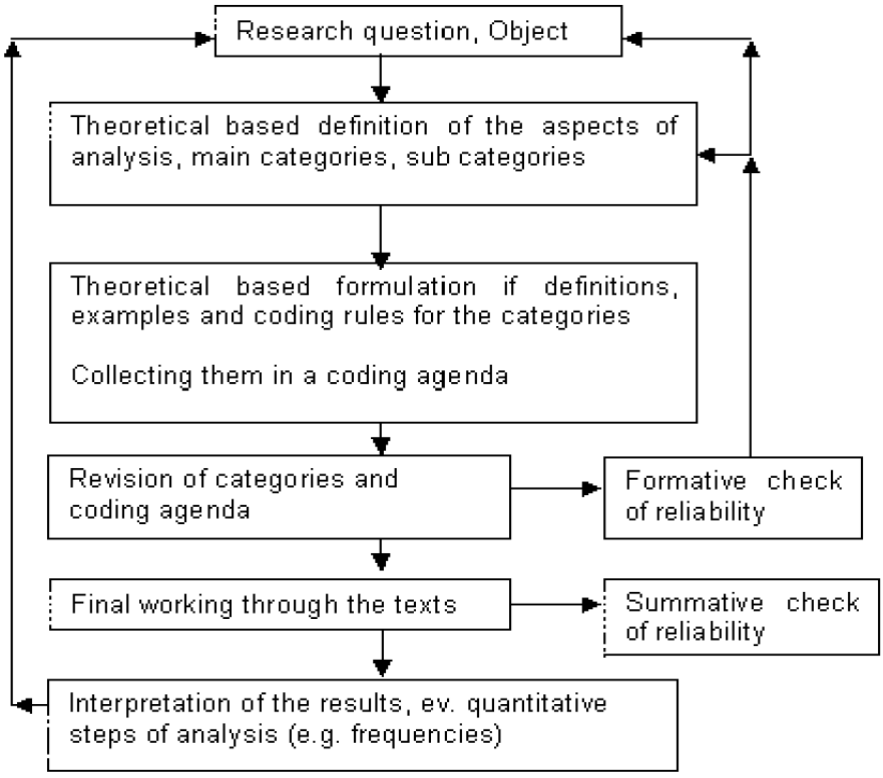
1. fitting the material into a model of communication
2. rules of analysis
3. categories in the center of analysis
4. criteria of reliability and validity

"The above-listed components of quantitative content analysis will be preserved to be the fundament for a qualitative-oriented procedure of text interpretation. We developed several procedures of qualitative content analysis, among which two

central approaches are inductive category development and deductive category application" (Mayring 2004, 161). This article is dedicated to deductive category application, meaning pre-formulated questions and existing categories in the expert interview move along the research questions from the literature analysis. Thus, a methodically controlled category assignment to a text passage occurs (Mayring 2004, 162-164).

As banks can cover more customer needs in the best possible way with the help of third parties and can, therefore, offer their customers a more comprehensive range of services, a holistic ecosystem of providers is developing around the customer that enables data exchange between partners and offers added value for the customer. Elements of a data strategy can be derived from this to regulate data exchange between partners. Expert interviews will be used to evaluate essential aspects of a possible data strategy in terms of opportunities and risks from the perspective of various role holders. To this end, it will be analyzed whether existing data governance frameworks (Bonvino & Giorgino 2024, 8-9; Karkošková 2023, 7-9) are already being used for this purpose and what content a framework should contain. The aim is not to develop a ready-made framework construct for a possible data strategy for banks. The paper initially intends to evaluate findings and potential elements and content of a possible data strategy and sensitize decision-makers to this topic. Further insights and possible ready-made data frameworks or decision matrices require further research.

Figure 1. Step model of deductive category application (Mayring 2004, 162)



In concrete terms, three research questions are initially set up as hypotheses for dealing with the topic. These are as follows:

RQ1: How do banks strategically utilize data within platform ecosystems to enhance customer experience and create value for different stakeholders?

RQ2: What are the potential risks associated with the data strategy of banks operating in a platform ecosystem environment, and how can these risks be effectively managed and mitigated?

RQ3: How can banks collaborate with other ecosystem players to establish data governance frameworks and standards that ensure data security, interoperability, and trust within platform ecosystems?

In the next step, further sub-questions are developed for the three main questions, intended to answer the main questions as a whole. For this purpose, main categories and sub-categories are formed for the main questions and sub-questions. After the interviews, the text passages of the interviewee's answers are coded and assigned to the appropriate categories in a coding agenda. After extensive research, the MAXQDA software (Friese 2016, 34-40) was chosen to conduct the qualitative data analysis (QDA) and evaluation of the interviews. In particular, the seamless integration of the AI, which takes over the automatic transcription and translation of the interview texts in a time-saving manner so that this content can be continued for further manual editing and coding by the author, was convincing (Cao et al. 2023, 5-6). Before data is collected, it is essential to identify the right experts (especially competencies and working environment) for the topic in question. According to Kuckartz (2012, 141-145), the quality of the information depends on the selection of the interview participants who take part in the expert interviews or whose answers are subsequently evaluated. On the other hand, Creswell (2009, 95-108) shows that a concept or phenomenon that needs to be understood because it has been little researched deserves a qualitative approach. For this reason, Mayring's deductive category application is followed by an iterative procedure that ensures a continuous formative review of the reliability of the categories and the coding agenda created so that any necessary adjustments can be made. This can be followed by final work on the interview texts and the subsequent interpretation of the results. Finally, quantitative elements of the analysis, such as frequency or correlation analyses, can be incorporated into the evaluation.

Selection of the experts

According to Kruse, the procedure was followed for the correct selection and grouping of the experts. This states that the following necessary expert groups are essential for adequate overall coverage of the know-how from different perspectives. The first of these is the expert group, which has technical know-how. The second group possesses process knowledge, which goes hand in hand with informal or hidden knowledge. The third group of experts comprises interpretative knowledge, which contains ideas, ideologies, and explanatory patterns (Kruse 2014, 176). The group of experts with technical know-how is attributed to the "IT providers," the

group with process knowledge to both the "regulators" and the "IT providers" and the group with interpretation knowledge to all groups "banks, IT providers, and regulators," but primarily to those of the "banks." All participants interviewed are proven experts in their field and have at least senior or lead positions and specific knowledge in branches like consultancies, IT providers, banks, and FinTechs.

Expert descriptions

Group 1 "Banks"

Expert 1 (Senior Organizational Developer): Senior professional with 30 years of bank experience. This expert is currently working as a Senior Organizational Developer in Corporate/Business Development and Data Management and, before that year, in requirements consulting, sales management, human resources, and corporate communications with a specific focus on human and customer interactions.

Expert 2 (Lead Process and Innovation Management): This expert has at least 18 years of professional experience in banks and is currently working in process and innovation management. Before this, the expert worked in many other areas of a bank, in particular back office and management positions for quality assurance for deposit business, data control with legal support, and evaluation of these topics.

Expert 3 (Senior Project Manager and Expert for Bank Organization): Senior Expert Bank Organization with 19 years of professional experience in ESG banks. Currently an expert for core banking procedures and Partnership Manager and, therefore, the first point of contact for IT providers with whom we work. Before this, the expert worked as an IT security officer.

Group 2 "IT providers"

Expert 4 (Senior Manager Digital Banking): Lead Professional in Digital Banking with 27 years of experience in various banks and consultancies. He focuses on sales and multichannel, product/project management, and mobile banking.

Expert 5 (Team Lead Software Development): Team Lead and Solutions Architect with 12 years of professional experience, mainly in FinTech and e-commerce for banking. He has also worked as a freelancer with programming languages Java and Java Script and as a lead responsible for project management and implementation.

Expert 6 (Founder and CEO): Corporate generalist and entrepreneur focusing on data-driven loyalty and ad technology. More than 23 years of professional experience building digital business intelligence solutions with millions of users. Core expertise in beyond banking, contextual banking, and sustainable banking solutions.

Group 3 "Regulators"

Expert 7 (Senior Product Manager and Chapter Lead): Senior and Lead Professional for Corporate Governance and Multi-Product Manager with more than 11 years of professional experience in banking. Expertise is mainly in Online Banking, Payments, Innovations, Request to Pay, PSD2/PSD3, and Beyond Banking.

Expert 8 (Deputy Data Protection Officer): This is a senior expert on data governance topics focusing on data protection. This includes data protection law assessment and advice on transparency requirements in contractual arrangements with service providers.

Expert 9 (Senior Consultant): This is a Senior Professional for data governance and IT core banking system migration. Before that, the focus for many years was on organizational consulting for banks, new development of direct banks and ecosystem landscapes, end-to-end customer onboarding processes, and accompanying project management activities.

Results and discussions

Before investigating the research questions with the help of QDA can begin, a look at the coding system must be taken. The three research questions are listed here in Table 1, including the corresponding main questions, which have been summarized in categories. Sub-codes are assigned to the categories, which outline the individual categories and are intended to provide further depth of analysis and insight. All sub-codes were developed using the deductive research approach. During the investigation, however, supplementary and for the answer to the research questions, relevant further codings occurred so that these correspond to the inductive approach. In the last column, in particular, under "Further findings worth mentioning under Sub Code 1", further inductive insights are listed that arose during the interview process and are increasingly found in a deeper sub-code dimension.

Investigation of the research questions

The research questions are dealt with by analyzing the coded segments from the categories and centrally summarizing the core statements obtained from them in the categories. An overall evaluation will be carried out in 2 steps:

Single-based expert analysis. All experts' central statements or summaries for each category are recorded here.

Role-based expert analysis using cross-tabulation analysis. For this purpose, the experts are assigned to the three groupings, "Banks," "IT Providers," and "Regulators," and their statements are compared cross-functionally with the statements of the other groupings.

Table 1. Overview coding system

Research Questions	Categories	Sub Code 1	Number of citations (frequency)	Frequency in % of 745 citations	Further findings worth mentioning under Sub Code 1
RQ1: How do banks strategically utilize data within platform ecosystems to enhance customer experience and create value for different stakeholders?			**261**	**35,03%**	
	Data strategy in platform ecosystems		**120**	**16,11%**	
		Classification	29	3,89%	Central data management system, specification and recommendation by partners, data models and analysis options, cost/benefit ratio, cooperations
		Collection, analysis and use of data	50	6,71%	Increasing revenues, standardization, getting to know/understanding customers, sales channels, data protection and law
		Type of data collected and data sources	41	5,50%	Customer master data, customer behavior/interaction, transaction data, data sources
	Improving the customer experience		**83**	**11,14%**	
		Improve customer experiences and generate added value	23	3,09%	New insights about customers, targeted customer approach, user experience, data compliance
		Concrete examples	10	1,34%	Banking products, payment services, personalization, loyalty programs
		Personalize customer data	34	4,56%	Challenges, creating customer profiles, use of AI, embedded finance, data protection, green offers
		Effects of data usage on customer loyalty/satisfaction	16	2,15%	Customer centricity, increased customer satisfaction, prevention of customer churn, cost savings
	Value creation for stakeholders		**58**	**7,79%**	
		What value measures/metrics?	22	2,95%	E-commerce KPIs, joint product use, none, higher-level quality management, contractual agreements
		Creating added value for other interest groups	18	2,42%	Creating and selling customer profiles, non-banking strategy, use and sharing of data
		Data sharing agreements and cooperation initiatives	18	2,42%	Challenges, loyalty programs, none, transparency
RQ2: What are the potential risks associated with the data strategy of banks operating in a platform ecosystem environment, and how can these risks be effectively managed and mitigated?			**178**	**23,89%**	
	Impact assessment		**64**	**8,59%**	
		Possible consequences for all participants	51	6,85%	Customers, banks, partners and everyone together
		Impact on trust in the ecosystem	13	1,74%	Customers, banks
	Risk mitigation strategies		**72**	**9,66%**	
		We banks proactively address and mitigate risks	40	5,37%	when initiating a possible cooperation, compliance
		Risk management frameworks, cyber security measures and data protection guidelines	32	4,30%	when initiating a possible cooperation, frameworks, guidelines
	Joint risk reduction		**42**	**5,64%**	
		Working together to jointly manage data-related risks	24	3,22%	Advice/training, central/secured data pool, pseudonymization of data
		Role of data sharing agreements/governance frameworks for risk mitigation	18	2,42%	Ensuring and tracking common minimum standards for regulation, preliminary review of contracts by experts, clean separation of data storage and use
RQ3: How can banks collaborate with other ecosystem players to establish data governance frameworks and standards that ensure data security, interoperability, and trust within platform ecosystems?			**306**	**41,07%**	
	Collaboration with players in the ecosystem		**52**	**6,98%**	
		Collaboration to create data governance frameworks	28	3,76%	Infrastructure and quality, joint supervisory bodies, cooperation in working groups, Europe-wide data standards are not enough
		Challenges and successful examples of cooperation	24	3,22%	
	Data security and data protection		**37**	**4,97%**	
		Measures	14	1,88%	IT security, modular system, joint data protection agreements, training courses
		Protocols for data sharing	23	3,09%	Joint compliance project
	Interoperability and data standards		**49**	**6,58%**	
		Data standards to ensure seamless interoperability	17	2,28%	Challenges, legal requirements (PSD2/3), specifications by network partners, joint requirements engineering, use of centrally controlled services
		Importance of data formats, APIs and protocols	32	4,30%	Forecast and analysis of future protocols and interfaces; common, standardized, easy-to-maintain interfaces
	Building trust in the sharing of data		**46**	**6,17%**	
		How banks build trust in data sharing	32	4,30%	Work with partners who stand for trust in the market; bank brand, open and clear communication, sensitization of all participants
		Transparency initiatives and mechanisms for fair data practices	14	1,88%	Data strategy, overarching contractual construct for the entire ecosystem, central control system
	Compliance with legal regulations		**65**	**8,72%**	
		Compliance with regulatory requirements	19	2,55%	Voluntary certifications by banks, consistently implement applicable law, only allow audited/certified partners
		Challenges and strategies	46	6,17%	
	Governance frameworks		**28**	**3,76%**	
		Existence of governance frameworks and guidelines	20	2,68%	No standards available; available, but not which ones; no data transfer
		Ongoing adaptation of the frameworks	8	1,07%	Experts needed, technical development
	Dealing with data ownership		**29**	**3,89%**	
		Question of data ownership and rights in the ecosystem	15	2,01%	Agreements, restrictive data transfer, only query of other databases
		Cooperative approaches to resolving potential disputes	14	1,88%	Common behavior towards customers, equal benefit for each partner - no overreaching, central arbitration office

Single-based expert analysis

Research questions 1 to 3 are evaluated below based on the experts' answers. The associated categories are summarized for each research question.

RQ1: How do banks strategically utilize data within platform ecosystems to enhance customer experience and create value for different stakeholders?

Table 2 primarily expresses the heterogeneous responses of the experts. The exact answers can also be seen here. The classification of the data strategy in platform ecosystems is often specified and recommended by IT providers. Experts also consider data control essential to fulfill legal requirements in an overarching central data management system. There is a willingness to cooperate, but implementing a partner ecosystem is challenging and complex, and experts are urgently needed. The approach to collecting, analyzing, and using data is based on higher revenue expectations through generating and using additional offers, new potential business models, and sales opportunities. Howanks are also being driven to act and think in ecosystem terms by the changing platform ecosystem world as a new competitive situation by new competitors such as (fin-)tech companies. For data analysis and evaluation, customer master data, transaction data for categorizing customer interests and needs, interaction data, some external data sources for enriching the customer database, and the networking of internal data with various departments are primarily used. To increase customer experience and generate further value, a user interface in the application where the customer can easily find their way around, transparency and fairness in the use of data, transparent and open communication, and, above all, a targeted customer approach are seen as success factors.

Table 2. Summary table for RQ1

		Data strategy in platform ecosystems			**Improving the customer experience**				**Value creation for stakeholders**		
		Classification	Approach why collection, analysis and use of data	Type of data collected and data sources	Improve customer experiences and generate added value	Concrete examples	Personalize customer data	Effects of data usage on customer loyalty/satisfaction	What value measures/metrics?	Creating added value for other interest groups	Data sharing agreements and cooperation initiatives
Banks	Expert 1 (SOD)	**Specification and recommendation by partner**	**Increase revenues by using additional offers**; get to know/understand customers to predict and plan resources; use sales channels and suitable marketing campaigns	Customer master data (demographic data); **tracking customer behavior; transaction data**, frequency of input channels; data sources such as ATMs, use of other platforms, offers	**New insights about customers**	Binding to regional roots through sponsoring		Presence at the customer, always available and finding suitable solutions	SLAs only		**Difficult, few skills available**, you don't want to make yourself measurable, transparency for the customer should be made measurable
	Expert 2 (LPM)	Data control through compliance with legal requirements and evaluation of customer data; specification and recommendation by partners, **lack of experience in building an external ecosystem**	**Generating added value through non-banking services**; dependence on IT partner to implement data protection slows down further development	Customer behavior is tracked less, but more click numbers, **customer interactions from transaction data using smart data**	**An interface where customers can easily find their way around**; transparency in declarations of consent, added value of the ecosystem must be greater than the regulatory framework, which currently ties up a lot of resources	Individual designs for current or credit cards, house bank program as a loyalty model	Individualization too expensive, therefore standards are used; AI is currently rated very highly, which models can the ChatGPT map in banks?; personalized CO2 tracker	**Cost savings through synergy effects** when using several banking products, favorable price for customers	**none available**		Investments in young companies, **otherwise no cooperations or agreements**
	Expert 3 (SPM + EBO)	**Data strategy is not part of the IT strategy**, it is a **separate strategy** because it goes **much deeper**; data protection as a central issue; tension between benefits and data protection	**Changed platform ecosystem world as a new competitive situation**; dilemma between collecting as much data as possible and the data protection issue, where banks have a significantly different relationship than other ecosystem providers such as Facebook, Meta or Twitter; current use of separate data pools	**Customer master data; tracking behavior** on the homepage via heatmap and conversation rate/abandonment rates; **transaction data**	New insights about customers, which target group, demographic data; **targeted customer approach**; but: tracking of the user experience in completion routes only possible to a limited extent, **systems do not support this function**	similar construct to Payback as a **loyalty program for organic supermarkets**	**Significantly more financial and technical resources required**; manual and rule-based processes; tracking of homepage click behavior to change customer onboarding process; restriction to certain people, groups and clusters of people; use of AI	Customer surveys; using **signs** to understand customers **when they want to leave the bank** (early filtering)	**Metrics for sales channel and product sales channel usage**, what is case-closed and what is done by manual rework; SLAs	Regional ecosystem through loyalty program with organic supermarkets, otherwise the bank is still in its infancy	Loyalty program with organic supermarkets

IT Providers	Expert 4 (SMDB)	Increase revenue per customer (share of wallet), use data models and analysis options; the current topic is that banks use their own data in the best possible way and only start with cooperations	Data mining in the past, now smart data using AI with enrichment and refinement of internal and external data, drawing conclusions and generating added value; next best action and tracking product benefits and input channels; use of demographic data	Customer master data and demographic data; transaction data and payment flow analysis; use of external data sources to enrich customer data and gain new insights	**Targeted customer approach** by aggregating all data sources to obtain a **complete picture of a customer**	Buy now pay later	Identify certain characteristics in sales that suggest that a product could be of interest to the customer (meet and arouse customer demand); **prospective evaluation and submit offers to customers at an early stage; embedded finance**	**Prevention of customer churn** by providing suitable offers at an early stage	Utilization rate of partner products and joint product use; mutual customer acquisition	Non-banking strategy; Which products have I not recognized at the customer? What products does the customer have elsewhere? Permission to share data to offer products from the partner ecosystem; added value for partners is their targeted product placement; regional ecosystem as marketplace orchestrator	
	Expert 5 (TLSD)	**Central data management system** necessary; data control difficult as data is stored in different peripheral systems and with different service providers and often uses old core banking system, difficult implementation		Transaction data and **data in portals**	Targeted customer approach through **hyper-personalization**; address customers by name, display interesting and relevant content; **conversation rate as a central KPI**; **create a uniform user experience**	Locker management app, invoice management app	**Create customer profiles, display relevant content; use and train AI to anticipate what the customer needs**	By displaying relevant content, the **customer enjoys the application more**	**E-commerce KPIs** such as error rate, abandonment rate, conversion rate; **SLAs** such as software quality, bugs, downtime, Dora metrics	Providing applications via a marketplace (hub); creating customer profiles and selling (data), buying customer data from tech companies such as Google, Facebook, etc	
	Expert 6 (F + CEO)	**Specification and recommendation by partners**; many different ways to use data, analytics, business insights or the evaluation of data; protectionism still predominates	**Development of new products and business models**; use of **additional offers**; **future personalization of services**, especially **targeted customer approach**, avoidance of scatter loss in customer approach;	Transaction data, financial data (account information data), customer interaction and **behavioral data**	Improving customer interaction; **collecting interaction data from various sources, aggregating it and generating insights with the help of data analytics**; but: compliance more relevant, which data is actually used?		Internal corporate culture at many banks does not allow the evaluation of data, **lack of skills**; personalized customer approach by creating customer profiles, **picking up customers much more specifically with the topics that interest them**	**Customer centricity in overall strategy**, employees must go along with it; sustainable extension of customer relationships, prevention of customer churn		Internal networking of customer data in various departments of a bank, corporate customer segment has a lot of catching up to do; offering additional services from Beyond Banking through targeted sales measures and customer approaches	**none**; challenges: very political and rigid structures, mindset often lacking, politically unwanted; upcoming EPI could help as a transparency initiative
Regulators	Expert 7 (SPM + CL)	From a data protection perspective; banks are reluctant to pursue the topic, to what extent may this data; **Open questions from a legal perspective**; data models and analysis options, derivation models; **difficult to implement**	**Generation of added value**; customer has several business connections, use through Access to Account interface	Sales analysis, **cataloging and categorizing data; use of external data sources**	Central storage of data	Switch to electronic mailbox for customers: simple, long data retention, no unnecessary searching, no physical filing required	Conversion of mail dispatch to electronic mailbox for selected customers	Cost savings	Establishment of a higher-level, data-driven quality management system; the insights gained can be incorporated into data-driven requirements engineering	Buying customer profiles and customer data; using and sharing data in a network, but only as much as necessary; the use of data by third-party partners must be made clear to customers; omnichannel usage analysis	Challenges: **many data protection regulations play a major role, highly complex data** must be released in a clean and regulatory manner; clearly communicate data usage by third-party partners; shared portal usage
	Expert 8 (DDPO)	Data analysis only with customer consent; **analysis options reach their limits**	Find new sales opportunities; if there is no legal basis, then no analyses permitted	Customer master data, categorization of data	Targeted customer approach, **transparency and fairness towards customers**, **clear communication**	Photo bank transfer: convenient and simple transfer process		**Save costs, simplify processes, save time**		Use and sharing of data in the network, formation of banking cooperations	
	Expert 9 (SC)	**Specification and recommendation by partners**, tasks and services distributed responsibilities within the network; cost/benefit strategy; expansion of cooperation and partner management	**Generating added value**, listening to customers and adapting products, **getting to know and understand customers**; aggregating and bundling customer data using a standard; volume and economies of scale	Customer behavior, interactions, interests, transaction data, **networking of internal data sources**	Individual customer and product advice	**CO2 tracker based on transaction data**	**Create customer profiles based on interests; categorization of purchases using AI; prospective evaluation, not reactive**; data protection as a challenge, customer consent is not sufficient to obtain all data; green offers	**Customer feels understood and in good hands, needs are recognized and taken into account**	**Google Analytics**, tracking systems for customer movements; **joint product use, which customers come to the bank from the partner**; **reputation and performance of the partners**; SLAs	Use and sharing of data in the ecosystem; kind of voluntary commitment so that the ecosystem remains interesting for all participants; regional ecosystem with integration of suppliers and consumers	Loyalty program Cooperation between banking and retail (supermarkets); active approach to partners; development of a joint reporting system to create transparency

Specific examples of enhancing the customer experience include sponsoring regional roots, individual designs, loyalty programs such as the house bank program, loyalty programs for organic supermarkets or retail, or a CO2 tracker based on transaction data. The personalization of customer data takes place by awakening or covering customer needs and a prospective evaluation of a customer to send suitable offers to customers early. This is done by creating customer profiles so customers are only shown relevant content that interests them. Using and training AI makes it possible to anticipate the customer's needs.

However, banks require significantly more technical and financial resources for implementation, and manual and rule-based processes still dominate. Data protection is again seen as an implementation and risk factor here. Data usage measures have a positive impact on customer loyalty and satisfaction. Here, a more favorable offer can be made to the customer, as cost savings arise from synergy effects when using several banking products. In addition, customers who are ready to churn or cancel can be identified early and encouraged to stay by displaying suitable offers. By displaying relevant content, the customer has more fun with the application, extending the customer relationship. In addition to simplifying processes and applications and saving time, the customer feels understood and in good hands. Needs are recognized and taken into account in good time.

Value creation for stakeholders can be defined using various value measures and metrics. These include SLAs (Service Level Agreements), frequently mentioned contractual constructs. However, the usage rate of partner products, joint product usage, and benchmarks for mutual customer acquisition can also be important indicators. Important e-commerce KPIs such as conversion rate and establishing and tracking a higher-level, data-driven quality management system are also mentioned. However, some experts say that they are not aware of or do not use any metrics on this topic (table no. 2, exp. 2, 6 and 8, cat. 8). To generate additional value for other stakeholders in an ecosystem, loyalty programs, beyond/non-banking strategies to create a marketplace where bank as orchestrator brings providers and consumers together on one platform, the associated use and sharing of data in an ecosystem as well as the buying and selling of customer data or profiles are mentioned.

Data-sharing agreements and collaboration initiatives that contribute to the ecosystem's overall value proposition are often lacking. Challenges such as complex implementation, the need for more skills and mindset, political and rigid structures, and many data protection regulations make agreements challenging to design. On the other hand, there are ideas for implementing various loyalty programs and cooperation initiatives. To implement these cooperation initiatives, a joint reporting system must be set up to create transparency and ensure regulatory compliance.

RQ2: What are the potential risks associated with the data strategy of banks operating in a platform ecosystem environment, and how can these risks be effectively managed and mitigated?

First, the impact assessment and the possible consequences for all participants are examined. On the customer side, there is an unwanted sharing of their data, resulting in a loss of control over data sovereignty and the risk of sensitive data being used for analysis. For banks, there is the risk of incorrect conclusions being drawn from data, an increased reputational risk with third-party companies, and, if applicable, the risk of sanctions in the event of data protection violations in the ecosystem, unauthorized data use beyond the intended purpose and, finally, the loss of customer trust and termination by the customer. In turn, the cooperation partner may need better performance or fail to keep its performance promise. These risks hurt trust in the ecosystem. Experts agree that inconsistent data processing disturbs customer trust and that such data breaches can quickly go viral, accelerating the unsettled customer trust and the associated terminations. Banks, in turn, feel compelled to check their partner network more closely to ensure data consistency in the case of new systems or cross-systems. A poor reputation of the partner can weaken the bank's reputation and the brand, and the partnership can be permanently damaged. Banks can proactively address and mitigate risks as follows. When initiating a potential partnership, the choice should be made to favor high-performance partners with banking experience. For this purpose, a joint, modern, or currently used software that technically implements current law should be used. Before the application is introduced, the risks and requirements should already be recorded and taken into account in the decision-making process when choosing the application (table no. 3, exp. 1, 3 and 5, cat. 3). In addition, a precise definition and procedure for the use of the data should be recorded at the outset. The roles of each partner in the ecosystem should be clarified. Early and regular involvement of internal auditors and consultants and the implementation of monitoring and control systems should continuously monitor and, if necessary, identify risks. Contractual frameworks can prevent risks. It is essential to meticulously document objectives, findings, and joint measures with partners, such as cyber security and data protection guidelines. Furthermore, the contract should be balanced and fair and specify which partner may use which customer data. Dedicated encryption and access management must also be described in detail.

Other frameworks that should be considered for data and IT security are ISMS (Information Security Management System) for protecting all information in the company, ISO (International Organization for Standardization), and, in particular, ISO 27001 to reduce information security risks. Furthermore, the ISMS helps to better fulfill security regulations and promote the development of a security culture. BAIT (Regulatory Requirements for IT) helps financial companies create a framework for trusting cooperation between specialist departments and IT managers, reduce cyber risks, and optimize IT processes. PCI DSS compliance (Payment Card Industry Data Security Standard) establishes essential consumer protection. It helps reduce data breaches and fraud throughout the payment system and ITIL (Information Technology Infrastructure Library), thus representing a collection of processes and tasks considered best practices for IT service

management. Compliance with and implementation of these frameworks must be monitored and checked continuously. External (renowned) audit experts such as the Chaos Computer Club can provide new impetus from outside and enhance the reputation of the bank or partner in the event of a positive audit result.

Table 3. Summary table for RQ2

		Impact assessment		Risk mitigation strategies		Joint risk reduction	
		Possible consequences for all participants	Impact on trust in the ecosystem	How banks proactively address and mitigate risks	Risk management frameworks, cyber security measures and data protection guidelines	Working together to jointly manage data-related risks	Role of data sharing agreements/governance frameworks for risk mitigation
Banks	Expert 1 (SOD)	Customers: Sharing of data with many participants, **loss of control**; data easily accessible due to EU directive Banks: **drawing false conclusions from data**; right to be forgotten, correct control that customer data is eliminated on departure, otherwise claims for damages	Customers: **Distrust of data storage**	When initiating a possible cooperation: **precise definition/procedure with data**, **pseudonymization** of customer data	when initiating a partnership: **project screening**, agreement on objectives and findings, **measures with partners** such as cyber security measures, implement and document **data protection guidelines**; use **experienced, protected cloud environment**; **compliance training for employees**; encryption and access management; but: people remain a risk	Create joint training courses/mindset; **central, secure data pool**, central partner for IT systems; **agreement on the use of shared systems**	Record a **dedicated, detailed list/needs** and **tasks of individual partners**
	Expert 2 (LPIM)	Banks: **increased audit risk**, **reputational risk** with third-party companies and possible **sanction risk**; **dependency** on the **third-party partner** depending on specificity	Banks: **Ensuring and implementing increased audit requirements** in the environment	When initiating a possible cooperation: recommendation from the association partner and experience of banks, rely on **third-party partners with banking experience**; **proactive checks**; enter into few or no partnerships		**Consistent exchange with partners**	**Preliminary review of contracts by experts** (data protection, etc.)
	Expert 3 (SPM + EBO)	Banks: Reputational risk with third-party companies, **lasting disruption of trust in the customer relationship until termination**; regulation, i.e. handling of data in the ecosystem		When initiating a possible cooperation: Mitigate risks as early as the **requirements for creating the application**, such as data protection, prior checking of data use, introduction of systems; product proposals for sensitive data (quality assurance); **incremental introduction process** (iterative fixing)	**Encryption and access management**, systems should only be operated by experts	Creating a **common understanding of insights, data interpretations and behavioral structures**; creating a common ecosystem in the network of banks for shared user insights	
IT Providers	Expert 4 (SMDB)	Banks: high regulation, risk and sanctions when evaluating data, which is not permitted; no data use beyond purpose; loss of customer trust and even customer relationship; overreaching of partners		Introduction of monitoring and control systems; creating more transparency than required by law; ensuring data autonomy for the customer	**Designing a fair and balanced contract**, who is allowed to do what with customer data; encryption and access management for confidential data; data security	**Partner** must have a **suitable mindset**	Uniform risk claim, ensuring and tracking common minimum standards for regulation; **economic definition in contracts, especially lead management, how follow-up business of the partner is handled**; **clearly defined interfaces and transfer of responsibilities**
	Expert 5 (TLSD)	Banks: Reputational risk with third-party companies, **small partner companies are not aware of the banks' regulatory requirements**, among other things, or are **inexperienced**; **no data use beyond the intended purpose**; single point of failure; risk of data loss for banks and customers Partners: poor performance	Customers: Data protection problems quickly go viral, customer confidence/customers lose;	When initiating a possible partnership: do not rely on inexperienced partners, mitigate risks in the case of requirements for shared, modern, utilized software	Encryption and access management, **use of the latest standards, correct documentation and archiving for control bodies**		Clearly defined interfaces and transfers of responsibility, definition of shelf lives, responsibilities and update cycles for certain data

	Expert 6 (F + CEO)	Customers: Use of sensitive data Banks: Reputational risk with third-party companies, **strong controversy, high regulation, high security standards essential for partners**; lose customer trust/customers; change risk awareness and focus on international banks	Banks and third-party partners: **Ensuring data consistency** when switching/crossing systems; customers are not allowed to see other customers' data, but this sometimes happens; banks set themselves strong guidelines on data protection; poor reputation of the partner can weaken the bank's reputation	When initiating a potential partnership: **use current technology that implements current law**; Compliance, i.e. involving internal auditors and consultants at an early stage and on a regular basis; **monitoring and control systems**, proof of security standards through **external certifications**; trustworthy handling or pseudonymization of customer data; **tracking opt-in and opt-out processes**	When initiating a partnership: project screening Frameworks: **ISMS, ISO, BAIT and PCI compliance**; **do all relevant legal documents comply with customer and applicable law?**	**Work with external consultants** because this is **not** the **banks' core business/know-how**; pseudonymization of data, personal data does not leave the bank; use **SaaS/PaaS as a central, secure data pool**; agreement on the use of shared systems	Ensuring and tracking common minimum standards for regulation, **powers of instruction, technical and organizational measures** and order processing agreements; **definition of risks**
Regulators	Expert 7 (SPM + CL)	Banks: regulatory gaps in contractual agreements, sanctions; no consistent data collection	Customers: Uncertainty in the event of inconsistent data processing Banks and third-party partners: Ensuring data consistency when converting/crossing systems	**Involve internal auditors and consultants at an early stage and on a regular basis**	Frameworks: **DIN standards**	Advice and training, **exchange formats in committees, specialist councils**, etc.	Clean separation of data storage and use
	Expert 8 (DDPO)	Customers: Use of sensitive data Banks: Reputational risk with third-party companies, damage to image, risk of fines Banks and customers: no data use beyond the intended purpose		Involve internal auditors and consultants at an early stage and on a regular basis; monitoring and control systems such as IT security management, internal audits by **Internal Audit and external audits**	Frameworks: internal control system assessments Compliance guidelines: Follow up and monitor implementation	Advice and training, exchange formats in committees, specialist councils, etc.	Preliminary review of contracts by experts (data protection, etc.)
	Expert 9 (SC)	Banks: Reputational risk with external companies, **onboarding of poor partners** Partners: poor performance	Banks and partners: poor reputation of the partner can weaken the reputation of the bank, **brand and ecosystem/partnership can be permanently damaged**	When initiating a potential partnership: rely on experienced, strong banking partners; clarify who plays which role in the ecosystem	Frameworks: internal control systems, **ITIL, BSI guidelines**; rely on **renowned external audit experts** such as the Chaos Computer Club	Data storage in a central, secure environment; evaluations are carried out via a central location through data queries from other participants; **data pool owner acts in an advisory capacity for smaller, less IT/banking-savvy partners**	**Clean separation of data storage and use**; control via central data pool, **definition of data flows to the central location**; stay in contact, talk to each other and listen to what **the needs of the other ecosystem** partners really are

How banks can reduce risks together with other players in the ecosystem starts with communication and the skillset to create a common mindset, which can be supported with training. The mindset includes a uniform understanding of the ecosystem's findings, data interpretations, and behavioral structures. Regular exchange formats in committees and expert councils and consistent exchange with partners should be used for this purpose. On the technical side, the agreement to use shared systems and a central, secure data pool that performs evaluations via a central location by querying data from other participants can help. On the other hand, it is criticized that the mindset for participation in the ecosystem does not exist and does not reflect banks' know-how and core business. For this reason, collaboration with external experts and data pool owners who can demonstrate experience in the platform economy is recommended. Agreements on the shared use of data and governance frameworks should initially be subject to a preliminary review by experts.

Other contents to be considered in such agreements include ensuring and tracking common minimum standards for regulation related to current laws like GDPR (General Data Protection Regulation) and PSD2/3, powers of instruction, technical and organizational measures, order processing agreements, and the definition of risks. In terms of technical implementation, clearly defined interfaces and transfers of responsibility and a clear separation of data storage and use are essential.

RQ3: How can banks collaborate with other ecosystem players to establish data governance frameworks and standards that ensure data security, interoperability, and trust within platform ecosystems?

According to experts (table no. 4, exp. 1, 3, 8 and 9, cat. 1), banks should agree on a standard system to improve collaboration with ecosystem participants. A participant, such as a data owner or orchestrator, can ensure consistent data storage, management, and IT security. In addition, there should be a uniform and shared understanding of the quality and interpretation of data and common control instances.

Table 4. Summary table for RQ3 part 1

		Collaboration with players in the ecosystem		**Data security and data protection**		**Interoperability and data standards**		**Building trust in the sharing of data**	
		Collaboration to create data governance frameworks	Challenges and successful examples of cooperation	Measures	Protocols for data sharing	Data standards to ensure seamless interoperability	Importance of data formats, APIs and protocols	How banks build trust in data sharing	Transparency initiatives and mechanisms for fair data practices
Banks	Expert 1 (SOD)	Agreement on a **common system**, use of the **same data fields/ consistency**; **common understanding of quality and data interpretation**; access only for authorized persons	**Data outflow/control of any data loss**; agreement and tracking of who gets which access rights; **precisely defining** and **tracking** the **tasks of each participant**; **unequal mindset** Example: auditor who is given access to a bank system	**Joint data protection agreements, deletion concepts; training and sensitization of employees**	**ISMS**, common authorization concept	**Experts needed**	**XML** is widely used, audio and multimedia too complex	Do not pass on data to third parties without being asked; **sensitization and training of employees**	**Central control system**
	Expert 2 (LPIM)		**Dependencies and requirements of umbrella organizations**			Specification by association partner		**Bank brand as trust**, open and clear communication; advising customers on IT security; **raising awareness and training all participants**	
	Expert 3 (SPM + EBO)	Agreement on a common system, common understanding of quality and interpretation of data; consistent data management; **common control instances**; access only for authorized persons; **joint cooperation for uniform governance structures**	Agreement on who gets access rights; **agreement on the use of interfaces**; interface control at the IT service provider	Permanent and immediate security updates, **more investment in IT security**	**Common authorization concept with security levels; coordinated protocols**		**JSON, XML or CSV** for temporary data exchange; **forecast, analysis and use of future-proof protocols and interfaces**; coordinated interfaces, data formats and security protocols	Work with **partners** who stand **for trust in the market**; open and clear communication, **data autonomy remains with the customer**; training courses	**Data contradiction possible directly and at any time**, so that actions lead to immediate constraints; central control system end to end

IT Providers	Expert 4 (SMDB)	**Common understanding of quality and implementation**; **common opt-in procedure**; access controls and logging of accesses			Common authorization concept; common standard for customer identification (two-factor authentication)	**Open Banking standards such as PSD2/3 requirements** should also be **demanded and implemented by partners**; Open Banking Access to Account interface	Encryption via HTTPS, API standards such as JSON and XML	Bank brand as trust, cooperative data promise; **open, clear and transparent communication on data use and purpose**; awareness-raising and training for all participants	**Cooperative data promise**
	Expert 5 (TLSD)	Define common processes and criticalities of data durability	startup in luxembourg collaborates with some participants within the ecosystem		Common authorization concept, latest encryptions see BSI recommendations; current common interfaces	**Experts required; today often individual, bilateral agreements; joint recording of requirements;** use of centrally controlled services	Encryption via HTTP, **better HTTPS**; **JSON**; common, standardized, **easy-to-maintain interfaces**	Appropriate corporate design; communicate honesty for data use openly and clearly; training courses	
	Expert 6 (F + CEO)	**Europe-wide, central data standard necessary for competitive advantages**; PSD2 is not enough; PSD3 will not be enough either; regulation always lags behind innovations; no exchange options, banks have heterogeneous interfaces	No know-how in banks, lack of speed; **clean interfaces and data standard required, control of data flows and data security; control of authentication missing**	Modular system, exercise of data control via interfaces; **clear guidelines and a clear usable everyday framework**	VPN, SSL encryption; sensible interfaces with appropriate protection; **defined communication channels described in BAIT, PCI and ISO**	Affiliate networks do not use a standard, **platform is built before the platform in order to harmonize the data**; stipulation by PSD2/3; **make self-built standard available to other participants**	Protocols: **https, tcp, ip.log** Data formats **JSON and XML**, **GraphQL** for **content areas**; **occasionally old standards** such as VPN, Excel, CSV or DB2 data tables		Guidelines such as **BAIT and PCI**, **contracts such as order processing agreements and technical organizational measures**; **new certification standard required**; international, meaningful exchange standard, support through higher-level contractual construct for the entire ecosystem; central reporting system
Regulators	Expert 7 (SPM + CL)		Do **not send** too much **data beyond the intended purpose**; paradigm shift in mindset, adaptation to new market conditions	**Open and honest communication with customers** on data use **increases acceptance**	**Higher-level protocol for identifying the customer at each partner level**; current, common interfaces	**Joint recording of requirements**; use of centrally controlled services	Definition of common interfaces	Open and clear communication; **transparency about data use**; do not use data unsolicited or pass it on to third parties if no consent has been given and is not defined in the contract	
	Expert 8 (DDPO)	Cooperation in working groups; centralized data management, bundling of data flows via one system	Example: Introduction of a central communication system, communication was too little on one side, with the introduction of working groups communication and cooperation was good	Joint data protection management; processes for deletion concepts	Current, common interfaces	Joint inclusion of data exchange requirements in contracts; **guarantee of confidentiality**		**Establishment of data protection guidelines**, regular employee training	
	Expert 9 (SC)	**One participant as orchestrator** for consistent data storage and processing and IT security; use of the same data fields/consistency; **further development of the ecosystem by obtaining additional data**, new insights and data connections via data mining	**New data can send the wrong signals to customers** Example: Due to changes in purchasing behavior, customers receive offers related to their new life situation	A/B testing, **a shared portal use of the customer**	Common authorization concept; **personalization by creating an account**, do **not offer guest login**		**Standardized, easy-to-maintain interfaces** so that **new participants can be integrated quickly**	Work with partners who stand for trust in the market; rely on **partners with banking experience** who know and already implement the regulations of the banking environment; open and clear communication of the security aspect	National or international data storage; **contractual fixation and establishment of control systems**

Challenges include possible dependencies on the IT provider or orchestrator, uncontrolled data outflow or loss of data control, finding consensus when using standard interfaces, as banks often still use heterogeneous interfaces, unequal mindset or lack of know-how, and slow bank implementation and agreement on who gets access rights. Joint data protection agreements, guidelines, a clear, usable everyday framework, deletion concepts, and customer tracking via a jointly developed portal framework are required to ensure data security and protection. Joint authorization concepts and a common standard and higher-level protocol for identifying the customer at each partner level should enable data sharing. In addition, the customer should be personalized and tracked through the mandatory creation of an account. Guest login should no longer be an option.

Data standards to ensure seamless interoperability should be open banking standards by PSD2/3 specifications and should be required and implemented by all partners, as bilateral agreements still prevail today. For this reason, technical requirements are to be adopted jointly, and standards already developed in-house are to be made available to other participants. However, experts are required to implement these standards. HTTPS for current encryption and JSON and XML for current APIs for data exchange will help as common technological standards (table no. 4, exp. 1, 3, 4, 5 and 6, cat. 6). The contracts should define these standards and be as standardized and easy to maintain as possible so that new participants can be integrated quickly.

To build trust in the ecosystem, banks should, above all, communicate openly, honestly, and clearly with customers regarding the use and purpose of data. The bank's brand stands for trust. That is why they should only work with experienced partners who also stand for trust in the market. Data sovereignty is the responsibility of the customer. All participants in the ecosystem and their employees should be sufficiently sensitized and trained for this. Transparency initiatives and mechanisms for fair data practices include establishing a central control system, the cooperative data pledge, a new certification standard, and a direct, feasible data appeal at any time.

Banks should ensure that the other ecosystem participants implement applicable laws and guidelines such as ISO, GDPR, and PSD2/3 to guarantee the legal regulations in the ecosystem. However, the cooperating partners must also be audited and certified. Here, voluntary certifications of the partner and the banks that go beyond the legal requirements can create trust and be decisive in the choice of a partner. Employees should also be sensitized and trained for this purpose. However, there are many challenges involved. Maintaining compliance is complex and requires external experts for implementation. The shortage of skilled workers and the further increase in regulation exacerbate this situation, making implementation more complex and delaying it. At the same time, there is criticism that the regulatory requirements are too generic and general and do not reflect reality. On the other hand, heterogeneous standards for data exchange prevail, which are opaque and complex. Furthermore, it must be ensured that each participant and their service

providers/partners also implement all regulatory requirements and that monitoring is established. Experts have answered that governance frameworks and guidelines for data sharing are heterogeneous. Either no such frameworks exist (table no. 5, exp. 3, cat. 3), the existence of such frameworks is confirmed but not which ones exist (exp. 4, 8 and 9, cat. 3), or individual frameworks such as ISO27001, SfO (Written fixed Order) as the umbrella term for instruction management in the financial sector and, according to AT 5 MaRisk (Minimum Requirements for Risk Management), contains important provisions for an organization, its internal control system and its IT systems, PCI-DSS compliance, outsourcing management, and the internal specialist service standards are mentioned by the governance department (exp. 1, 5, 6 and 7, cat. 3) for treating the data strategy. It is also noted that some standards need to be updated or recorded to control the data flows. The frameworks are continuously adapted annually and in the event of changes to the provider or technical developments.

The handling of data ownership is primarily ensured by the fact that the customer retains data sovereignty, meaning that he has control over the data relating to himself or to which he is entitled (Gray et al. 2024, 7-8). This is regulated in the customer master agreement or if the customer's declaration of consent is required. Full data traceability should be consistently maintained. The players in the ecosystem are permitted to create a shared data pool from metadata and to compare it to evaluate their own needs so that the individual's data pool remains unaffected and there is no mixing of data, only a query of other data pools.On the other hand, a non-competition clause or a limitation of follow-up business can be agreed upon in contracts. Most experts mention the cooperative approach, which involves establishing a uniform, central arbitration body with a neutral stance and expertise to settle potential disputes. Other collaborative approaches to resolving potential conflicts, for example, in the case of uncoordinated or inappropriate use of data or data breaches, include common behaviors such as openness and transparency towards customers and ensuring equal benefits for each partner so that one or more partners are not unduly advantaged.

Table 5. Summary table for RQ3 Part 2

		Compliance with legal regulations		**Governance frameworks**		**Dealing with data ownership**	
		Compliance with regulatory requirements	Challenges and strategies	Existence of governance frameworks and guidelines	Ongoing adaptation of the frameworks	Question of data ownership and rights in the ecosystem	Cooperative approaches to resolving potential disputes
Banks	Expert 1 (SOD)	**Only allow verified, certified partners** (e.g. ISO certification)	**Raising employee awareness; maintaining compliance, shortage of skilled workers**	Guideline: **ISO 27001**	**Ongoing adjustments in the event of changes to the provider**; in the event of technical (further) development	**Customer master agreement** and **customer consent**	**Uniform, central arbitration body**
	Expert 2 (LPIM)	consistently implement applicable laws such as ISO, MARisk, market catalogs; **new customer processes and materiality checks**	Maintaining business operations due to excessive regulatory requirements, **insufficient capacity for implementation; regulatory requirements continue to increase**	No data transfer, only to fulfill legal requirements		No data transfer, only to fulfil legal requirements e.g. PSD2	

		Compliance with legal regulations		Governance frameworks		Dealing with data ownership	
IT Providers	Expert 3 (SPM + EBO)	**ISO, BSI guidelines, IT security from BaFin, BAIT Risk**, Dora, **EU GDPR, sfixO** according to KWG, audits	Sensitizing employees; maintaining business operations due to high compliance requirements, **hiring of external employees necessary for compliance; know-how and experts needed**, as implementation is difficult; regulatory requirements continue to increase	**none available or partially outdated**	**Experts needed**, shortage of skilled workers	**Full data traceability**, conviction through scientific evaluation approach; customer goodwill	Arbitration board/ombudsman with a neutral stance and expertise; **each partner should have a data protection officer**
	Expert 4 (SMDB)	**Voluntary certifications by third parties**, audited by ISO standard	Use state of the art encryption technologies; external, independent certification of the partner	**available, but not which**		**Non-compete clause or limitation of follow-up business in contracts**	**Common behaviors** such as **openness and transparency** towards customers
	Expert 5 (TLSD)	**ISO 27001**	Training for employees; **which peripheral systems are affected? Dependencies**; monitoring obligations for document-based processing; capacities required for implementation	ISO 27001		Full data traceability for the customer	
	Expert 6 (F + CEO)	Voluntary certifications; **BaFin regulations**	**regulatory requirements too general and generic, not reflecting reality**; **overarching contract that accurately captures data flows desirable for all parties**; **heterogeneous standards for different data flows**, which is burdensome and opaque	**ISO and PCI** as essential; bilateral standards such as AVV and TOM, accompanying audits such as pentests and **technical audits that check implementation**; **otherwise no standard that only checks the actual data flows**; streamlining of contracts and processes to be checked	centralised standard in Europe, not only raw data as in PSD2	Restrictive, no disclosure of data - only if required by law according to PSD2	
Regulators	Expert 7 (SPM + CL)	Applicable law such as GDPR	Communicate legislative changes at an early stage and implement them in teams; who is responsible?	**Specialist service standards** in the governance department	**Ongoing adjustments**	Payment services agreement in multibanking	
	Expert 8 (DDPO)	Implement applicable law GDPR	Onward transfer/outsourcing management; **monitoring** that **each participant and their service providers/partners also implement all regulatory requirements**; monitoring obligations of partners for their service providers in the ecosystem; **very extensive regulatory requirements**, difficult to implement	Guidelines: **sfixO**, data protection management Frameworks: **many available, but not which ones**	**Annual review** cycle		**Liability clauses in contracts**
	Expert 9 (SC)	Implement applicable law, **need-to-know principle**	**Mutual submission of regular reports/evaluations**; central point for maintaining regulatory requirements; what do I do with other data?	Framework: **Outsourcing management** Guideline: ISO 27001 **Further frameworks available, but not which ones**		**Data autonomy for the customer**, simple and fast deletion of data and data traceability; **creation of a common data pool from metadata and comparison for own needs**, data pool of the individual remains untouched, no mixing of data - only query of other data pools; customer behavioral data on a platform (expert system with AI)	Common behavior towards customers, **personal acquaintance of the participants/partners**; **equal benefit for each partner - no overreaching**; uniform, central arbitration office/ombudsman

Role-based expert analysis using cross-tabulation analysis

In the following chapter, the experts are assigned to the three groups, "Banks," "IT Providers," and "Regulators," and their statements are compared cross-functionally with the statements of the other groups. The frequencies of the sub-codes of each group are examined so that the relevance of the informative value of the answers is assessed using matches and deviations.

RQ1: How do banks strategically utilize data within platform ecosystems to enhance customer experience and create value for different stakeholders?

Table 6 shows the role-based expert analysis for RQ1. At first glance, the answers are very heterogeneously distributed, and it takes work to recognize patterns in the analysis. It is noticeable that there needs to be more evidence of concrete examples for improving the customer experience. Furthermore, the experts from the bank's group provided little evidence in the "value creation for stakeholders" category, with 13 quotes compared to the other two groups. This shows the somewhat restrictive attitude of the banks, which is that the focus is not on generating value for different interest groups. Therefore, there are also few data-sharing agreements and cooperation initiatives. For example, expert six from the "IT Providers" group provided nine quotes on the sub-code "Personalise customer data." In contrast, Expert 1 (group "Banks") and Expert 8 (group "Regulators") were unable to add anything to this topic. It can also be noted that the entire "IT Providers" group was able to contribute more content with 18 quotes than the "Banks" group with nine quotes and the "Regulators" group with seven quotes.

Table 6. Role-based expert analysis for RQ1

	Categories / Sub Codes / Expert	Data strategy in platform ecosystems				Improving the customer experience			Value creation for stakeholders		
		Classification	Approach why collection, analysis and use of data	Type of data collected and data sources	Improve customer experiences and generate added value	Concrete examples	Personalize customer data	Effects of data usage on customer loyalty/satisfaction	What value measures/metrics?	Creating added value for other interest groups	Data sharing agreements and cooperation initiatives
Banks	Expert 1 (SOD)	1	9	9	2	1	0	1	2	0	2
	Expert 2 (LPIM)	4	4	6	2	2	3	2	1	0	2
	Expert 3 (SPM + EBO)	3	3	5	3	1	6	2	3	2	1
IT Providers	Expert 4 (SMDB)	2	10	10	3	1	7	1	3	5	0
	Expert 5 (TLSD)	4	0	1	5	1	2	1	6	3	0
	Expert 6 (F + CEO)	3	7	2	2	0	9	4	0	2	7
Regulators	Expert 7 (SPM + CL)	6	5	3	1	2	1	3	2	3	3
	Expert 8 (DDPO)	3	3	1	3	1	0	1	0	1	0
	Expert 9 (SC)	3	9	4	2	1	6	1	5	2	3
	Total	29	50	41	23	10	34	16	22	18	18

Compared to the other two groups, the IT Providers consistently provided the most quotes in their answers. This indicates a high level of expertise and relevance to the ecosystem environment. On the other hand, this role group's nature and professional practice also imply a presumed obligation to market this subject area positively.

RQ2: What are the potential risks associated with the data strategy of banks operating in a platform ecosystem environment, and how can these risks be effectively managed and mitigated?

Table 7 shows the role-based expert analysis for RQ2. It is striking that many possible risks are mentioned with a data strategy in the ecosystem. Half of the risks are mentioned by the IT provider group, which, as the connecting arm, can provide the most comprehensive view of the different perspectives of the participants. In addition, the slightest evidence was provided on how the risks can affect trust in the ecosystem. The Regulators group contributed the most minor evidence overall, which is surprising as this is about risk identification and mitigation. Banks and regulators provided the most minor content in the category of joint risk mitigation. However, the statements in this category were supported with the fewest citations compared to the other two groups.

Table 7. Role-based expert analysis for RQ2

	Categories / Sub Codes / Expert	Impact assessment		Risk mitigation strategies		Joint risk reduction	
		Possible consequences for all participants	Impact on trust in the ecosystem	How banks proactively address and mitigate risks	Risk management frameworks, cyber security measures and data protection guidelines	Working together to jointly manage data-related risks	Role of data sharing agreements/governance frameworks for risk mitigation
Banks	Expert 1 (SOD)	5	1	2	11	6	1
	Expert 2 (LPIM)	4	2	9	0	1	1
	Expert 3 (SPM + EBO)	6	0	5	1	2	0
IT Providers	Expert 4 (SMDB)	8	0	3	2	2	4
	Expert 5 (TLSD)	8	3	5	1	0	3
	Expert 6 (F + CEO)	9	4	8	6	8	3
Regulators	Expert 7 (SPM + CL)	2	2	1	2	1	1
	Expert 8 (DDPO)	5	0	5	3	2	1
	Expert 9 (SC)	4	1	2	6	2	4
	Total	51	13	40	32	24	18

RQ3: How can banks collaborate with other ecosystem players to establish data governance frameworks and standards that ensure data security, interoperability, and trust within platform ecosystems?

Table 8 shows the role-based expert analysis for RQ3. The fewest statements with evidence are cited for "Governance frameworks" and "Dealing with data ownership," which means that the existence of such governance frameworks and guidelines is not or only partially available, which the experts were not always able to define. Many experts, especially IT providers, need help answering how data ownership is dealt with in the ecosystem or only have a few approaches. Much evidence was found in the "Compliance with legal regulations" category, with particular reference being made here to challenges and the fact that the regulatory requirements are already immense and that, as a participant in the ecosystem, regulation increases even further, which banks generally find difficult to implement due to a lack of expertise, capacity, and speed. External experts are often required here. The group of regulators provided the slightest evidence in the "Interoperability and

data standards" category, and the group of banks in the "Data security and data protection" category.

Table 8. Role-based expert analysis for RQ3

	Categories / Sub Codes / Expert	Collaboration with players in the ecosystem		Data security and data protection		Interoperability and data standards		Building trust in the sharing of data		Compliance with legal regulations		Governance frameworks		Dealing with data ownership	
		Collaboration to create data governance frameworks	Challenges and successful examples of cooperation	Measures	Protocols for data sharing	Data standards to ensure seamless interoperability	Importance of data formats, APIs and protocols	How banks build trust in data sharing	Transparency initiatives and mechanisms for fair data practices	Compliance with regulatory requirements	Challenges and strategies	Existence of governance frameworks and guidelines	Ongoing adaptation of the frameworks	Question of data ownership and rights in the ecosystem	Cooperative approaches to resolving potential disputes
Banks	Expert 1 (SOD)	4	5	3	2	1	3	3	1	1	2	1	2	2	2
	Expert 2 (LPIM)	0	4	0	0	1	0	4	0	1	7	2	0	1	0
	Expert 3 (SPM + EBO)	7	4	2	3	0	7	3	3	5	10	1	3	2	4
IT Providers	Expert 4 (SMDB)	5	0	0	4	2	4	6	1	2	1	1	0	1	2
	Expert 5 (TLSD)	1	1	0	4	7	5	8	0	1	9	1	0	1	0
	Expert 6 (F + CEO)	6	3	4	3	3	10	0	6	3	5	5	1	1	0
Regulators	Expert 7 (SPM + CL)	0	2	1	2	2	1	4	0	1	2	1	1	1	0
	Expert 8 (DDPO)	1	3	2	1	1	0	1	0	2	5	4	1	0	2
	Expert 9 (SC)	4	2	2	4	0	2	3	3	3	5	4	0	6	4
	Total	28	24	14	23	17	32	32	14	19	46	20	8	15	14

Conclusions

According to the first research question, most experts say banks are willing to cooperate as participants in the ecosystem. However, implementing a partner ecosystem is challenging and complex; experts are urgently needed. With the addition of partners, banks can now cover further customer needs and create added value. By making customer profiles based on customer interests, categorizing purchases and transactions using AI, and evaluating the data prospectively through individual and targeted personalization of services, banks can create added value outside of their traditional banking business (e.g., through loyalty programs). On the other hand, banks are also being driven to act and think in ecosystems by the changing platform ecosystem world as a new competitive situation by new competitors such as (fin-)tech companies. In addition, banks need significantly more technical and financial resources for implementation, and manual and rule-based processes still predominate. Data protection is again seen as an implementation and risk factor.

For treating the second research question, bank experts identified several risks when exchanging data in the ecosystem, such as incorrect conclusions being drawn from data, an increased reputational risk with third-party companies, and, if applicable, the risk of sanctions in the event of data protection violations in the ecosystem, unauthorized data use beyond the intended purpose and, finally, the loss of customer trust and termination by the customer. To mitigate these risks, when initiating a potential partnership, the choice should be made in favor of partners with banking experience and high performance, a joint, modern, or up-to-date software that technically implements current law, a precise definition, and procedure for the use of data as well as the roles of each partner in the ecosystem and the early and regular involvement of internal audit and advisory bodies as well as the implementation of monitoring and control systems.

For banks to collaborate with other participants in the ecosystem, this requires jointly developed data governance frameworks (third research question). The definition of a shared, centrally used system, which can ensure more consistent data storage and management and IT security, a uniform and shared understanding of quality and interpretation of data, and shared control instances are essential. Challenges include possible dependencies on the IT provider or orchestrator, uncontrolled data outflow or loss of data control, finding consensus on the use of standard interfaces, as banks often still use heterogeneous interfaces, unequal mindset or lack of know-how, slow implementation by banks and agreement on who gets access rights. To build trust in the ecosystem, banks should, above all, communicate openly, honestly, and clearly with customers regarding the use and purpose of data. Data sovereignty must remain the responsibility of the customer.

The experts reflect a heterogeneous picture regarding governance frameworks and guidelines for data sharing. Either no frameworks exist, some exist but cannot be mentioned, or few exist. Furthermore, a central, neutral arbitration body is desired to intervene and resolve a dispute. There is still room for improvement here for both banks and other participants in the ecosystem. Measures for action can include the establishment of an expert committee before entering into a multilateral business relationship where each participant involves experts. These can define the overarching shared goal and which customer needs and services will be served before the contract is concluded (holistic approach). Once the big picture has been derived and the business strategy has been jointly defined, IT due diligence with IT alignment can translate the business strategy to the data strategy of an individual participant and as a participant in a joint ecosystem construct for feasibility. For the translation of the business strategy into the data strategy to succeed, the joint development of a data governance framework for the shared use of data in the ecosystem must be ensured at this point at the latest. Here, the use of data and its definition and interpretation of use, data exchange relationships and the centrally used IT architecture required for this, and the distribution of roles, etc., can be worked out at a detailed level to be able to deliver added value to customers as an ecosystem network.

A central, neutral arbitration body should be installed once a functioning data exchange has been established in the ecosystem. To maintain neutrality, avoid potential conflicts of interest, and avoid taking sides, this body must be someone who is not a participant in the ecosystem.

Based on recommendations and use cases from experts, the outlook for possible future developments in data utilization strategies within platform ecosystems is that the experts see the centralized or holistic use of customer data with the help of intelligent data and a significant expansion in the use of AI use cases as critical success factors. It is worth looking at overseas trends in the USA and Asia. At the same time, the experts point out that there are still too many doubters in the banking environment who are afraid of data usage and complexity. In addition, the level of regulation in Europe and Germany remains high and is often a blocker to the progress

of further projects and innovations. Possible improvements in data governance include synergy effects and better cooperation between partners to increase efficiency. Finally, framework agreements should be more transparent and tangible for employees and customers.

References

Abraham, Rene, Schneider, Johannes, and vom Brocke, Jan. 2019. "Data governance: A conceptual framework, structured review, and research agenda." *International Journal of Information Management* 49: 424–438. doi: https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

Anjum, Rubi, Anwar, Ammar Ibne, Khan, Abdul Aziz and Mazhar, Syeda Ayeman. 2021. "Methods of data collection: A fundamental tool of research." *Journal of Integrated Community Health* (ISSN 2319-9113) 10(1): 6-10.

Ballon, Pieter, D'Hauwers, Ruben and Walravens, Nils. 2022. "Data Ecosystem Business Models: Value and control in Data Ecosystems." *Journal of Business Models* 10(2): 1-30.

Bellos, Ioannis and Kavadias, Stylianos. 2021. "Service design for a holistic customer experience: A process perspective." *Management Science* 67(3): 1718-1736.

Bonvino, Claudio and Giorgino, Marco. 2024. "A valorization framework to strategically manage data for creating competitive value." *International Journal of Production Economics* 109152. doi: https://doi.org/10.1016/j.ijpe.2024.109152.

Boso, Nathaniel, Hultman, Magnus, Leonidou, Constantinos N. and Olabode, Oluwaseun E. 2022. "Extensive data analytics capability and market performance: The roles of disruptive business models and competitive intensity." *Journal of Business Research* 139: 1218–1230.

Brodsky, Laura and Oakes, Liz. 2017. *Data sharing and open banking*. McKinsey & Company, 1105.

Cao, Junming, Choo, Kenny Tsu Wei, Gao, Jie, Lee, Roy Ka-Wei and Perrault, Simon. 2023. *Feasibility, Opportunities, and Challenges of Utilizing AI for Collaborative Qualitative Analysis*. arXiv preprint arXiv:2304.05560.

Choi, Hyoung-Yong and Park, Junyoung. 2022. Do data-driven CSR initiatives improve CSR performance? The importance of extensive data analytics capability. Technological Forecasting and Social Change, 182, Article 121802.

Coche, Eugénie, Dekker, Martijn and Kolk, Ans. 2024. "Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector." *Internet Policy Review*, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 13, Iss. 1, pp. 1-32, doi: https://doi.org/10.14763/2024.1.1738.

Creswell, John W. 2009. "Editorial: Mapping the Field of Mixed Methods Research." *Journal of Mixed Methods Research* 3 (2): 95–108. doi: https://doi.org/10.1177/1558689808330883.

Cummins, Mark, Lynn, Theo and Rosati, Pierangelo. 2020. "Exploring Open Banking and Banking-as-a-Platform: Opportunities and Risks for Emerging Markets." Edited by Darek Klonowski, *Entrepreneurial Finance in Emerging Markets*. Cham: Palgrave Macmillan. doi: https://doi.org/10.1007/978-3-030-46220-8_20.

European Union. 2015. Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector, OJ L 318, 2015b, p. 1–16.

Fader, Peter. 2020. Customer centricity: Focus on the right customers for strategic advantage. Philadelphia: University of Pennsylvania Press.

Friese, Susanne. 2016. "Qualitative data analysis software: The state of the art." *Kwalon*, 21(1).

Giebe, Carsten. 2022. *Big Data Analytics and the Discovery of the Hidden Data Treasure from Savings Banks in Germany*. Handbook of Research on Foundations and Applications of Intelligent Business Analytics, 350-373. IGI Global.

Gray, Joanne E., Hutchinson, Jonathan and Stilinovic, Milica. 2024. "Data sovereignty: The next frontier for internet policy?" *Policy Internet* 16: 6-11. doi: https://doi.org/10.1002/poi3.386.

Grossman, Robert L. 2018. "A framework for evaluating the analytic maturity of an organization." *International Journal of Information Management* 38(1): 45-51.

Hopf, Christel. 2004. *Qualitative interviews: An overview. A companion to qualitative research*, edited by Uwe Flick, Ernst von Kardorff and Ines Steinke, *203*(8), 100093. Reinbek: Rowohlt Ttaschenbuch Verlag GmbH.

Karkošková, Soňa. 2023. "Data Governance Model To Enhance Data Quality In Financial Institutions." *Information Systems Management* 40(1): 90-110. doi: 10.1080/10580530.2022.2042628.

Kruse, Jan. 2014. Qualitative Interviewforschung. Ein integrativer Ansatz. Weinheim, Basel: Beltz Juventa.

Kuckartz, Udo. 2012. Qualitative inhaltsanalyse: methoden, praxis, computerunterstützung. Weinheim, Basel: Beltz Juventa.

Langer, Arthur and Mukherjee, Arka. 2023. Data Strategy for Exponential Growth. In Developing a Path to Data Dominance: Strategies for Digital Data-Centric Enterprises. Cham: Springer International Publishing.

Legner, Christine and Pentek, Tobias. 2020. Datenstragegien als Grundlage der Transformation zum datengetrieb- enen Unternehmen. Troisdorf: SIGS DATACOM GmbH.

Lipton, Alex, Pentland, Alex and Shrier, David. 2016. *Digital banking manifesto: the end of banks?* Cambridge: Massachusetts Institute of Technology.

Mayring, Philipp. 2004. *Qualitative content analysis. A companion to qualitative research*, edited by Uwe Flick, Ernst von Kardorff and Ines Steinke *1*(2): 159-176. Reinbek: Rowohlt Ttaschenbuch Verlag GmbH.

Omarini, Anna. 2023. *Shifting Paradigms in Banking: How New Service Concepts and Formats Enhance the Value of Financial Services*, edited by Maher Kooli, Elaheh Nikbakht and Thomas Walker, The Fintech Disruption. Palgrave Studies in Financial Services Technology. Cham: Palgrave Macmillan. doi: https://doi.org/10.1007/978-3-031-23069-1_4.

Rufo, Raúl Cruces. 2023. *Data Governance in the Banking Sector*, edited by Ismael Caballero and Mario Piattini, 165-178. Cham: Springer. doi: https://doi.org/10.1007/978-3-031-43773-1_8.

Wendlinger, Benedikt. 2022. "The challenge of FinTech from the perspective of german incumbent banks: an exploratory study investigating industry trends and considering the future of banking." Doctoral dissertation, Universidade Católica Portuguesa.