European Business Organization Law Review
https://doi.org/10.1007/s40804-022-00252-4

ARTICLE

Cloud Outsourcing in the Financial Sector: An Assessment of Internal Governance Strategies on a Cloud Transaction Between a Bank and a Leading Cloud Service Provider

Jamelia M. Anderson-Princen[1]

Accepted: 2 May 2022

Abstract
Cloud applications are becoming central and critical to the delivery of financial services. Despite their significance, banks face increased exposure to transaction risks related to the use of cloud services and internal and external pressures to improve their risk management practices. In this study, we use a unique data set from a bank's cloud register to examine the effectiveness of internal governance on an ongoing cloud outsourcing transaction between a bank and cloud service provider. We employ structural equation modeling and a simple linear regression to test for transaction misalignment and causes of governance inefficiencies. We find that a strong degree of misalignment is largely due to poor design of internal controls and a weak control system that does not provide acceptable indications of residual risk likelihood. The findings indicate that cloud risks are driven not only by agency costs, but also by firm-specific risks which contribute to a number of transaction uncertainties and governance misalignment.

Keywords Cloud outsourcing · Transaction risks · Cloud service provider (CSP) · Financial institutions · Internal governance efficiencies · Transaction misalignment · SEM analysis

1 Introduction

Third-party cloud applications have emerged in recent years as central and critical to the delivery of financial services. While cost reduction and scaling up on efficiencies (i.e., 'make or buy decision') are major reasons for this shift, financial institutions have become increasingly exposed to a spectrum of cloud transaction risks (e.g., legal risks, technology risks and firm risks). This highlights the importance of

✉ Jamelia M. Anderson-Princen
j.m.anderson@uvt.nl

[1] PhD Candidate, Tilburg Law School, Department of Private, Business and Labour Law (PBLL), Tilburg University, Tilburg, The Netherlands

Published online: 20 June 2022

devising an efficient control framework. An efficient internal governance structure is one which innately matches or mirrors the risks of the transaction to a cost-economizing effect.[1] However, firms are not all equally effective in designing appropriate governance mechanisms that can create an effective risk management and oversight framework. For cloud arrangements, some of these challenges originate from the emergence of cross-border risks associated with differences in legal regimes governing data privacy and security. More specifically, the fragmented nature of data privacy regulation and the absence of well-defined policies can, at times, complicate compliance and risk management for financial institutions which operate in multiple jurisdictions. Therefore, it is necessary for these institutions to have a sound understanding of local and foreign laws and identify whether foreign laws of third-party service providers can present additional risks.

In light of this, the main focus of this article is to examine internal governance approaches applied by a bank in a material cloud services agreement. A unique set of risk and governance data from a bank's cloud risk register is applied to a structural modelling equation (SEM) and simple linear regression to test for transaction misalignment and causes of governance inefficiencies. The objective of this study is to contribute to the development of policies on cloud regulation and sound internal governance practices. This paper reconciles and extends two strands of literature, namely transaction cost theory and finance, to illustrate that causes of misalignments can also be found by looking further into components of internal control.

Through the means of a cloud outsourcing case study,[2] the study sets out to answer three main questions: (1) What is the degree of transaction misalignment in the cloud outsourcing transaction?; (2) To what extent is a bank's internal control framework useful in predicting the likelihood of residual risk?; (3) Are there potential issues/flaws in the internal control framework which contribute to transaction misalignment? Overall, the results provide conclusive evidence supporting a strong degree of misalignment (.47), largely due to the poor design of internal controls. The empirical approach is validated by good model fit indices, which confirms that including indicators of residual risk provides an improved measure of transaction risks[3] and governance efficiencies. The model results confirm that most misalignment is caused largely by high degrees of legal and technological uncertainties on data privacy regulation and technology processes. Consequently, this translated into poor design of internal controls and a weak control system with unacceptable ($R^2$50) indications of residual risk likelihood.

The paper contributes to cloud outsourcing literature in a number of ways. First, our findings shed light on the degree of misalignment between specific risk types and related control features. In this regard, we believe that our findings make an

[1] Williamson (1985).

[2] The institution studied is a development bank which finances private and economic development projects in Latin America, Europe and the Caribbean region. The institution has requested to remain anonymous given the sensitivity of the financial data provided. The author thanks the risk managers for providing direct access to raw cloud risk and governance data from the cloud risk registry. The data was analyzed and collected in 2019. For more, see Table 1.

[3] Anderson et al. (2017).

important contribution to the literature on the role of monitoring and governance in shaping cloud outsourcing policies. Secondly, our evidence on the content of these risk categories contributes to recent cloud outsourcing literature which has tended to apply more indirect measures to capture cloud risks. Finally, this study also contributes to the body of literature examining the development of residual risk models, by using a linear regression model to analyze data from a financial institution.

The article is divided into six main sections. Section 1 discusses the institutional background to the case and the regulation which governs the transaction. Section 2 discusses the literature review and hypothesis development. Section 3 discusses the SEM model construction and data in the study. Section 4 provides a practical and theoretical discussion on inherent risk exposures in the cloud transaction. Section 5 then presents the results on the SEM model which confirms the tests for misalignment. Section 6 presents the results of the linear regression model which confirms existing irregularities in the Bank's internal control framework which relate to the misalignment.

2 Institutional Profile

A topic of much interest concerns the connection between risk and governance data on existing cloud outsourcing transactions. This case study focuses on a five-year SaaS cloud outsourcing arrangement between a bank and a leading cloud service provider (CSP) in order to draw inferences about how banks manage the different sources of risk that affect data management and other activities. Table 1 below outlines the institutional profile of the financial institution and CSP.

The Bank in this study adheres to European regulatory standards on cloud outsourcing. The upcoming section discusses the development of cloud regulation in the European Union (EU) and UK, which are major ICT jurisdictions and locations for cloud computing. The section explains how the fragmented nature of data privacy regulation and the absence of well-defined policies contribute to cross-border risks, which complicates compliance and risk management for financial institutions.

2.1 Cloud Outsourcing in the European Union and the United Kingdom

The use of cloud technologies can result in a spectrum of diverse risks which threaten data security. For instance, the prevalence of ICT security risks which stem from inadequate or failed internal processes or external events can ultimately impact

Table 1 Case overview

Firm type	Market cap	Interviewee	Location
Bank A	€2.1b	Operational risk manager	Europe, Latin America, Caribbean
CSP	€110b	Head of IT	
		Legal	

This table provides an overview of the firm type, market capitalization, location and data collection approach adopted in this study

a firm's systems and data security.[4] In fact, many jurisdictions have introduced a legal and regulatory framework for governing cloud use in order to prevent unlawful data processing and data access,[5] security risks, technological risks and concentration risks. The EU in particular has had a major influence on the global regulatory landscape[6] and the regulation of cloud arrangements. This has led to a number of jurisdictions (e.g., the UK, Germany, France, Italy, Ireland) adopting privacy and internet laws based on the legal notions and patterns of European legislation.[7] The regulation governing cloud computing is largely unharmonized, fragmented and governed by a set of different regulations and policies.[8] Notwithstanding this, some of the most influential guidelines issued by the European Banking Authority (EBA) are the Final Guidelines on Outsourcing Arrangements (EBA/GL/2019/02),[9] the ICT Guidelines and Internal Governance Guidelines (EBA/GL/2019/04, EBA/GL/2017/11).[10] Indeed, the UK has implemented most of these guidelines[11] to establish how institutions should manage third-party and ICT risks. More specifically, the development of their regulatory initiatives has also been influenced by events such as Brexit, and by the need to further specify and define the risk requirements set by the EBA.

[4] See EBA (European Banking Authority) Guidelines on ICT and Security Risk Management (EBA/GL/2019/04) of 29 November 2019, laying down specific guidelines on the mitigation and management of ICT and security risks for credit institutions, investment firms and payment service providers.

[5] Krebs (2012).

[6] Kontargyris (2018), p 58.

[7] For a more in-depth analysis of European influences on international data privacy laws, see Kontargyris (2018) and Greenleaf (2012).

[8] For more information on other relevant pieces of legislation affecting cloud services, see the EU NIS Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, the Markets in Financial Instruments Directive-MiFID (Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance) and the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)).

[9] Overall, the development of EU cloud policies has been slow but forthcoming. This has led to the introduction of the EBA Guidelines on Outsourcing Arrangements EBA/GL/2019/02, of 25 February 2019, repealing the CEBS (Committee of European Banking Supervisors) Guidelines on Outsourcing of 14 December 2006, and the EBA Recommendations on outsourcing to cloud service providers of 20 December 2017 (EBA/REC/2017/03), with effect from 30 September 2019.

[10] For more specific guidelines on ICT and internal governance strategies, see EBA ICT Guidelines, EBA/GL/2019/04, Guideline 3.2, and Internal Governance Guidelines, EBA/GL/2017/11, Titles III & V.

[11] For more details, see final supervisory statement SS2/21 (Bank of England, Prudential Regulation Authority (2021) which clarifies how the Prudential Regulatory Authority (PRA) expects banks to approach the EBA Outsourcing Arrangements (EBA/GL/2019/02) and EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04). See specifically ibid., SS2/21, s.2.17, chapters 7 and 10, expanding and clarifying expectations regarding data security, business continuity and exit plans. See also Policy Statement PS7/21 (Bank of England, Prudential Regulation Authority (2021b) for feedback responses on outsourcing and third party risk management.

In particular, a key focus of the Prudential Regulatory Authority (PRA) is to assess third-party risks according to their level of dependencies and to establish whether such arrangements are material.[12] As a result, some of the main post-Brexit amendments include the introduction of additional criteria to evaluate whether outsourced functions or activities automatically[13] qualify as a material function.[14] The significance of these amendments is that they strengthen and streamline the risk assessment process by reducing uncertainties on whether a risk is material, and in doing so, establish whether enhanced governance measures should be applied. There are a few other amendments that have been introduced in areas such as the scope of outsourcing, data security, sub-outsourcing, business continuity and exit plans.[15] However, the requirements do not appear to diverge significantly from the EBA Guidelines on Outsourcing Arrangements but only provide greater regulatory certainty in key, complex areas.[16]

In practice, the impact of the EU General Data Protection Regulation (GDPR) has been significant for cloud service providers and financial institutions outsourcing cloud services. Over the last few years, the GDPR has expanded its scope to limit significant privacy threats associated with cloud computing and transboundary data transfers by enforcing compliance requirements on EU-established organizations and on non-EU controllers and processors.[17] The global response to rising privacy concerns has led to the implementation of inward-looking policies such as data localization mandates and international privacy acts which either allow or restrict data access by foreign authorities. In the UK, regulators have opted for the latter by enacting the US Cloud Act (2019)[18] into their Data Protection Act (2018).[19] The outcome of the Act is that it removes any conflicts of laws (UK/US Cloud Act, Art. 3) which may obstruct enforcement actions or prevent CSPs and internet service

[12] See SS2/21, Bank of England, Prudential Regulation Authority (2021a), specifically chapter 5.12, para. 3.12, with reference to the assessment of material risks. In accordance with these requirements, institutions are required to assess the potential impact of outsourcing or third party arrangements on their safety and soundness, including their operational resilience, their ability to comply with legal and regulatory obligations, and the risk that their ability to meet these obligations could be compromised if the arrangement is not subject to appropriate controls and oversight.

[13] Ibid.

[14] See specifically EBA/GL/2019/02, p. 13, where the EBA has replaced the term 'critical or important' with the term 'material', according to the definitions provided under the MiFID Directive (Directive 2014/65/EU) and the Payment Services Directive (PSD2) (Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC).

[15] See SS2/21, Bank of England, Prudential Regulation Authority (2021a).

[16] Bank of England, Prudential Regulatory Authority (2021b), specifically PS7/21, paras. 2.9 and 2.16.

[17] For specific details on how GDPR compliance requirements impact financial institutions, see Matheson (2017).

[18] UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019], Washington, 3 October 2019.

[19] The United Kingdom Data Protection Act (2018).

providers from responding directly and freely to requests for data stored in the US or abroad.[20]

Alternatively, some regulators, such as those in Germany (and France), have instead opted for stricter data regulation practices such as data localization mandates, for example, the *Bundescloud*, a German federal cloud initiative. In particular, this mandate only allows data storage and processing of federal data in private clouds and within federal-owned data centers by approved cloud providers in Germany.[21] However, in light of this initiative and the current EU regulatory focus (e.g., Gaia-X project),[22] it is likely that similar proposals will soon follow in the private sector. However, the implementation of strict data localization mandates can generate weak points in security systems due to data concentration. In contrast, encouraging institutions to take advantage of storing data in multiple locations, while managing 'legal risks stemming from conflicting or less developed relevant legal or regulatory requirements'[23] can result in significant risk exposures. This is largely because the high degree of variance on data transfers creates regulatory arbitrage,[24] adds to regulatory complexity and creates less clarity on rules[25] required to manage cloud risks. Jansen and Grance[26] also note that the key challenge with transborder data flows is that firms may be uncertain as to

> whether the laws in the jurisdiction where the data was collected permit the flow, whether those laws continue to apply to the data post transfer, and whether the laws at the destination present additional risks or benefits.

Ultimately, this implies that UK and EU institutions which are subject to international privacy acts or less stringent data localization mandates can face greater privacy and security risk exposures. As a consequence, not only may this increase transaction costs but it may also be burdensome and difficult for institutions to

[20] According to the US Department of Justice (2019), p. 6, a number of countries require cloud service providers to disclose data in certain instances. For a discussion on similar agreements enacted by other governments (e.g., Australia, Belgium, Norway, Denmark, Portugal and Spain) see ibid. See also Maxwell and Wolf (2012), as cited in US Department of Justice (2019).

[21] See the Federal Cloud Policy, Resolution 2015/5 of the Federal Government's IT Council. https://www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/Beschluesse/Tabelleninhalte/beschluss_2015_05.html (accessed 24 April 2022).

[22] The Gaia-X project is a German-led EU initiative aimed at promoting fair and open use of sovereign data based on EU values and regulations. Financial institutions and EU stakeholders are working on setting common policy rules to ensure transparent use of data and its protection at European level. These efforts are geared towards addressing key concerns which hinder the adoption of cloud technology in the financial sector, such as lack of trust in cloud service providers and the concern over the use of international cloud platforms operating under extra-territorial laws. For more, see Gaia-X European Association for Data and Cloud AISBL, Project Gaia-X, specifically the Federal Ministry for Economic Affairs and Energy (BMWi) and Federal Ministry of Education and Research (2019).

[23] See Bank of England, Prudential Regulatory Authority (2021a), specifically para. 7.8.

[24] See EBA Guidelines on Outsourcing Arrangements, EBA/GL/2019/02, of 25 February 2019, para. 18.

[25] For details on how data sovereignty and GDPR requirements impact financial institutions and investment firms when storing and transferring client data within the European Union, see Royal Bank of Canada (RBC) (2017) and Matheson (2017).

[26] Jansen and Grance (2011), p 16.

leverage global risk management and compliance programs.[27] Therefore, it is imperative for institutions to have a good understanding of local and foreign laws, especially when operating in multiple jurisdictions. Against this backdrop, this may be a daunting task, due to the absence of cohesive, consistent, harmonized regulatory frameworks,[28] which is caused by divergent jurisdictional tendencies and the use of omnibus laws.[29] The next section, discusses how these challenges and the absence of well-defined policies complicate compliance for financial institutions.

2.2 Cross-border Risks: Uncertainties in Cloud Risk Management

In light of the discussion above, the absence of a consistent regulatory framework can hinder sound institutional compliance. This is largely because there is currently no common set of comprehensive and well-defined cloud risk methodologies. Nevertheless, EU and UK regulators have made some efforts to clarify expectations about risk management. For instance, in 2019, the PRA introduced a policy proposal which recommends the use of metrics (e.g., extent of business disruption, and/or the volume or value of impact) to evaluate the tolerance impact of certain business disruptions arising from failed systems or process failures.[30] In contrast, although EU regulators have yet to issue a comprehensive risk methodology to measure cloud risks, a complex privacy risk methodology was introduced by the European Union Agency for Cybersecurity (ENISA)[31] and some EU data protection regulators (Greece and Germany) in 2013. While there is no indication of whether this risk methodology is applied by financial institutions, data protection authorities have already identified noticeable differences amongst the privacy risk assessment of supervisors, CSPs and controllers.[32] Arguably, these inconsistencies could be driven by uncertainties in compliance or lack of harmonization of existing practices. In fact, both factors contributed to uncertainties for the institution in this study, which ultimately led to challenges in devising a suitable risk framework. Table 2 below outlines the risk parameters used to evaluate the transaction.

A pivotal question is whether the existing regulatory guidelines provide sufficient criteria or guidance required to manage cloud risks. These concerns have been highlighted by industry experts during the EBA consultations on the implementation of the ICT security risk guidelines and the use of contracts and service level

[27] Financial Stability Board (2019), p 14.

[28] See Smith (2010).

[29] Kontargyris (2018).

[30] For more, see the Bank of England, Prudential Regulatory Authority (2019b). See also Financial Conduct Authority (2019), p 6, para. 6.4. Consultation Paper CP19/32 is a joint effort of the Bank of England, PRA and the FCA to clarify the requirements for impact tolerance assessments, and harmonizing risk concepts with international approaches. For more details on these efforts, see also BCBS (2020).

[31] In line with their methodology, the severity of data privacy security incidents is evaluated according to the following criteria: (1) data processing content, (2) ease of identification, and (3) circumstances of data breach (SE = DPC x EI + CB). For more specific insight into their risk methodology, see ENISA (2013) and CNIL (2015) for the privacy methodology of the French Data Protection Authority.

[32] For more insight, see Rozendaal (2019).

Table 2 Cloud risk parameters and governance strategy

Thresholds (severity)	Risk frequency	Financial impact USD (in millions)	Non-financial impact	Management actions
High risk	> 2 years	> 10	Reputational impact	Yes
Medium risk	< 2–5 years	> 500,000–< 3	Reputational impact	Yes
Low risk	< 5 years	> 50,000 < 100,000	No impact	No

agreements to ensure that institutions apply appropriate cyber and security measures.[33] In response to these requirements, participants requested further guidance on key risk and performance indicators (KPIs) to ensure some degree of consistency among financial institutions, particularly in light of conflicting laws which impose diverse requirements.[34] These issues have been noted by UK authorities, in particular, which addressed some of these concerns by introducing common criteria to improve the consistency of firms' materiality assessments, and tolerance impacts.[35] Inevitably, these concerns highlight the need for greater specification on the policies intended to address ICT and other cloud risks.

As will be discussed below, a number of transaction uncertainties in the cloud arrangement are caused by a failure to understand the inherent nature of transaction risks and the regulatory requirements associated. Most of these risks relate largely to poor design of data governance strategies and data privacy measures. Consequently, these design strategies and measures often contribute to greater transaction risk exposures and a larger degree of misalignment. Thus, regulators may be encouraged to consider introducing soft law mechanisms and usefully combine them with comprehensive, flexible privacy and technology-enhancing policies and practices.[36] The next section will explore the conceptual framework and conditions required to address these challenges.

3 Theoretical Perspectives on Cloud Risks and Governance

As concluded above, an important challenge for financial institutions is devising suitable governance strategies in the face of divergent legal systems. Therefore, the focus of this section is to lay the theoretical framework required to empirically test

[33] See EBA Guidelines on ICT and Security Risk Management, EBA/GL/2019/04, specifically the feedback on public consultations, p 54, para. 8.

[34] Subsequently, this request was dismissed by the European Banking Authority, which was of the opinion that additional guidelines would lead to too detailed requirements.

[35] For more specific details, see supervisory and policy statements from the Bank of England, Prudential Regulation Authority, for additional guidelines and clarification on third party risk management processes (specifically Bank of England (2021a), pp 6–8; Bank of England (2021b), and Bank of England (2021c)). See also consultation papers from the Bank of England, Prudential Regulatory Authority, which outline governance requirements for key stakeholders (specifically Bank of England (2019a) and Bank of England (2019b)). The PRA expects UK banks to comply with these policies by March 2022.

[36] Kulesza (2014), p 304.

for the degree and causes of governance inefficiencies in the cloud transaction. This section first discusses some important theoretical assumptions of the transaction cost theory and concludes with the main research hypotheses to be tested.

Transaction cost economics (TCE) is widely used by authors in studies on IT outsourcing. The relevance of the theory lies in its ability to theoretically recognize sources of transaction hazards, anticipate internal organizational changes and empirically test for governance efficiencies in the risk mitigation process. To develop our research hypothesis, the study applies the concept of 'transaction misalignment', which is one of the most basic propositions of transaction cost theory. The hypothesis claims that transactions (which differ in their attributes) are aligned with related governance structures (which differ in their cost and competence) so as to result in a transaction cost-economizing effect.[37] Hence, organizations that choose the wrong governance structure will incur higher transaction costs for a given level of output than organizations that choose more efficient governance structures.[38]

In the most basic context, transaction misalignment is considered as a simple 'matching principle', whereby transaction risks are matched to firm controls to assess the extent to which transaction risks are mitigated. The assumption is that more efficient governance structures are those in which there is a close alignment between transaction risks and controls. The degree of alignment is assessed through regression analysis, which is applied to empirically test the association between the 'attributes' of a transaction which serve as a measure of transaction risk and the use of internal controls which model the governance structure.[39] Notably, a dominant cause of transaction misalignment is inadequacies with internal controls. According to Anderson and Dekker,[40] misalignments are often a consequence of inappropriate use of controls or a failure to design adequate contracts in response to transaction characteristics. In this study, we propose that inappropriate governance responses are likely to be caused by uncertainties about regulations governing cloud use.

Generally, the process of measuring misalignment is not straightforward, as it is often difficult to estimate transaction risks due to the lack of consensus on the factors which define the risks of a transaction.[41] Notwithstanding this, the three main dimensions or 'attributes' commonly applied to measure transaction risks are: (1) asset specificity, (2) transaction uncertainty, and (3) transaction frequency.[42] According to transaction cost theory, these dimensions are critical in explaining the nature of risks which firms face; however, within the field of cloud outsourcing, only a few studies have applied the framework to measure cloud transaction risks.

According to these studies, asset specificity is defined as the degree of investment in the asset required to make it work, or the costs of reallocating it for another use such as investment in cloud applications, IT training, meta services costs, new

[37] Williamson (1998).

[38] Sampson (2004).

[39] Williamson (1985, 1991).

[40] Anderson and Dekker (2005).

[41] Williamson (1979), p 234.

[42] Ibid. See also Williamson (1985), p 37.

vendor transition costs, and cloud customization risks.[43] Transaction uncertainty relates to primary and behavioral uncertainties which arise from legal risk, technological risk and vendor opportunism.[44] In contrast, the dimension transaction frequency or 'cloud transaction frequency' refers to the frequency of the adoption of cloud services and how often a service is called.[45]

The transaction attributes defined by the TCE framework are also important in determining appropriate risk responses and the governance structures firms adopt. For outsourcing, the management control structure of outsourcing arrangements is based on a hybrid form of governance.[46] However, Williamson[47] states that the main features which characterize any given governance structure are administrative controls, incentive intensity and contract law. For cloud outsourcing, the governance structure is likely to be defined by administrative controls designed to protect data, contract law defined by cloud contracts, and data protection law which regulates data use.

Therefore, from a general perspective, this implies that the efficiency of a governance structure relates to the way in which protection is established to design and organize appropriate governance structures.[48] Therefore, misalignment can be estimated if the risks of a particular transaction are invariant to the cost of control.[49] With this perspective, the study embarks on a more direct strategy for measuring misalignment by regressing all unique inherent transaction risks in a single cloud transaction with related governance (e.g., contractual and institutional) controls. As there is very little theory motivating cloud computing, the study builds on the work of Williamson[50] by keeping in line with the basic propositions of transaction cost theory.

Hypothesis 1 The first hypothesis suggests that greater misalignments between inherent cloud risks and internal controls are synonymous with greater inefficiencies in cloud governance.

Alongside the empirical approach, the study also arranges all inherent risks according to the TCE transaction risk framework to provide a descriptive analysis of the consequences associated with the misalignment. This approach supplements and enriches the empirical results of the study, while highlighting key governance issues

[43] Makhlouf (2020), Yigitbasioglu (2014), p 195, Trenz et al. (2013), p 4.

[44] More specifically, Yigitbasioglu (2014) concludes that primary uncertainties arise due to natural events, consumer preferences, technology and regulations, whereas behavioral uncertainties relate to opportunism which often results in incomplete contracts and lack of trust. According to Trenz et al. (2013) these uncertainties are manifested in the users' concerns about privacy, security and IT availability.

[45] Makhlouf (2020), p 9.

[46] Van der Meer-Kooistra and Vosselman (2000), p 11.

[47] Williamson (1991).

[48] Van Genugten (2008), p 35.

[49] Anderson et al. (2017), p 2165.

[50] Williamson (1979, 1981, 1985, 1991).

in the transaction. This approach differs to other studies which predominantly apply survey techniques to categorize risk and governance data before applying regression analysis to measure misalignment.[51] Therefore, the results of this test will confirm that misalignments in cloud transactions can be meaningfully tested using a unique set of risk and governance data. Figure 1 below conceptualizes how all cloud transaction risk data[52] and related governance controls are applied to test for misalignment.

3.1 Internal Control and Transaction Misalignment Hypothesis

Having concluded on the approach to measure governance inefficiencies, this section outlines the method which will be applied to evaluate whether complexities in regulation contribute to poor internal control design. This question is answered by paying particular attention to the design of the Bank's internal control framework. From a theoretical perspective, this step is also important as the TCE proposition is limited in establishing causes of misalignments and in determining whether the causes of misalignment are not mistakes or chance incidents.[53]

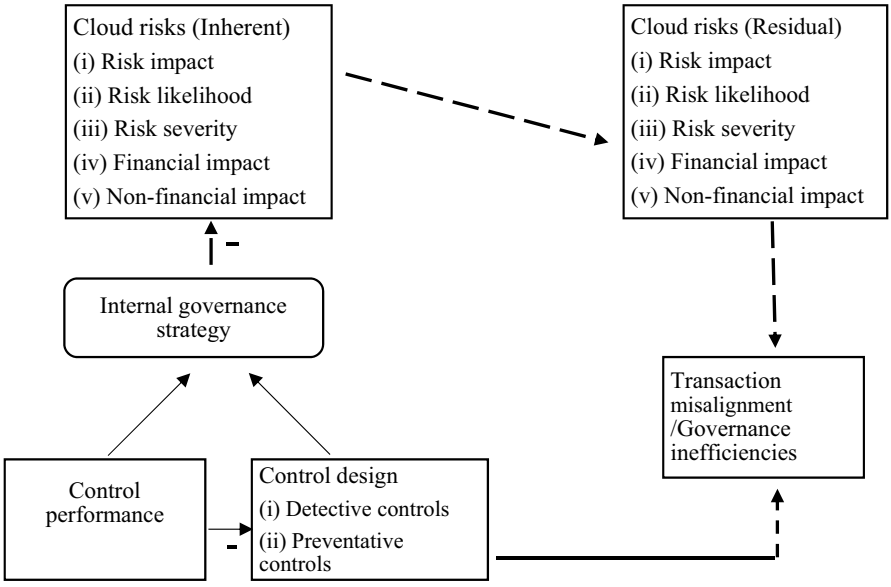

Fig. 1 Testing for transaction misalignment

[51] For details on these studies, see Anderson et al. (1988), Leiblein et al. (2002), Reuer and Ariño (2002), Argyres and Bigelow (2007).

[52] Figure 1 illustrates our approach to testing for misalignment along with all risk and governance data obtained from the cloud registry. All inherent cloud transaction risks are defined as the risks before controls are applied, whereas residual risks are risks which remain after controls are applied. Total risks are determined by the variables: risk likelihood, financial impact and non-financial impact. The governance structure or internal control strategy is determined by two variables: control design and control performance. The alignment between risks and controls determines the extent of transaction misalignment.

[53] Johansson (2015), p 675.

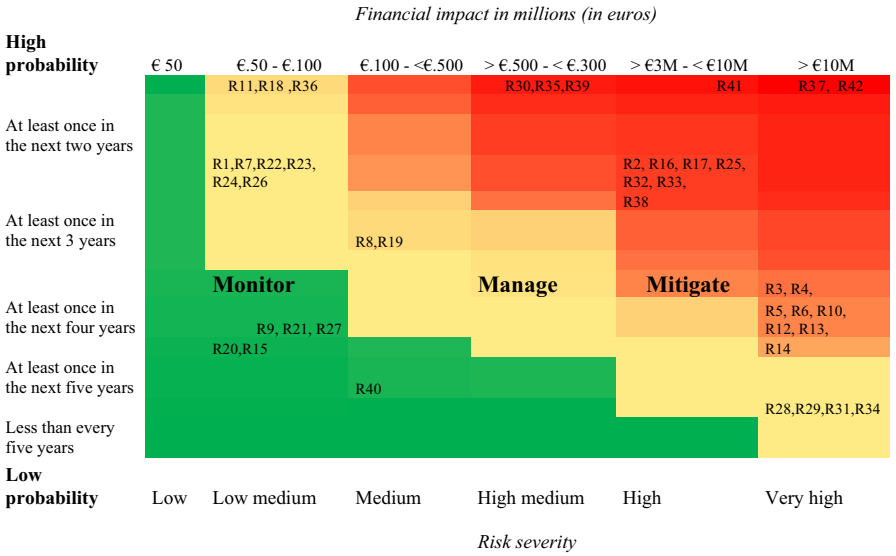

Fig. 2 Cloud risk assessment heat map (All risks are color coded to demonstrate the degrees of severity for each risk category. Dark grey (red) depicts medium/high risk levels which lead to major financial impacts and reputational losses. Grey (yellow) depicts medium/low risk levels, and light grey (green) depicts low risk with lower levels of financial and reputational impacts) (color figure online)

As internal control is explicitly tied to risk treatments, the study relies on some basic fundamentals of finance and internal control to infer whether any causes of misalignment relate to internal control issues. More specifically, the study examines the strength of the control framework in predicting residual risks and associations amongst risk and internal control components. The first investigation is imperative in assessing the reliability of cloud risk assessments in the identification of residual risk. The latter is focused on identifying whether irregularities exist in the control environment and the source of the irregularities (Fig. 2).

To begin with, there is very little evidence on how effective risk management approaches are applied in IT projects[54] and/or how they relate to misalignment. However, the control environment[55] is useful in assessing the effectiveness of an internal control system.[56] For instance, Kountur[57] developed a residual risk model using risk and control variables, and concluded that control systems with $R^2$52 provide unacceptable indications of residual risk, thus threatening risk planning. From

[54] Taylor et al. (2012).

[55] In this case study, the internal control environment is defined according to the COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control-Integrated Framework, COSO (2013, 1992) which describes the control environment as consisting of the following five components: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring activities.

[56] Mangasih et al. (2020).

[57] Kountur (2018).

a risk management perspective, estimating the occurrence of residual risk is critical, as it sets the stage for risk measurement, reduction, and risk tolerance.[58] Therefore, assessing whether the Bank's system can accurately estimate the risks which remain after internal control measures are applied helps to establish the strength of its control system and its true degree of institutional risk exposures.

Hypothesis 2 In line with these arguments, the study hypothesizes that control systems which have greater predictive strength (R^2) more accurately estimate the occurrence of residual risks and such control systems lead to more efficient governance outcomes. Hence, control systems with weak predictions (R^2) of residual risks are synonymous with weaker internal control systems.

The second part of the analysis is focused on examining correlations derived from the multiple regression model which provides a prediction for residual risk. The results derived from this analysis will be used to establish whether there are any internal control design issues in the institution's internal control framework. As studies have established that several interrelations exist in the control environment,[59] we propose that such interrelations can be used to assess the strength of any internal control framework. For instance, Kountur[60] found that the quality and appropriateness of risk treatments reduce the likelihood of residual risks, whereas Anderson et al.[61] found that negative correlations between control use and residual risks are consistent with controls reducing residual risk. On the other hand, Messier and Austen,[62] found that positive correlations between inherent risk and control risk reflect a weak control system, which increases transaction risk exposures.

Additionally, there are other factors in the control environment which directly influence internal control, such as management conduct and risk management expertise. For instance, Rae et al.[63] found that although a direct association exists between risk assessment and control activities, both risk and controls are subsequently associated with monitoring. According to Bruwer et al.,[64] empirical relationships exist between two of the elements of a sound internal control system, namely internal control activities and managerial conduct (e.g., industry-specific knowledge, etc.).

To date, only one known study has examined the relationship between governance misalignment and managerial capabilities. Handley[65] confirmed that the inferior process performance (e.g., technical expertise, and outsourcing knowledge) of internal control corresponds directly with transaction costs' discriminating alignment hypothesis via the relationship with governance misalignment. Altogether,

[58] Tolbert (2005), p 29.

[59] Rae et al. (2017).

[60] Kountur (2018), p. 58.

[61] Anderson et al. (2017), p 2173.

[62] Messier and Austen (2000), p 30.

[63] Rae et al. (2017).

[64] Bruwer et al. (2017), p 6.

[65] Handley (2017), p 151.

these findings suggest that elements of the Bank's control framework such as outsourcing knowledge, risk responses, and the appropriateness or quality of control are positively correlated but negatively associated with inherent risk and residual risk.

Hypothesis 3 In light of these arguments, the study hypothesizes that positive interrelations between elements of internal control (e.g., control design and control performance) reflect more efficient governance structures and are likely to reduce governance misalignments. On the other hand, negative correlations among elements of internal control are expected to reflect weaker governance structures and contribute directly to greater misalignments.

While the study does not test directly for the influence of managerial capabilities on internal control, it does reflect on major risk sources and control irregularities to formulate whether such factors contributed to any misalignment in the transaction. This is based on the expectation that examining cloud transactions from this perspective helps to extend core elements of theories on transaction cost, finance and internal control, which adds to results on potential internal governance issues. The next section discusses the data and empirical models employed in this study.

4 The Data

The risk registry provides data on 42 risk exposures and governance controls in the cloud arrangement. All cloud risk assessments are prepared in accordance with EU cloud regulation (see footnote 66) and represent original observations as maintained in the cloud risk registry. All risks and control indicators are assessed using a 7-point Likert scale to represent risk severity and control strength. In the SEM model, the variable 'cloud transaction risks' serves as the independent variable and is measured by six indicator (endogenous) latent variables (x1 to x6).[66] These variables are: inherent impact, inherent risk likelihood, residual impact, residual risk likelihood, financial impact and non-financial impact. The variable 'governance strategies' is the dependent variable, defined by two indicator (exogenous) latent variables (y1 to y2),[67] namely control performance and control design. On the linear regression

[66] In accordance with the EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02, Title II), institutions are required to evaluate risk exposures arising from outsourcing arrangements (e.g., legal risks, reputational risks, disruption of revenue, data integrity, risks to institutional viability). In line with these requirements, the Bank in our case study evaluates the criticality of these risks according to their degree of financial and non-financial impacts. Here, financial impacts relate to monetary losses arising from cloud failures and non-financial impacts relate to reputational risks which can result in adverse changes such as brand erosion, stock market impact, or losses in material earnings of the institution. Total cloud risks are a product of risk likelihood and risk impact. The likelihood of risks and its severity is determined by the frequency of risk occurrence. Inherent risks are risks before controls are applied, residual risks are risks after controls are applied.

[67] Internal controls are assessed on the basis of control performance and control design. The control design element consists of the detective and preventative controls broadly defined by contractual agreements (e.g., cloud contracts, service level agreements (SLAs), contracts for cyber security insurance) and

model, inherent risk likelihood, control design and control effectiveness serve as the independent variables (x), while residual likelihood serves as the dependent variable (y).

4.1 The Models

4.1.1 The SEM Model and Linear Regression Model

The studies which test for transaction misalignment usually apply a variety of regression models such as Two Stage Least Squares, Probit Model, and/or Factor Analysis with Structural Equation Modelling.[68] Generally, the choice of empirical method varies as researchers also analyze the effect of external factors (e.g., influence of alliance governance, prior ties, performance risk, etc.) on transaction risk and how they relate to governance outcomes. In such cases, a series of tests is required to establish the validity of the hypothesized constructs. However, this study adopts a less complex approach to testing for misalignment, given the access to already existing data, the simplicity of hypothesized constructs, and the direct approach to testing for misalignment. Applying the SEM model to our existing data set allows us to analyze structural relationships in the risk and governance data, estimate latent (unobserved) variables in the data, determine measurement errors and model fit[69] and derive the residual from the regression, which provides the test for misalignment. As it relates to the linear regression model, the advantages of applying this model is that it supplements the results of the SEM by identifying irregularities in the control framework. These results are important as they will be used to establish reasons for the misalignment on the SEM model, which will serve as valuable evidence contributing to the further development of residual risk models.[70] The next section discusses the SEM construction.

4.1.2 SEM Construction

A common challenge with measuring misalignment is the issue of measurement errors. Although the study applies original risk and governance data from the cloud risk registry, no variable, whether directly or indirectly measured, provides an accurate estimate. This is especially the case for the data set in this study, as

Footnote 67 (Continued)

institutional measures (e.g., physical controls, IT controls, data privacy policies and other institutional procedures and processes). Detective controls reduce risk likelihood, and preventative controls reduce risk impact. Control performance relates to the strength of control measures applied in mitigating inherent risks.

[68] For more details on these studies, Silverman et al. (1997), Anderson et al. (1988), Leiblein et al. (2002), Reuer and Ariño (2002), Sampson (2004), Anderson and Dekker (2017), amongst others.

[69] Hox and Bechger (1999).

[70] To date, very few studies have contributed to the development of residual risk models, with the exception of Kountur (2018). This paper therefore builds on his work and contributes to the advancement of residual risk models by applying a similar model, but with two alternative independent variables, i.e., control performance (X1) and control design (X2).

risk and governance assessments are largely subjective and prone to error in estimation. Additionally, while the SEM model provides the true score (t) on measured data, Anderson et al.[71] confirm that the TCE regression model contains misspecification errors which can impede the results on misalignment. Notwithstanding this, they find that direct measures of residual risk correct for misspecification errors and confirm the presence of control misalignments.[72] As a result, to construct our SEM model, both inherent risk and residual risk variables are incorporated as indicators of the latent construct 'cloud transaction risk'.

As transaction characteristics relate (weakly) to residual risk and (primarily) to control design[73] we assume that residual risk measures can contribute to more accurate measures of inherent risk and control effectiveness. This is largely because it allows the model to structurally analyze the probability of cloud risks ex ante and ex post so as to enhance the detection of measurement errors. To validate the approach adopted, two alternative models[74] were constructed to determine the best model fit relating to our data. However, both models yielded less promising results (see Sect. 6.1). The next section of this article provides an overview and analysis of all transaction risk data obtained from the cloud risk registry.

5 An Overview of Cloud Transaction Risk Exposure

As mentioned above, institutions are exposed to significant privacy, technology and security-related risks when cloud services are outsourced. The main objectives of this section are to first outline all inherent cloud risk exposures according to the TCE framework, secondly, to establish how such risks translate into internal control challenges, and lastly, to examine risk by source and severity. In summary, the findings derived from these analyses confirm that some of the most important cloud risks are driven not only by agency cost, but also by firm-specific (or internal) risks, which contributes to a number of transaction uncertainties and potential governance challenges. Table 3 reports the frequency of all cloud risks (N = 42).

[71] Anderson et al. (2017).

[72] In their paper on residual risk trade-offs, they modelled a series of complex risk relationships on 234 risky IT transactions to test whether the control-residual risk trade-off varies in the cost of control with partnership-specific factors such as prior ties and the criticality of strategic resources to the transaction. However, their approach differs from that applied in this study, as they examined associations between control misalignment derived from the TCE regression, and direct measures of residual risk. For more on their work, see ibid.

[73] Ibid, p 2179.

[74] In M1, all residual risk indicators were fixed to 0 so as to exclude the residual risk parameters in the estimation of transaction risks. In M2, equality constraints were applied on the residual risk indicators to match the estimates of inherent risks. Overall, both models reported poorer fit indexes (e.g., mediocre RSMEA, poor TLI with weaker fit indices on all levels). These results confirm that our suggested model provides a more accurate representation of the hypothetical relationships. The results are discussed in more detail in Sect. 6.

Table 3 TCE cloud risk assessment framework

	Transaction risk proxy	Frequency	Percent
1	Asset specificity	8	19
2	Transaction (legal and technological) uncertainties	31	74
3	Task frequency	3	7
	Total	42	100

5.1 Theoretical Analysis on Cloud Risks

As illustrated above, the Bank was exposed to 42 unique cloud transaction risks, which were all categorized and analyzed according to the TCE risk framework. An analysis of this nature provides valuable insights and confirmatory evidence on the content of the risk categories identified in this study and related governance challenges. These results will be particularly useful due to the limited number of studies which have applied this framework to measure cloud risks.[75] According to the data, legal and technological uncertainties account for the highest source of inherent risk exposures (74%), followed by asset specificity (19%), and task frequency (7%). These findings are similar to those of Makhlouf[76] who concluded that the cloud has considerable levels of uncertainty and asset specificity, with lower levels of task frequency for SaaS models. Notably, most transaction uncertainties relate to legal and technology uncertainties. Like Trenz et al.,[77] the study finds that privacy, security and IT availability concerns are the major sources of these uncertainties. Similarly, these transaction uncertainties correlate well with the behavioral and primary uncertainties dimension as described by Yigitbasioglu.[78] For example, for our case in particular, primary 'legal' uncertainties such as regulatory and compliance risks arise due to uncertainties with data privacy legislation caused by poor data governance, immature internal privacy policies on data privacy, and poor contracting knowledge.[79]

According to the data, primary 'technological' uncertainties concern risks associated with IT system exposures such as IT availability risk, risk of ISP disruptions, IT prioritization risks, external cyber breaches, and capabilities of the CSP. The data also confirms that behavioral uncertainties relate to opportunism and the lack of trust in the arrangement. More specifically, in this case study, these risks relate

[75] For more details, see Trenz et al. (2013), Yigitbasioglu (2014) and Makhlouf (2020).

[76] Makhlouf (2020).

[77] Trenz et al. (2013).

[78] Yigitbasioglu (2014).

[79] According to the data, the most critical technological uncertainties include the risk of service disruptions, data loss due to migration issues, disaster and business continuity risks, CSP security breaches, and cyber security risk. The most critical legal risks consist of legal knowledge risks such as lack of knowledge on the implementation of the cloud contract, compliance risks due to immature internal privacy policies on data privacy (e.g., poor data mapping assessments) and reputational risks which are driven by poor internal policies on international data transfers for EU or international data subjects.

to potential security breaches by the cloud provider, data theft and opportunistic increases in contract prices. However, the Bank categorized these risks as low due to prior outsourcing relationships with the vendor. These results are expected as studies suggest that trust and prior ties are known to have positive influences on contractual outcomes and some agency costs.[80]

In line with the assumptions of TCE, transactions with high levels of uncertainties result in a number of governance challenges. According to Makhlouf,[81] higher levels of uncertainties result in implied costs relating to contract management, monitoring and legal compliance. This will likely be the case for the Bank given the high level of uncertainties which will ultimately translate into a number of organizational challenges, such as the inability to anticipate or predict future outcomes in the arrangement.[82] In such cases, the costs of reducing this uncertainty can exceed the costs of internal governance.[83] Consequently, this can increase initial and ongoing transaction costs such as due diligence search costs and the cost of anticipating and monitoring ex-post and unspecified transaction hazards and contingencies.

Against this backdrop, the degree of asset specificity (19%) is expected to contribute to institutional challenges, particularly as the bank has identified human resource risk, customization risk and cost overrun risk as high-risk sources. This can be problematic as familiarity and specialized knowledge are essential requirements to realize any transaction savings associated with specific investments.[84] In addition, as studies confirm that managerial conduct is associated with better governance outcomes, lack of knowledge on outsourcing processes can be a hindrance in devising a suitable control strategy. In addition to these factors, the risk of vendor lock-in[85] will likely influence the ability of the firm to transition to another cloud provider due to the dependencies created in the arrangement. For the Bank in particular, this is a major concern as both traditional and cloud services are outsourced to the same provider. With regard to the task frequency dimension (7%), a lower frequency is recorded largely because of the deployment type (SaaS). Notwithstanding this, more coordination effort, internal adjustments and structured governance forms may be required given the hybrid governance structure. This is expected as cooperative adaption mechanisms are often required in frequent and uncertain transactions.[86]

Having established how the aforementioned risk categories can contribute to governance challenges for the Bank, this section examines risks by severity and source so as to establish whether internally (firm risk) or externally driven factors contributed to the greatest source of institutional exposures discussed above.

According to the data, 62% of all inherent risks are of medium/high level, 33% are of medium/low level and 5% are of a low risk level. This implies that more than

[80] Reuer and Ariño (2002).

[81] Makhlouf (2020).

[82] Leblebici and Gerald (1981) and Rindfleisch and Heide (1997).

[83] Eisenhardt (1989).

[84] Williamson (1979), p 240.

[85] De Vita et al. (2011).

[86] Reimers et al. (2019).

half of cloud risks can result in severe financial and non-financial impacts. The data shows that firm risk is an important source of inherent risk exposure as 45% of all risks are caused by internal risk factors such as lack of knowledge of suitable IT processes and regulatory uncertainties.[87] Interestingly, the data also shows that the highest source of residual risks are legal uncertainties (e.g., reputational risk, data governance risk) which arise due to internal risk sources.

Ultimately, these results confirm that legal risks stemming from complexities in data privacy regulation are the most critical risk category facing the institution, and are likely to be a major impediment to effective governance. These results are not surprising given the complexities of data privacy regulation and the absence of a comprehensive set of cloud risk methodologies. To explore this further, Fig. 2 above depicts the inherent risk exposures by financial impact, severity and risk mitigation strategy.

The next section investigates these issues further by first measuring the degree of inefficiencies in the transaction and then providing empirical evidence to demonstrate how efficiently the bank was able to mitigate all inherent risks.

6 The SEM Results: Measuring Transaction Misalignment

The results so far indicate that firm-specific risk contributed to a significant degree of inherent risk exposures in the cloud transaction. In light of the previous discussion, we now provide the SEM results which evaluate how effectively the institution mitigated those inherent risk exposures. The first part of this section provides a graphical depiction (Fig. 3) of the SEM model to illustrate the relationship between risk and governance. The second part analyzes the results of the measurement model which confirm model strength and validity.

As illustrated in Fig. 3, the Bank was only able to mitigate 47% (e.47) of risks with institutional controls. Overall, the model provides a positive measure for misalignment, as evidenced by a significant p value (0.003) and 95% confidence interval, which illustrates the positive effects of governance strategies on the reduction of cloud risks. These findings provide support for the first hypothesis (H1) in this study which suggests that misalignments between inherent cloud risks and governance controls are synonymous with inefficiencies in cloud governance. Figure 3 provides a graphical depiction of the SEM model applied in this study.

Similar to other studies, we assume that the error term on the regression is associated with inefficiencies in governance which are likely caused by inappropriate or poor design of controls. To further interpret these results, the study applies the approach of Argyres and Bigelow[88] which suggests that a measurement error of.47 represents a relatively strong degree of misalignment. In accordance with transaction cost theory, this therefore means that the Bank will incur higher transaction

[87] See footnote 79.

[88] Argyres and Bigelow (2007), p 1338, assessed firm misalignment on a scale of 0–1, whereby the value of zero (0) signaled complete alignment, 0.25 signaled better alignment, 0.5 signaled strong misalignment, and 1 signaled complete misalignment.

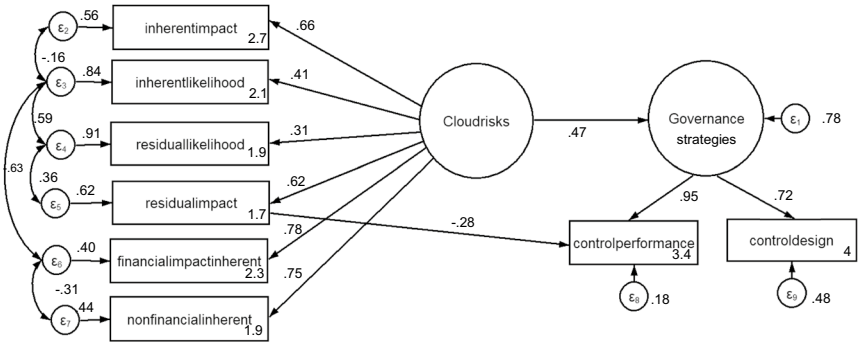

Fig. 3 (As illustrated, the graphical model contains eight latent variables and two latent constructs. Note, the latent constructs are variables which are not directly observed (denoted by the circle). Cloud transaction risks serve as the exogenous latent variable, and governance strategies serve as the endogenous latent variable. The estimates from both latent constructs are derived from the observed variables (N = 42) which are directly obtained from the Bank's risk registry. The independent variables which provide a measure of transaction risks are: (1) financial impact, (2) non-financial impact, (3) inherent risk, (4) inherent likelihood, (5) residual impact and (6) residual likelihood. The dependent variables which provide a measure of governance controls are (7) control performance and (8) control design. One variable per latent construct was constrained to 1, so as to provide an interpretable scale to estimate the factor variances and factor loadings. The residual errors are denoted by Ɛ and are provided on the latent variables and constructs (Ɛ1 to Ɛ9).) Mitigation of cloud outsourcing risks

costs to reflect its 'suboptimal' governance structure. However, some degree of inefficiency is expected as no control system can eliminate all risk factors. Therefore, there will always be a risk trade-off, whereby the institution has to decide its risk appetite and the level of risks which is tolerable. Table 4 below provides the output of the structural equation along with the corresponding standard errors, p values and confidence intervals.

Table 4 Structural model (standardized scores)

Standardized	Coef.	OIM				
		Std. err.	z	P > |z|	[95% conf.	interval]
residual~t						
transact~s	.6172208	.1126858	5.48	0.000	.3963608	.8380808
_cons	1.748.475	.2453657	7.13	0.000	1.267.567	2.229.383
controlp~e						
residual~t	− .2775653	.1503789	− 1.85	0.065	− .5723025	.017172
Governance~s	.9478695	.1948285	4.87	0.000	.5660127	1.329.726
_cons	336.616	.425204	7.92	0.000	2.532.775	4.199.544
Governance~s						
transact~s	.4665754	.159119	2.93	0.003	.154708	.7784429

Table 5 Measurement model (standardized scores)

Measurement	Coef.	OIM				
		Std. err.	z	P >|z|	[95% conf.	interval]
Inherent impact						
transact~s	.6623839	.1140924	5.81	0.000	.4387668	.8860009
_cons	2.740.131	.3364436	8.14	0.000	2.080.714	3.399.549
Inherent likelihood						
transaction risks	.4055035	.1635048	2.48	0.013	.08504	.725967
_cons	213.976	.2735622	7.82	0.000	1.603.588	2.675.933
Residual likeli~d						
Transaction risks	.3066869	.1524288	2.01	0.044	.0079319	.605442
_cons	1.934.657	.2553804	7.58	0.000	143.412	2.435.193
Financial inherent						
Transaction risks	.7757425	.12488	6.21	0.000	.5309821	1.020.503
_cons	2.315.987	.2960155	7.82	0.000	1.735.807	2.896.167
Non financial~t						
Transaction risks	.7477517	.1161791	6.44	0.000	.5200449	.9754585
_cons	1.913.615	.2596225	7.37	0.000	1.404.764	2.422.466
Control_Design						
Governance strategies	.720382	.15151	4.75	0.000	.4234279	1.017.336
_cons	4.011.287	.4640713	8.64	0.000	3.101.724	492.085

6.1 The Measurement Model Results

As we have completed our discussion on the degree of inefficiency in the transaction, the objective of this section is to discuss the results of the measurement model. This discussion is particularly important in light of our SEM construction (see Sect. 3.1.2). Additionally, these results are also significant as they help to establish which measure is most closely related to the latent variables and whether there are any correlated or unique relationships amongst the risk and governance indicators as predicted by the model. As illustrated in Table 5, all latent variables have a strong significance in estimating the latent constructs 'cloud transaction risk' and 'governance controls' according to related p-values (< .05). These results provide confirmatory evidence on our empirical approach as SEM studies suggest that latent variables

Table 6 SEM covariance (standardized) estimates

	Coef.	OIM Std. error	z	P > |z|	[95% conf.	interval]
cov(e.Residualimpact,e.Residual-likelihood)	.3608513	.1208006	2.99	0.003	.1240864	.5976162
cov(e.inherentimpact,e.likelihood)	− .1600041	.1814617	− 0.88	0.378	− .5256626	.1956544
cov(e.Inherent _ likeli, e.residual_ likeli)	.589204	.0969612	6.08	0.000	.3991635	.7792444
cov(e.Inherent_likeli, e.financialimpact)	− .6264535	.2577278	− 2.43	0.015	− 1.131.59	− .1213163
cov(e.financialimpact, e.nonfinancialimpact)	− .306416	.4241438	− 0.72	0.470	− 1.137.72	.5248906

with strong significance confirm the strength of the factors in providing a measure of the variable to be tested.

In light of the alterations applied to the SEM model, the results also show that residual likelihood is significant (.044) in estimating the latent construct 'cloud transaction risk'. These results confirm that residual risk contributes to a more accurate measure of risk and governance. To further validate the approach applied, two alternative SEM models (M1, M2)[89] were constructed. The results derived from these models were also compared to the original residual estimates by the Bank, and the SEM model in this study. Notably, all models provide a close degree of misalignment (M1 =.38; M2 =.40, SEM =.47), but the alternative models provided less significant coefficients and poorer fit indices than the model in this study. Taken together, the results suggest that there may be some weaknesses in the Bank's estimation of transaction risks or possibly in the evaluation of internal controls.

Table 6 reports the covariance and variance scores which confirm a number of significant correlations between risk and controls. These relationships are important as studies suggest that a latent variable is defined more accurately when indicator variables are strongly related to one another.[90]

As illustrated, a significant correlation (0.015) is recorded between 'e.inherent_ likeli' and 'e.financial impact', which indicates that a rise in the likelihood of a cloud failure increases the risk of financial impact. Significant positive associations are also recorded between variables 'e.residual impact' and 'e.residual likelihood' indicating that changes in the likelihood of residual risk, increases residual impact. However, non-significant correlations are recorded for variables 'inherent likelihood and inherent impact' and 'financial and nonfinancial impact'. A negative correlation between 'e.inherent impact and e.inherent likelihood' is common as most cloud risks (47%) have a low probability of occurrence, (e.g.,

[89] As mentioned previously, two alternative models (M1 and M2) were constructed to validate the model choice. In M1, all residual risk indicators are controlled (fixed to 0), so as to only observe the effect of inherent risks on governance controls. In M2, equality constraints were applied on the residual risk indicators to match the estimates of inherent risks. Notably, both models provided poorer fit indexes (e.g., RSMEA, TFI) on all levels, with M1 providing the poorest overall fit evidenced by other poor fit scores (e.g., poorer upper and lower confidence intervals).

[90] Bollen and Noble (2011).

Table 7 Model fit results

Fit statistic	Value	Parameters
Population error		
RSMEA	.056	Close fit
CFI comparative fit index	.983	Good fit
TLI Tucker-Lewis index	.964	Good fit
CD (coefficient of determination)	0.961	Good fit
Cronbach alpha	.745	Moderate fit
SRMR	.076	Good fit
Df (degrees of freedom)	15	

cyber security risks, business continuity risks), but result in high or medium risk impacts. As it relates to the variables 'e.financial impact' and 'e.non-financial impact', a negative non-significant correlation exists, which is in line with expectations as financial and non-financial impact are driven by different risk factors.

Lastly, the discussion now turns to the variance scores and the model fit indices which add validity to the model. According to the output from the SEM, the model explains 96% of the variance in the endogenous latent construct and reports mostly very good (> .63) factor loadings.[91] Further, the model fit (Table 7) confirms that the hypothesized model fits well to the data, as indicated by RMSEA < .06, CFI > .95, TLI > .95 and SRMR, < 0.08.[92] These results suggest that the observed data and the model results are likely to reflect a real situation. The SRMR index indicates that the model has a low possibility of misspecification, bias and discrepanies between the observed correlation and predicted correlations. Other fit indicators such as the 90% confidence intervals (upper bounds > 0.10 and lower bounds < 0.05%) and the Cronbach alpha are also consistent with good model fit and internal realiability. Given the limitations of a single case study, the minimum sample size requirement[93] suggested by SEM simulation studies served as the main basis for constructing the model. Altogether, these studies and others[94] confirm that two factor models, with sample sizes of N = 30 or no less than N = 40[95] have sufficient statistical power to

[91] See graphical SEM model (Fig. 3) in which 6/8 loadings are of very good/excellent strength. Generally, studies suggest that factor loadings between +/-0.30 to 0.40 are considered to meet the minimal level for interpretation. Factor loadings are commonly interpreted as follows: 0.32 (poor), 0.45 (fair), 0.55 (good), 0.63 (very good) or 0.71. (excellent). For more on these rules, see Comrey and Lee (1992).

[92] Hu and Bentler (1999).

[93] Notwithstanding the commonly applied rules of thumb (e.g., variables rule of thumb, or minimum sample size requirements), some simulation studies have proven that small sample sizes have adequate statistical power to derive meaningful associations in SEM models. For more on SEM sample size criteria, see Wolf et al. (2013), Sideridis et al. (2014) and Preacher and MacCallum (2002). For recent studies which have applied the criteria of Wolf et al. (2013) and Sideridis et al. (2014), as the sole indicator to validate sample sizes, see Kamble et al. (2021), Ghaithan et al. (2021) and Sission (2021). Consistent with our single case study design, see also the study of Van Den Heuvel et al. (2020) where SEM analysis (N = 71) was applied to a single organization to evaluate how employees adapt to organizational changes and work engagement.

[94] For additional studies which justify smaller sample sizes (N = 10), see Mundfrom et al. (2005).

[95] For more details see Wolf et al. (2013) and Sideridis et al. (2014).

derive meaningful associations in SEM models. Table 7 above provides an overview of the model fit results.

Overall, the SEM provides strong model output and conclusive evidence confirming a strong degree (.47) of misalignment or inefficiencies in cloud governance. These results suggest that some misalignments identified are more likely to relate to inefficiencies in the internal control environment. The next section seeks to establish the validity of these claims.

7 Cloud Governance Strategies

In light of the previous discussions, this section seeks to establish whether the degree of inefficiencies identified was caused by poor internal control design issues, arising from the complex nature of cloud regulation. To answer this question, elements of the Bank's internal control framework were applied to a simple linear regression model. Through this approach we are able to establish whether the Bank's control system provides acceptable indications of residual risk, whilst capturing the factors which contribute to weak internal governance. This section begins by presenting the results of the regression model so as to assess the strength of the Bank's control framework before concluding on the main control inconsistencies identified. Altogether, these analyses show that the requirements for cross-border transfers of personal data and the absence of a comprehensive risk methodology (and KPIs) create less clarity on the rules required to manage cloud risks. Ultimately, these factors translate into poor governance strategies and highlight the need for financial institutions to have a good understanding of local and foreign laws to implement a sound compliance program.

7.1 The Strength of Residual Risk Predictions

According to the data, the model reports a significant regression ($p < .0005$) indicating that (i) inherent risk likelihood (x), (ii) control design (x) and (iii) control effectiveness (x) are significant predictors of residual likelihood. This confirms that the linear regression model can be used to provide strong indications of whether any misalignment on the SEM is associated with internal control issues. From a theoretical perspective these results can prove to be significant as they validate the model and contribute to the advancement, development and use of residual risk models, particularly in light of limited studies. As the data relates to the model output, it shows that the Bank has a weak control framework. More specifically, as illustrated in Table 8, (i) inherent risk likelihood (x), (ii) control design (x) and (iii) control effectiveness (x) have 50% predictive power in estimating residual likelihood. In other words, this indicates that the model only explains 50% of variance in the likelihood of residual risk impacts. Essentially, this means that the control framework can only anticipate the occurrence of half ($R^2$50) of all residual risks modelled in the SEM (47%). Table 8 below shows the model summary and results of the simple linear regression.

Table 8 Strength of internal control

Model summary[a]

Model	R	R square	Adjusted R square	Std. error of the estimate
1	.709[a]	.502	.461	.463

[a]Predictors: (constant), control design, inherent likelihood, control performance
[b]Dependent variable: residual likelihood

ANOVA[b]

Model	Sum of squares	df	Mean square	F	Sig.
1					
Regression	7.782	3	2.594	12.100	.000[b]
Residual	7.718	36	.214		
Total	15.500	39			

[a]Dependent variable: residual likelihood
[b]Predictors: (Constant), control design, inherent likelihood, control performance

According to Kountur[96] a residual model which predicts an $R^2$52 is considered unsatisfactory in estimating the likelihood of residual risk, as it can have implications for risk planning. As a result, a higher R^2 would symbolize greater reliability and predictability of internal controls in estimating the likelihood of residual risks. These results confirm our second hypothesis which suggests that models with a lower significance (R^2) are synonymous with weaker internal control systems.

Having concluded on the strength of internal control, the next section provides the coefficients on the model which will help to establish whether the Bank suffered from any control design issues arising from poor institutional compliance practices regarding data privacy.

7.2 Interconnections Between Internal Control and Risk Assessments

As mentioned previously, the study pays particular attention to correlations amongst elements of internal control to identify control irregularities and the source of those irregularities. In line with the hypothesis (H3) posed earlier, it is expected that positive interrelations reflect more efficient governance outcomes, which are likely to reduce governance misalignments. These relationships were confirmed in this study (Table 9), as a number of common significant associations are identified between predictors of residual risk. For instance, a negative significant correlation between control performance and residual risk indicates that as control performance increases, the impact of residual risk decreases, which is in line with expectations (Table 10).

A significant association between inherent and residual likelihood is also common, as it indicates that any rise in inherent likelihood increases residual likelihood. On the other hand, negative correlations are reported between control performance

[96] Kountur (2018), p 54.

Table 9 Coefficients[a]

Model		Unstandardized coefficients		Standardized coefficients	t	Sig.	95% confidence interval for B		Collinearity statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	.260	.541		.480	.634	− .837	1.357		
	Control performance	− .317	.123	− .390	− 2.571	.014	− .568	− .067	.602	1.662
	Inherent likelihood	.462	.125	.516	3.693	.001	.208	.716	.707	1.414
	Control design	.371	.163	.310	2.275	.029	.040	.702	.746	1.340

[a]Dependent variable: residual likelihood

Table 10 Coefficient correlations[a]

Model			Control design	Inherent likelihood	Control performance
1	Correlations	Control design	1.000	.098	− .397
		Inherent likelihood	.098	1.000	.449
		Control performance	− .397	.449	1.000
	Covariances	Control design	.027	.002	− .008
		Inherent likelihood	.002	.016	.007
		Control performance	− .008	.007	.015

[a]Dependent variable: residual likelihood

and control design. These results are uncommon or 'irregular' as elements of internal control, such as the quality and appropriateness of control, should contribute to control effectiveness and risk reduction. Therefore, a negative correlation indicates that control design contributes negatively to the performance of internal controls and will likely increase the probability of residual risks.

These results confirm the hypothesis that suggests that some misalignment identified can be explained by inefficiencies in internal control, particularly as it relates to the design of controls. Additionally, the $R^2$50 on the model indicates the existence of a weak control system, incapable of predicting at least half of the misalignment identified on the model. These results are in line with expectations, as most inherent risk exposures were driven by internal risks arising from technological and legal uncertainties (e.g., poor data mapping strategies, IT prioritization risks) which may have translated into poor internal control design. Ultimately, these results confirm that a significant number of risks are driven by cross-border risks arising from divergent data privacy regimes.

Altogether, the results of the above analyses are consistent with the hypothesis that managing data privacy risks may be a key challenge for financial institutions. In this regard, a good starting point for compliance is understanding 'what, why, how and where' data is processed, thoroughly evaluating the terms and conditions in cloud contracts and in data transfer agreements, and ensuring compliance by cloud providers.[97] In addition, there may well be advantages for regulators to consider introducing soft law mechanisms and key performance indicators (KPIs) so that institutions can sufficiently evaluate the appropriateness of internal control measures. Ultimately, applying KPIs and usefully combining them with comprehensive, flexible privacy and technology-enhancing policies and practices may reduce some transaction uncertainties in cloud risk management.

[97] Matheson (2017).

8 Conclusion

The study examined the effectiveness of internal governance on an ongoing cloud outsourcing transaction between a bank and cloud service provider (CSP). We use the empirical analysis in this case study to show that data governance is a key challenge for financial institutions. More specifically, the SEM provided evidence indicative of a strong degree of misalignment in the cloud transaction. The results show that firm-specific risk is a significant risk factor as it contributes to a number of transaction uncertainties and misalignment in the cloud transaction. Our results of the multiple linear regression confirmed that most of the misalignment relates to inadequate design of controls on a number of legal risk exposures (e.g., poor practices regarding data governance strategies and privacy policies on international data transfers). Ultimately, the results tend to show a weak control system, which provides unacceptable indications of residual risk exposures. Overall, it is clear from these findings that there are still considerable uncertainties in devising sound internal governance strategies, largely due to uncertainties in cloud regulation. Through the outcomes of the study, it should become easier to examine more closely how firms assess critical cloud risks and devise sound internal governance strategies to mitigate cloud risk exposures in the financial industry. Most importantly, it is also crucial to steer studies towards research that assesses whether there is a need for more specification on risk criteria and responses, given the regulatory complexity of the cloud landscape. However, in light of the limitations of this single case study, future research could focus on other types of financial institutions that may might benefit from improved cloud risk management practices.

Acknowledgements The author thanks Prof. Dr. Joseph McCahery J.D. for valuable comments and suggestions on the article, as well as, in particular, the seminar participants of the 4th TILT International PhD Colloquium (TIPC2021) at the Tilburg Institute for Law, Technology, and Society (TILT) for their comments on the paper, and, lastly, the financial institution for providing data analyzed in this study.

References

Anderson E (1988) Strategic implications of Darwinian economics for selling efficiency and choice of integrated or independent sales forces. Manag Sci 34(5):599–618. https://doi.org/10.1287/mnsc.34.5.599

Anderson SW, Dekker HC (2005) Management control for market transactions: the relation between transaction characteristics, incomplete contract design, and subsequent performance. Manag Sci 51(12):1734–1752. https://doi.org/10.1287/mnsc.1050.0456

Anderson SW, Dekker HC, Van Den Abbeele A (2017) Costly control: an examination of the trade-off between control investments and residual risk in inter-firm transactions. Manag Sci 63(7):2163–2180. https://doi.org/10.1287/mnsc.2016.2435

Argyres N, Bigelow L (2007) Does transaction misalignment matter for firm survival at all stages of the industry life cycle? Manag Sci 53(8):1332–1344. https://doi.org/10.1287/mnsc.1070.0706

Banerjee AV, Duflo E (2000) Reputation effects and the limits of contracting: a study of the Indian software industry. Q J Econ 115(3):989–1017. https://doi.org/10.1162/003355300554962

Bank of England and Financial Conduct Authority (2021) Operational resilience: impact tolerances for important business services. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf. Accessed 8 Nov 2021

Bank of England, Prudential Regulation Authority (2019a) Consultation Paper, CP30/19. Outsourcing and third party risk management. December 2019. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019a/cp3019.pdf. Accessed 8 Nov 2021

Bank of England, Prudential Regulation Authority (2019b) Consultation Paper, CP29/19. Operational resilience: impact tolerances for important business services. December 2019. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019b/cp2919.pdf. Accessed 8 Nov 2021

Bank of England, Prudential Regulation Authority (2021a) Supervisory Statement, SS2/21. Outsourcing and third party risk management. March 2021. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021a/ss221-march-21.pdf. Accessed 8 Nov 2021

Bank of England, Prudential Regulation Authority (2021b) Policy Statement, PS7/21. Outsourcing and third party risk management, feedback to CP30/19. March 2021. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2021b/march/ps721.pdf. Accessed 8 Nov 2021

Bank of England, Prudential Regulation Authority (2021c) Policy Statement, PS6/21. Operational resilience: impact tolerances for important business services, feedback to CP29/19. March 2021. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021c/march/ps621.pdf?la=en&hash=A15AE3F7E18CA731ACD30B34DF3A5EA487A9FC11. Accessed 8 Nov 2021

Basel Committee on Banking Supervision (BCBS) (2020) Consultative Document. Principles for operational resilience. August 2020. Bank for International Settlements. https://www.bis.org/bcbs/publ/d509.pdf. Accessed 8 Nov 2021

Bentler PM, Chou CP (1987) Practical issues in structural equation modeling. Sociol Methods Res 16(1):78–117. https://doi.org/10.1177/0049124187016001004

Blunch NJ (2013) Introduction to structural equation modeling using IBM, SPSS statistics and AMOS. 2nd edn. SAGE, Los Angeles. https://doi.org/10.4135/9781526402257

Bollen KA, Noble MD (2011) Structural equation models and the quantification of behavior. PNAS Proc Natl Acad Sci USA 108(3):15639–15646. https://doi.org/10.1073/pnas.1010661108

Boomsma A (1985) Nonconvergence, improper solutions, and starting values in LISREL maximum likelihood estimation. Psychometrika 50:229–242. https://doi.org/10.1007/BF02294248

Bruwer JP, Coetzee P, Meiring J (2017) The empirical relationship between the managerial conduct and internal control activities in South African small, medium and micro enterprises. S Afr J Econ Manag Sci 20(1):1–19. https://doi.org/10.4102/sajems.v20i1.1569

Commission Nationale de l'Informatique et des Libertés (CNIL) (2015) Privacy Impact Assessment (PIA) Methodology (how to carry out a PIA). https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf. Accessed 8 Nov 2021

Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control-Integrated Framework (2013; 1992). https://www.coso.org/pages/ic.aspx. Accessed 24 Apr 2022

Comrey AL, Lee HB (1992) A first course in factor analysis, 2nd edn. Psychology Press, East Sussex. https://doi.org/10.4324/9781315827506

Cortina JM, Green JP, Keeler KR, Vandenberg RJ (2017) Degrees of freedom in SEM: are we testing the models that we claim to test? Organ Res Methods 20(3):350–378. https://doi.org/10.1177/1094428116676345

De Buysere KAS (2015) Legal & market infrastructure for technology-driven firms. Doctoral thesis dissertation. s.n. https://research.tilburguniversity.edu/en/publications/legal-amp-market-infrastructure-for-technology-driven-firms. Accessed 24 Apr 2022

De Vita G, Tekaya A, Wang CL (2011) The many faces of asset specificity: a critical review of key theoretical perspectives. Int J Manag Rev 13(4):329–348. https://doi.org/10.1111/j.1468-2370.2010.00294.x

De Winter JCF, Dodou D, Wieringa PA (2009) Exploratory factor analysis with small sample sizes. Multivar Behav Res 44(2):147–181. https://doi.org/10.1080/00273170902794206

Eisenhardt MK (1989) Building theories from case study research. Acad Manag Rev 14(4):532–550

European Union Agency for Cybersecurity (ENISA) (2013) Recommendations for a methodology of the assessment of severity of personal data breaches. European Union Agency for Network and Information Security, Working Document, v1.0, Galan Manso C, Gorniak S (eds). December 2013. https://op.europa.eu/en/publication-detail/-/publication/dd745e70-efb8-4329-9b78-79020ec69da5. Accessed 8 Nov 2021

Federal Ministry for Economic Affairs and Energy (BMWi) and Federal Ministry of Education and Research (2019) Project GAIA-X. A federated data infrastructure as the cradle of a vibrant European ecosystem. https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4. Accessed 24 Apr 2022

Financial Conduct Authority (2019) Building operational resilience: impact tolerances for important business services and feedback to DP18/04. Consulation Paper (CP19/32). December 2019. https://www.fca.org.uk/publication/consultation/cp19-32.pdf. Accessed 8 Nov 2021

Financial Conduct Authority (2021) Building operational resilience: feedback to CP19/32 and final rules. Policy Statement, PS21/3. March 2021. https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf. Accessed 8 Nov 2021

Financial Stability Board (2019) Third-party dependencies in cloud services. Considerations on financial stability implications. https://www.fsb.org/wp-content/uploads/P091219-2.pdf. Accessed 20 Oct 2021

Ghaithan A, Khan M, Mohammed A, Hadidi L (2021) Impact of Industry 4.0 and lean manufacturing on the sustainability performance of plastic and petrochemical organizations in Saudi Arabia. Sustainability 13(20):11252. https://doi.org/10.3390/su132011252

Greenleaf G (2012) The influence of European data privacy standards outside Europe: implications for globalisation of Convention 108. Int Data Priv Law 2(2):68–92. https://doi.org/10.1093/idpl/ips006

Handley SM (2017) How governance misalignment and outsourcing capability impact performance. Prod Oper Manag 26(1):134–155. https://doi.org/10.1111/poms.12609

Hox JJ, Bechger TM (1999) An introduction to structural equation modeling. Fam Sci Rev 11:354–373

Hu L, Bentler PM (1999) Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. Struct Equ Model 6(1):1–55. https://doi.org/10.1080/10705519909540118

Jak S, Jorgensen TD, Verdam MGE, Oort FJ, Elffers L (2020) Analytical power calculations for structural equation modeling: a tutorial and Shiny app. Behav Res Methods 53(4):1385–1406. https://doi.org/10.3758/s13428-020-01479-0

Jansen W, Grance T (2011) Guidelines on security and privacy in public cloud computing. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg. https://doi.org/10.6028/NIST.SP.800-144. Accessed 24 Apr 2022

Johansson T (2015) A critical appraisal of the current use of transaction cost explanations for government make-or-buy choices: towards a contingent theory and forms of tests. Public Manag Rev 17(5):661–678. https://doi.org/10.1080/14719037.2013.848922

Jöreskog KG (1970) A general method for estimating a linear structural equation system. ETS Res Bull Ser 2(1):41. https://doi.org/10.1002/j.2333-8504.1970.tb00783.x

Kamble SS, Gunasekaran A, Subramanian N, Ghadge A, Belhadi A, Venkatesh M (2021) Blockchain technology's impact on supply chain integration and sustainable supply chain performance: evidence from the automotive industry. Ann Oper Res. https://doi.org/10.1007/s10479-021-04129-6

Kline RB (2011) Principles and practice of structural equation modeling, 3rd edn. Guildford Press, New York

Kontargyris X (2018) IT laws in the era of cloud computing, a comparative analysis between EU and US law on the case study of data protection and privacy. Schriften der Albrecht Mendelssohn Bartholdy Graduate School of Law. Nomos Verlagsgesellschaft. https://doi.org/10.5771/9783845295626

Kountur R (2018) The likelihood value of residual risk estimation in the management of enterprise risk. Invest Manag Financ Innov 15(3):49–55. https://doi.org/10.21511/imfi.15(3).2018.04
Krebs D (2012) Regulating the cloud: a comparative analysis of the current and proposed privacy frameworks in Canada and the European Union. CJLT 10(1):29–74
Kulesza J (2014) Transboundary data protection and international business compliance. Int Data Priv Law 4(4):298–306. https://doi.org/10.1093/idpl/ipu020
Leblebici H, Salancik GR (1981) Effects of environmental uncertainty on information and decision processes in banks. Admin Sci Q 26(4):578–596
Leiblein MJ, Miller DJ (2003) An empirical examination of transaction- and firm-level influences on the vertical boundaries of the firm. Strateg Manag J 24:839–859. https://doi.org/10.1002/smj.340
Leiblein MJ, Reuer JJ, Frédéric D (2002) Do make or buy decisions matter? The influence of organizational governance on technological performance. Strateg Manag J 23(9):817–833. https://doi.org/10.1002/smj.259
Lopes AEMP (2017) Resource dependence and transaction costs: towards a convergent model. Gestao E Producao 24(4):806–813. https://doi.org/10.1590/0104-530X2819-16
MacCallum RC, Browne MW, Sugawara HM (1996) Power analysis and determination of sample size for covariance structure modeling. Psychol Methods 1(2):130–149. https://doi.org/10.1037/1082-989X.1.2.130
Makhlouf R (2020) Cloudy transaction costs: a dive into cloud computing economics. J Cloud Comput Adv Syst Appl 9(1):1–11. https://doi.org/10.1186/s13677-019-0149-4
Mangasih ET, Pinasti M, Bawono IR (2020) The effect of quality of internal audit and effectiveness of internal control systems on good corporate governance in finance companies. J Account Bus 5(1):56–82. https://doi.org/10.20884/1.sar.2020.5.1.2723
Marsh HW, Hau KT, Balla JR, Grayson D (1998) Is more ever too much? The number of indicators per factor in confirmatory factor analysis. Multivar Behav Res 33:181–220. https://doi.org/10.1207/s15327906mbr3302_1
Matheson (2017) GDPR in context: impacts on the asset management industry
Mayer KJ, Argyres NS (2004) Learning to contract: evidence from the personal computer industry. Organ Sci 15(4):394–410. https://doi.org/10.1287/orsc.1040.0074
Maxwell W, Wolf C (2012) A global reality: governmental access to data in the cloud. A comparative analysis of ten international jurisdictions. A Hoga Lovells White Paper. https://www.hoganlovells.com/-/media/hogan-lovells/pdf/publication/revised-government-access-to-cloud-data-paper-18-july-12_pdf.pdf. Accessed 9 Oct 2021
Messier WF, Austen LA (2000) Inherent risk and control risk assessments: evidence on the effect of pervasive and specific risk factors. Auditing 19(2):119–131. https://doi.org/10.2308/aud.2000.19.2.119
Moschandreas M (1997) The role of opportunism in transaction cost economics. J Econ Issues 31(1):39–57. https://doi.org/10.1080/00213624.1997.11505890
Mundfrom DJ, Shaw DG, Ke TL (2005) Minimum sample size recommendations for conducting factor analyses. Int J Test 5(2):159–168. https://doi.org/10.1207/s15327574ijt0502_4
Nunnally JC (1967) Psychometric theory. McGraw-Hill, New York
Preacher KJ, MacCallum RC (2002) Exploratory factor analysis in behavior genetics research: factor recovery with small sample sizes. Behav Genet 32(2):153–161. https://doi.org/10.1023/A:1015210025234
Quélin B, Motlow D (1998) Outsourcing: a transaction cost theory approach. Réseaux 6(1):75–98. https://doi.org/10.3406/reso.1998.3338
Rae K, Sands J, Subramaniam N (2017) Associations among the five components within COSO internal control-integrated framework as the underpinning of quality corporate governance. Australas Account Bus Finance J 11(1):28–54. https://doi.org/10.14453/aabfj.v11i1.4
Reimers K, Guo X, Li M (2019) Beyond markets, hierarchies, and hybrids: an institutional perspective on IT-enabled two-sided markets. Electron Markets 29(2):287–305. https://doi.org/10.1007/s12525-018-0319-0
Reuer JJ, Ariño A (2002) Contractual renegotiations in strategic alliances. J Manag 28(1):47–68. https://doi.org/10.1016/S0149-2063(01)00130-1
Rindfleisch A, Heide JB (1997) Transaction cost analysis: past, present, and future applications. J Mark 61(4):30–54. https://doi.org/10.2307/1252085
Rozendaal M (2019) Do not underestimate risks to data subjects. EDPS-ENISA Conference: Towards assessing the risk in personal data breaches, Brussels (BE), 4 April 2019. https://www.enisa.europa.eu/events/edps-enisa-conference. Accessed 24 Apr 2022
Royal Bank of Canada (RBC) (2017) The question of data sovereignty and the influence of GDPR. https://www.rbccm.com/assets/rbccm/docs/news/2017/mifid-6.pdf. Accessed 24 Apr 2022

Sampson RCS (2004) The cost of misaligned governance in R&D alliances. J Law Econ Organ 20(2):484–526. https://doi.org/10.1093/jleo/ewh043
Schreiber JB, Nora A, Stage FK, Barlow EA, King J (2006) Reporting structural equation modeling and confirmatory factor analysis results: a review. J Educ Res 99(6):323–337. https://doi.org/10.3200/JOER.99.6.323-338
Sideridis G, Simos P, Papanicolaou A, Fletcher J (2014) Using structural equation modeling to assess functional connectivity in the brain: power and sample size considerations. Educ Psychol Meas 74(5):733–758. https://doi.org/10.1177/0013164414525397
Silverman BS, Nickerson JA, Freeman J (1997) Profitability, transactional alignment, and organizational mortality in the U.S. trucking industry. Strateg Manag J (summer Special Issue) 18:31–52. https://doi.org/10.1002/(SICI)1097-0266(199707)18:1+%3c31::AID-SMJ920%3e3.0.CO;2-S
Sission AD (2021) Music festival supervisor leadership style and organizational citizenship behavior: the effects of employee and volunteer relationships and dependence on their leader. Int J Event Festiv Manag 12(4):380–398. https://doi.org/10.1108/IJEFM-11-2020-0070
Smith B (2010) Building confidence in the cloud: a proposal for industry and government action for Europe to reap the benefits of cloud computing. Brookings Institution Forum on Cloud Computing for Business and Society, 20 January 2010, Washington DC. https://www.brookings.edu/events/cloud-computing-for-business-and-society/. Accessed 24 Apr 2022
Taylor H, Artman E, Woelfer JP (2012) Information technology project risk management: bridging the gap between research and practice. J Inf Technol 27(1):17–34. https://doi.org/10.1057/jit.2011.29
Tolbert GD (2005) Residual risk reduction: systematically deciding what is 'safe.' Prof Saf 50(11):25–33
Trenz M, Huntgeburth J, Veit D (2013) The role of uncertainty in cloud computing continuance: antecedents, mitigators, and consequences. ECIS 2013 Completed Research. Paper 147. https://www.researchgate.net/publication/259780986_The_Role_of_Uncertainty_in_Cloud_Computing_Continuance_Antecedents_Mitigators_and_Consequences. Accessed 8 Nov 2021
US Department of Justice (2019) Promoting public safety, privacy, and the rule of law around the world: the purpose and impact of the CLOUD Act. White Paper, April 2019. https://www.justice.gov/dag/page/file/1153436/download. Accessed 9 Oct 2021
Van den Heuvel M, Demerouti E, Bakker AB, Hetland J, Schaufeli WB (2020) How do employees adapt to organizational change? The role of meaning-making and work engagement. Span J Psychol 23(e56):1–16. https://doi.org/10.1017/SJP.2020.55
Van der Meer-Kooistra J, Vosselman EGJ (2000) Management control of inter-firm transactional relationships: the case of industrial renovation and maintenance. Acc Organ Soc 25(1):51–77. https://doi.org/10.1016/S0361-3682(99)00021-5
Van Genugten ML (2008) The art of alignment, transaction cost economics and the provision of public services at the local level. PhD Disseration, University of Twente. https://research.utwente.nl/en/publications/the-art-of-alignment-transaction-cost-economics-and-the-provision. Accessed 24 Apr 2022
Weston R, Gore PAJ (2006) A brief guide to structural equation modeling. Counsel Psychol 34(5):719–751. https://doi.org/10.1177/0011000006286345
Williamson OE (1979) Transaction cost economics: the governance of contractual relations. J Law Econ 22(2):233–261. The University of Chicago Press. http://www.jstor.org/stable/725118. Accessed 8 Nov 2021
Williamson OE (1981) The economics of organization: the transaction cost approach. Am J Sociol 87(3):548–577. https://doi.org/10.1086/227496
Williamson OE (1985) The economic institutions of capitalism: firms, markets, relational contracting. Free Press, London
Williamson OE (1991) Strategizing, economizing, and economic organization. Strateg Manag J 12(S2):75–94. https://doi.org/10.1002/smj.4250121007
Williamson OE (1998) Transaction cost economics: how it works; where it is headed. De Econ Q Rev R Neth Econ Assoc 146(1):23–58. https://doi.org/10.1023/A:1003263908567
Wolf EJ, Harrington KM, Clark SL, Miller MW (2013) Sample size requirements for structural equation models: an evaluation of power, bias, and solution propriety. Educ Psychol Meas 76(6):913–934. https://doi.org/10.1177/0013164413495237
Yigitbasioglu O (2014) Modelling the intention to adopt cloud computing services: a transaction cost theory perspective. Australas J Inf Syst 18(3):193210. https://doi.org/10.3127/ajis.v18i3.1052