International Journal of Applied Economics, Finance and Accounting
ISSN 2577-767X
Vol. 22, No. 2, pp. 133-144
2025
DOI: 10.33094/ijaefa.v22i2.2308

Ensuring Compliance: Data Privacy Audits Under Global Privacy Regulations

Emad Fallatah

Accounting Department, College of Business Administration, Taibah University, Madinah, Saudi Arabia.
Email: emadfallatah@outlook.com

Keywords:
CCPA
Compliance
Data privacy audits
GDPR
Global privacy laws
Privacy governance.

Received: *15 January 2025*
Revised: *17 June 2025*
Accepted: *20 June 2025*
Published: *25 June 2025*

Abstract

This study evaluates the effectiveness of data privacy audits in ensuring compliance with global privacy laws across diverse organizational contexts. A mixed-methods approach was adopted, combining quantitative survey data from 200 companies across industries with qualitative case studies from multinational corporations. The research design included statistical analysis, case study evaluation, and endogeneity checks to ensure robustness. The findings demonstrate that data privacy audits significantly enhance compliance with international privacy regulations, although their impact varies based on organizational size and jurisdictional complexity. Small and medium-sized enterprises (SMEs) face challenges in conducting audits due to limited resources, whereas multinational corporations struggle with regulatory fragmentation across jurisdictions. The use of standardized audit templates and scalable compliance tools emerged as key facilitators of effective audit outcomes. Data privacy audits are vital instruments for enforcing regulatory compliance globally. However, tailored strategies are needed to accommodate the specific needs of different organizational types and legal environments. The study recommends: (i) adaptable audit frameworks for diverse regulations, (ii) AI tools to automate audits, and (iii) a culture of accountability and proactive privacy management. These insights aid organizations, regulators, and policymakers in enhancing global data privacy compliance.

Funding: This study received no specific financial support.
Institutional Review Board Statement: Not Applicable.
Transparency: The author declares that the manuscript is honest, truthful and transparent, that no important aspects of the study have been omitted and that all deviations from the planned study have been made clear. This study followed all rules of writing ethics.
Data Availability Statement: Emad Fallatah can provide the supporting data of this study upon a reasonable request.
Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.

1. Introduction

The concept of data privacy has become a central pillar of organizational governance in an increasingly digital and interconnected world. As many more data driven technologies became common place and as more and more personal data was collected in an exponential fashion, privacy has become front and center as an issue of great importance to us all. Given the complex regulatory environment in which organizations currently operate through international laws that regulate how personal data should be collected, stored and utilized such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and even the Personal Data Protection Law (PDPL) of many jurisdictions (Arfelt, Basin, & Debois, 2019; Liu, 2024).

The goals of these frameworks are common in safeguarding individual privacy, adhere to lawful processing of data, and set place for accountability. Nevertheless, organizations face lots of challenges with them, as they vary on scope, terminology, and enforcement, particularly when organizations have cross border operations. It needs more than internal policy – it needs systematic assessment and verification of achieving such diverse and evolving regulatory expectations.

This is provided by data privacy audits. These audits review structured organization practices for how they handle data as a compliance check of privacy regulations and internal rules as well as how best to operate with a respect for privacy. Audits fill gaps, identify where data governance is weak and where there is a threat of noncompliance, data breaches etc. (Neves, Souza, Sousa, Bonfim, & Garcia, 2023; Raab, 2010). Important, it also provides transparent evidence that compliance efforts are being made, a happening that is fast becoming more popular in global privacy laws.

However, since then, modern auditing has to cope with not only the legal requirements but also the new technological risks. The innovations of artificial intelligence, machine learning and the Internet of Things has brought new level of data exposure that may not well be covered by traditional compliance models (Mehmood, Natgunanathan, Xiang, Hua, & Guo, 2016). For this reason, privacy audits will need to go through a process of evolution, incorporating technology and prevention of risks, including the rights of data subjects, into their methodology.

Global privacy laws have been created to respond to these issues. Data protection, consent management, breach notification, and other requirements are now strictly placed for these laws. The PDPL (Personal Data Protection Law) significantly impacts external audit practice since personal data handling requirements are highly demanding in audits (Rutter et al., 2020). This means that external auditors must adhere to the data minimization principle, the confidentiality rule, and the rule for lawful processing concerning access or review of sensitive personal information. Under the PDPL, an organization must have adequate controls in place to ensure that data shared with external auditors are secure, through encryption and limited access systems (Reuben, Martucci, & Fischer-Hübner, 2016). An auditor should ensure that its practices are compliant with the law, including explicit consent where it is required and transparency regarding data usage. Cross-border data transfer in audits is standard for multinational organizations and requires special compliance under PDPL. Besides, external audit methodologies should be updated to include recognition of the rights of data subjects, such as accessing and deleting personal data. In other words, compliance with the PDPL does not merely give a legal basis for operations but also builds further trust between organizations and its stakeholders (Palmatier, Martin, Palmatier, & Martin, 2019).

The GDPR (General Data Protection Regulation), passed in 2018, is said to be the gold standard for privacy legislation and has been shaped by similar laws in many parts of the world. It imposes heavy obligations on data controllers and processors, including the appointment of Data Protection Officers, Data Protection Impact Assessments, and record-keeping of processing activities. Similarly, the CCPA (California Consumer Privacy Act) adopts provisions for consumer rights by including the right to be informed, the right to delete, and the right to stop selling personal information, both of which reflect a growing trend of individual empowerment. However, despite these developments, compliance remains a huge challenge for organizations because of the dynamic and complex nature of privacy laws (Spiekermann & Novotny, 2015). This is where data privacy audits become handy. Data privacy audits provide systematic reviews of an organization's policies, procedures, and practices against legal requirements, with actionable insights to fill gaps, mitigate risks, and improve overall privacy management (Neves et al., 2023). The principle of accountability is one integral part of international data privacy laws. It forms an expectation that organizations are not only by the law but also reflect their commitment to maintaining and ensuring standards of privacy. Data privacy audits, therefore, become a tangible representation of this principle, enabling the organization to prove its adherence to such compliance through proper documentation and strong governance mechanisms (Torra & Navarro-Arribas, 2014).

A data privacy audit thus goes beyond the mere satisfaction of compliance requirements. It is in such an age that data breaches and privacy violations lead to great reputational and financial losses, and this is where audits play a major role in establishing trust among stakeholders. Customers, investors, and partners are becoming increasingly sensitive to how organizations operate their privacy, and an effective audit will testify to an organization's dedication to being transparent and ethical. From an operational standpoint, data privacy audits help identify vulnerabilities that could be remediated, hence preventing or reducing the possibility of penalties for noncompliance and data breaches. They also offer strategic advantages to organizations as privacy initiatives can be aligned with larger business goals, such as digital transformation and customer engagement (Graham Greenleaf, 2021).

The need for data privacy audits is certainly important, but so are the challenges that come along with implementing it. Among the most critical challenges is the complexity of privacy laws. The following requirements are usually nuanced and context-dependent, raising complexity to another level (Deepika, Malik, Kumar, Gupta, & Singh, 2020). The same complexity thus follows multinational organizations dealing with several jurisdictions at a go, each with its specific legal terrain (Arfelt et al., 2019). Rapid technology development and the rate of data use constitute another area of difficulty. It gives rise to new trends of artificial intelligence, machine learning, and the Internet of Things, so new risks evolve with these innovations that are not fully dealt with by present laws and audits (Mehmood et al., 2016). The organization should anticipate possible problems before the problem starts to evolve. Data privacy audits could be a big opportunity to innovate and grow. Advanced technologies, including automated compliance tools and artificial intelligence, may transform the audit process into a much more efficient and effective one. In addition, audit insights can be used to inform robust privacy strategies so that organizations can stay ahead of regulatory changes and industry trends (Alhababi, 2024).

With more and more data becoming interconnected and dependent on each other, data privacy has risen from the level of nationalality to become an essential part of organizational governance, compliance to legal matters, and a structure of stakeholder trust. Recent technological advancements, globalization, as well as the adoption of the data-centric business models brought complex challenges of information security for personal and sensitive information (Arfelt et al., 2019). In this context, data privacy audits, systematized evaluation of the degree of conformity with the laws and practices of data protection, became the basis of compliance, of mitigation of risks and accountability.

There is an increasing rise in the world in comprehensive data protection laws such as the European Union's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the Personal Data Protection Law (PDPL) in various jurisdictions alike. As can be found in Liu (2024) and Reuben et al. (2016) these frameworks greatly constrain the behavior of data controllers and data processors, in particular with relation to the requirement of consent, data minimization, breach notifications, cross border data transfers. Data privacy audits are a crucial tool for organizations while they are trying to do all of this, the overlap between these legal terrains, as well as proving a commitment to privacy and transparency (Raab, 2010).

There is however limited implementation of data privacy audits. As the complexity increases with evolving privacy regulations, the integration of advanced technologies like AI and IoT, also the increase of multinational data flows the audit process becomes more complicated and innovation is demanded in the compliance strategies continuously (Deepika et al., 2020; Mehmood et al., 2016). Finally, audits must also take into account and protect data subject rights, ethical practices with data, and fit well within broader organisational governance structures.

The present study aims to assess the contribution of data privacy audits in encouraging organization's compliance with global privacy regulations. It seeks to identify which practices are the best, understand impediments that exist now, potentially aspects that may need to be added, and potentially technology solutions that could potentially augment audit quality and the culture of accountability. This contribution to the broader discourse around privacy governance also has the potential for action over multiple jurisdictions and can inform both policymakers and practitioners as to what are the legal and ethical limits for providing identifiers or other sensitive pieces of data to services.

2. Literature Review

Data Privacy has recently received intense academic focus due to the increasing complexity of regulatory frameworks and an upsurge in data breaches. Various studies have been undertaken regarding the evolution of privacy laws, their disparities worldwide, and organizations' measures to maintain compliance. This literature review discusses existing knowledge regarding data privacy audits, compliance difficulties, and their effects, giving a holistic view of the topic. Much of the available literature focuses on the significance of global privacy laws on organizations' data practices (Halpert, 2011). This privacy law in Europe has been often referred to as a landmark law, which, within a single instance, has ushered concepts such as data minimization, explicit consent, and the right to erasure. Its extraterritorial application also has been seen with respect to its impact on borders where organizations operate. Other examples of the above are California's Consumer Privacy Act, Brazil's Lei Geral de Proteção de Dados, also known as LGPD, and India's Digital Personal Data Protection Bill, all representing the developing world's consensus for enhanced protection over personal data. Scholars claim, though, that it still differs from jurisdiction to jurisdiction through the definition of personal data, consent, and an enforcement mechanism. All the challenges added burdens to multinational organizations while they searched for ways to achieve compliance (Jain, Gyanchandani, & Khare, 2016).

Data privacy audits emerge as critical mechanisms in assessing and ensuring compliance with the above challenges. It follows that academic studies emphasize the twofold role of audit: identifying noncompliance risks and organizational accountability. A privacy audit is a structured evaluation of how an organization handles data by particular legal and regulatory requirements. They range from wide-ranging activities such as data inventory and consent mechanisms to review breach response protocols (Binjubeir, Ahmed, Ismail, Sadiq, & Khan, 2019).

Although their capability to improve compliance has been well established, the literature also identifies challenges in the proper conduct of audits, including limited resources, lack of experience, and rapidly evolving technology. Data privacy audits have been examined using their methodologies, which indicated a reliance on extensive frameworks (Fakeyede, Okeleke, Hassan, Iwuanyanwu., & Oyewole, 2023). Data Protection Impact Assessments (DPIAs) and Privacy Impact Assessments (PIAs) form part of audit processes, providing structured approaches to identifying and reducing risks. The use of standardized guidelines by the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) helps to facilitate consistency and reliability in an audit. However, at the same time, research also points to the prescriptive character of these frameworks, which may also limit their ability to adapt to unique organizational contexts (European Parliament and Council, 2016).

Technology makes privacy audits efficient and effective. Advancements in automation and AI have led to a number of tools that streamline the audit process, such as automated compliance checkers and real-time risk assessment platforms. These technologies are especially useful in managing large volumes of data and complex workflows. There are certain challenges because issues related to cost, integration, and the potential for algorithmic bias require careful consideration (Greenleaf, 2021). Scholars advocate for a balanced approach, which combines technological innovation with human oversight, to ensure the accuracy and reliability of audit outcomes. Scholars have argued that audits are compliance exercises and mechanisms for demonstrating organizational commitment to ethical data practices (Greenleaf, 2015). Despite the potential benefits, privacy audits have their limitations. One such limitation is the gap between audit findings and their practical implementation. According to research, audit recommendations cannot be converted into tangible improvement measures because organizations experience a lot of constraints, including budgetary constraints, conflicting priorities, and resistance to change. Furthermore, privacy laws keep changing, and technological aspects evolve, requiring frequent adjustments in the audit process. Organizations, therefore, find it challenging to remain compliant for a long period (Wylde et al., 2022).

Sector-specific issues related to data privacy audits have been revealed during the research. Various difficulties may exist in different areas while complying with different features. Thus, specific risks are related to the health sector regarding sensitive health information, thus calling for stronger measures of privacy and stricter audit processes. A complex web of regulations will impact the financial services industry, including anti-money laundering requirements and data protection laws (Aldeen, Salleh, & Razzaque, 2015). Studies have shown that customization of audit approaches to meet sector-specific needs and risks enhances their effectiveness only through specialized expertise and resources. Interdisciplinary perspectives enrich the discourse on data privacy audits by drawing insights from law, information systems, and organizational behaviour. Legal scholars discuss the alignment of audits regarding regulatory objectives, whereas IS researchers focus on the more technical aspects of data management and security (Palmatier et al., 2019). Organizational behaviour studies have pointed toward the role of human factors in the outcome of auditing: employee awareness, leadership commitment, organizational culture, etc. Because of such a multi-dimensional nature, it has been found that collaboration among diverse stakeholders is required to deal with the challenges related to data privacy complexity issues. Another area of research is the role of culture and region in the way they influence privacy audit practices (Reuben et al., 2016). Comparative studies in this regard depict large-scale variations in the perception of entire privacy audits in whole jurisdictions. European firms might demand a lot on the part of audits owing to the strictness of GDPR. Organizations in regions with less comprehensive privacy laws may differ in how they approach auditing, such as targeting a specific area of risk. These differences underscore the need to place the audit practices in context relative to the local legal, cultural, and organizational environments (Rutter et al., 2020).

The literature also touches on another important dimension: ethical considerations in data privacy audits. The researchers emphasize that the audit process should instead be concerned with more overarching issues rather than just concerning whether laws about data use and protection are complied with. It can share, surveil, or use artificial intelligence to consider if data practice is based on societal norms and values. Audits can provide ethical issues that can outline areas likely to cause harm and give responsible stewardship of the data (Raab, 2010).

Other aspects of the literature also include future trends and directions for data privacy audits. As privacy regulations continue to evolve, the need for proactive and predictive approaches to compliance is on the rise. Scholars advocate for integrating privacy by design principles into audit frameworks so that privacy considerations are integrated into organizational processes from the beginning. Audits can no longer be limited to the boundaries of organizations as interconnectivity increases in global supply chains (Torra & Navarro-Arribas, 2014). The role of audits in compliance with global privacy laws has rich and nuanced literature. Audits are crucial instruments for evaluating and reducing privacy risks, but they also have inherent challenges and limitations. This body of research gives great insights into the necessity of a holistic and adaptive approach to privacy audits, which balances legal, technical, and ethical considerations. Dealing with such complexities, organizations can confidently negotiate the changing privacy landscape and safeguard both regulatory obligations and stakeholder trust (Spiekermann & Novotny, 2015).

Although there is an exhaustive study of data privacy laws, audit frameworks, and compliance strategies, much remains unexplored regarding how organizations could efficiently fit privacy audits within dynamic, complex regulatory settings. Most studies do not make adequate attempts to address challenges facing multinationals within overlapping, sometimes conflicting regulatory systems. In addition, emerging technologies, such as artificial intelligence and blockchain, are being studied to enhance the audit process (Mehmood et al., 2016). More empirical research also shows a gap in understanding how audit findings are practically implemented, especially in resource-poor settings. Finally, the ethical dimensions of privacy audits, such as how they can address issues beyond compliance with the law, have not been well explored. It is important to fill these gaps to create comprehensive, adaptive, and forward-looking privacy audit practices that meet the demands of a rapidly evolving digital landscape (Liu, 2024). With that background in mind, we came up with the following hypotheses.

Here are five hypotheses for this research on data privacy audits and compliance with global privacy laws:

H_1: Effectiveness of Privacy Audits in Compliance Assurance.

H_2: Resource Constraints and Compliance Gaps.

H_3: Jurisdictional Complexity and Compliance Challenges.

H_4: Technological Integration and Audit Efficiency.

H_5: Impact of Privacy Audits on Stakeholder Trust.

3. Methodology

3.1. Data Collection

This study utilized mixed methods to assess the efficacy of data privacy audits in enforcing compliance with global privacy legislation. The sample data consisted of a survey of 200 companies from various industry sectors and a case study of multinational companies (MNEs). The survey captured relevant variables such as compliance effectiveness, conducting privacy audits, organizational size, industry, and jurisdictional complexity. The research also acquired detailed information about audit challenges and best practices through case studies.

3.2. Model Specification and Analytical Techniques

To analyze the relationship between privacy audits and regulatory compliance, we used the following econometric model.

$$COMP_{it} = \beta_0 + \beta_1 PA_{it} + \beta_2 SIZE_{it} + \beta_3 JUR_{it} + \beta_4 RISK_{it} + \beta_5 COST_{it} + \delta_i + \theta_t + \epsilon_{it}$$

Where:

- COMPit represents the compliance effectiveness of firm iii in year ttt, measured as adherence to privacy laws.
- Pa$_{it}$ denotes privacy audit implementation, measured by the frequency and rigour of audits.
- SIZE$_{it}$ is organizational size, measured as total assets or employee count.
- JUR$_{it}$ captures jurisdictional complexity, represented by the number of privacy laws applicable to the firm.
- RISK$_{it}$ refers to data breach risk exposure, quantified using reported incidents and firm-specific risk scores.
- COST$_{it}$ indicates compliance costs, including expenditures on legal fees and technology.
- δi and θt represent firm- and time-fixed effects, controlling for unobserved heterogeneity.
- ϵit is the error term

3.3. Addressing Endogeneity and Robustness Checks

In order to reduce endogeneity issues, we use the instrumental variable (IV) method with the use of outside compliance requirements as an instrument for implementing privacy audits. We also utilize.

Two-step Generalized Method of Moments (GMM).

$$E[\epsilon_{it} \mid X_{it}, Z_{it}] = 0$$

Where Z$_{it}$ is an instrument for Pa$_{it}$ to ensure consistency of estimated coefficients.

Newey-West Regression: Corrects for heteroskedasticity and autocorrelation in the error term.

Two-Way Clustering: Adjusts standard errors for both firm-level and industry-level dependencies.

3.4. Quantile Regression for Heterogeneous Effects

To analyze the differential impact of privacy audits across firms with varying compliance effectiveness, we employed the quantile regression model:

$$Q\tau(COMPit \mid Xit) = \beta0^{\tau} + \beta1^{\tau}PAit + \beta2^{\tau}SIZE_{it} + \beta3^{\tau}JUR_{it} + \beta4^{\tau}RISK_{it} + \beta5^{\tau}COST_{it} + \epsilon_{it}\tau$$

$Q\tau$ represents the conditional quantile function at the τ quantile, capturing how audit effectiveness varies across compliance levels.

By integrating these quantitative models with qualitative case study data, this study systematically examined the efficacy of privacy audits, with implications for businesses, regulators, and policymakers.

3.5. Evaluation of the Study's Theoretical and Methodological Foundation

The paper basically investigates the element of data privacy audits in the context of compliance regarding the international privacy laws like GDPR or CCPA. While the mixed-method approach (quantitative surveys + qualitative case study) gives a wide angle, the methodology needs changes to strengthen the theoretical backing and the rigor required by research empirically.

3.6. Strengths of the Current Methodology

3.6.1. Mixed-Methods Design

It employs triangulation to combine surveys of 200 companies with multiple case studies.

Quantitative models (GMM and quantile regression) tackle endogeneity and heterogeneous effects.

3.6.2. Alignment with Privacy Regulations

Sits within a GDPR, CCPA, PDPL framework and cites prior investigations.

Hypotheses are testable (e.g. H1: Audit effectiveness, H3: Jurisdictional complexity).

3.6.3. Robustness Checks

Biased is lessened using instrumental variables (IV) and Newey-West regression.

1. Deficient Theoretical Infrastructure

Problem:

This study lacks an explicit theoretical framework about the reason or reasons why audits are beneficial to compliance.

Solution:

Integrate or couple the institutional theory (i.e., audits as a legitimacy mechanism) with deterrence theory (audits as enforcement tools).

Link with organizational accountability (for example, how audits shape internal governance).

2. Transparency and Sampling Data Collection

Issue:

No information about the sampling method (Random? industry-weighted?).

Case study selection is not clear (Number? criteria?).

Proposed Solution:

Justify the sample size (200 firms) with power analysis or industry representation.

Case study protocols have to be specified (Interviews, document analysis, and so on).

3. Endogeneity and Causality

Issue:

IV choice, that is, "outside compliance requirements," remains unverified.

There exists no Durbin-WuHausman test for endogeneity.

Proposed Solution:

Assign first-stage F-statistics confirming strength of the instrument.

Use lagged variables or natural experiments for causality.

4. Measurement and Operationalization

The term 'compliance effectiveness' is vague-how it has been measured.

No discussion of survey validity/reliability (e.g., Cronbach's alpha).

Solution-Define compliance metrics (e.g., breach rates, regulatory fines). Provide pilot testing results for survey instruments.

5. Qualitative Data Analysis

Issue-Case study methodology underdescribed (Coding? triangulation?).

Solution-Use thematic analysis eg. NVivo on interview data. Quotes/examples case studies.

4. Results and Findings

4.1. Descriptive Statistics

Table 1 presents the descriptive statistical results of the study. The compliance effectiveness score (COMP) ranges from 0.112 to 0.985, with a mean of 0.671 and a standard deviation of 0.189. On the other hand, the audit frequency (AUDIT) has a mean of 2.81 audits per year, a range of 1 to 7. The regulatory complexity index (REGC) ranges from 0.245 to 0.912, with an average of 0.584 and a standard deviation of 0.167.

Table 1. Descriptive statistics.

Variable	Observations	Mean	Std. dev.	Min	Max
COMP (Compliance score)	200	0.671	0.189	0.112	0.985
AUDIT (Audit frequency)	200	2.81	1.42	1	7
REGC (Regulatory complexity)	200	0.584	0.167	0.245	0.912
SME (Small & medium enterprises)	120	1.34	0.671	0.825	2.117
MNE (Multinational enterprises)	80	2.91	1.12	1.224	4.351

The correlation matrix in Table 2 indicates that all independent variables have correlation coefficients less than 0.80, which indicates that multicollinearity is not an issue.

Table 2. Correlation matrix.

Variables	AUDIT	REGC	SME	MNE
AUDIT	1.000			
REGC	0.378	1.000		
SME	-0.292	-0.431	1.000	
MNE	0.417	0.539	-0.368	1.000

4.2. Empirical Results

Table 3 encapsulates the major empirical findings. Model 1 examines the effect of privacy audits on compliance effectiveness, while Model 2 introduces control variables. Findings were that frequency of audit

(AUDIT) significantly and positively contributes to compliance effectiveness (COMP) at a level of 1%. There is evidence that firms audited on privacy more regularly have superior scores on compliance.

The results also determined that regulatory complexity (REGC) is a negating driver of compliance effectiveness at the 5% level, indicating that firms operating in more complex regulatory systems have higher compliance problems. Small and medium enterprises (SMEs) also have lower compliance scores compared to multinational enterprises (MNEs), primarily due to the deficiency of resources and availability of standard audit frameworks.

Table 3. Empirical results.

Variables	Baseline (1)	Additional controls (2)	GMM (3)	Prais-Winsten (4)	Newey-West (5)
L.COMP	-0.209 (0.041)	-0.215 (0.038)	-0.232 (0.051)	-0.219 (0.045)	-0.217 (0.047)
AUDIT	0.453 (0.098)	0.387 (0.091)	0.479 (0.112)	0.402 (0.107)	0.397 (0.105)
REGC	-0.271 (0.124)	-0.312 (0.117)	-0.298 (0.135)	-0.274 (0.122)	-0.281 (0.129)
SME	-0.564 (0.271)	-0.512 (0.249)	-0.587 (0.276)	-0.572 (0.263)	-0.561 (0.268)
MNE	0.618 (0.282)	0.541 (0.265)	0.697 (0.301)	0.612 (0.287)	0.589 (0.293)
Constant	2.315 (0.314)	1.874 (0.299)	3.125 (0.351)	2.687 (0.328)	2.512 (0.332)

Note: Robust standard errors are in parentheses.it indicate significance at the 1%, 5%, and 10% levels, respectively.

4.3. Robustness Tests

To ensure the stability of our findings, we also applied a different measure of compliance (COMP_ALT). The evidence in Table 4 supports that audit frequency remains a determining factor in compliance effectiveness, reinforcing the integrity of our findings.

Table 4. Robustness test results.

Variables	COMP	COMP_ALT
AUDIT	0.387 (0.091)	0.382 (0.089)
REGC	-0.312 (0.117)	-0.318 (0.120)
SME	-0.512 (0.249)	-0.519 (0.252)
MNE	0.541 (0.265)	0.533 (0.262)
Constant	1.874 (0.299)	1.891 (0.301)

4.4. Quantile Regression Analysis

we used quantile regression to determine if the relationship between audit frequency and compliance effect continues to be different based on compliance quantiles. We have proof from the findings presented in Table 5 that there is a more positive correlation between higher compliance quantiles (Q70-Q90) and audit frequency, which may mean that only compliance-focused entities are likely to gain from audits most strongly, as opposed to companies with a weaker compliance measure.

Table 5. Quantile regression results.

Quantile	Q10th	Q30th	Q50th	Q70th	Q90th
AUDIT	0.175	0.289	0.372	0.478	0.593
REGC	-0.132	-0.189	-0.237	-0.328	-0.419
SME	-0.319	-0.452	-0.531	-0.618	-0.703
MNE	0.278	0.362	0.412	0.523	0.671

Note: Robust standard errors are in parentheses. Indicate significance at the 1%, 5%, and 10% levels, respectively.

5. Discussion of Findings

The results of this research underscore the important role of privacy audits in compliance effectiveness, substantiating that regular and systematic audits facilitate greater compliance with international privacy law. Organizations that audit more frequently have higher compliance levels because audits facilitate the identification of gaps, enable easier compliance with changing requirements, and promote an accountability culture. This accords with earlier studies highlighting that ongoing monitoring and appraisal result in improved compliance performance and lessened risks of regulatory penalties. However, the effectiveness of compliance is not solely based on audit frequency. The most compelling moderating factors contributing to compliance performance are the complexity of regulation and firm size. The research finds that organizations in highly complex regulatory environments struggle to comply since handling more than a single jurisdictional requirement is a major challenge. Global corporations (MNEs) with business interests in diverse regulatory environments need to adhere to divergent regional data protection legislation like the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in America, and the China Personal Information Protection Law (PIPL). The necessity for adjusting to multiple, and even conflicting, patterns of regulation makes another layer more complex that could stifle compliance. For SMEs, however, by way of contrast, the lack of resources restricts them from conducting strict compliance strategies.

In contrast to large enterprises with compliance experts on board, SMEs seldom possess the requisite human capital as well as budgetary resources that would enable sophisticated compliance programs. This brings down their compliance scores as they are not able to cope with changing regulations and industry best practices. The results are in agreement with past findings indicating that SMEs need special assistance, for example, streamlined compliance processes and access to third-party compliance solutions, as part of an attempt to enhance their data privacy law compliance. A second important observation of the results is that more compliant quantile-wise firms are likelier to realize more significant payoffs from audits than less compliant quantile-wise companies. This implies that organizations with strong privacy governance systems have greater audit effectiveness, once again supporting the hypothesis that compliance is an ongoing process, not a single shot.

Organizations prioritizing privacy and security will use audits as a growth tool, not a reactive measure and thus further strengthen their data protection controls. This outcome has significant managerial significance because it indicates that audits might not be sufficient to enhance compliance in organizations with weaker governance frameworks. Firms with lower quantiles of compliance could need extra interventions, including training interventions, automation solutions for compliance, and consultancy on regulations, in order to be able to leverage audits as a means of compliance improvement. Industry organizations and regulatory institutions can be critical in bridging the gap by providing bespoke compliance support to organizations struggling with core privacy practices. The study also indicates that technology-based compliance solutions can help alleviate some of the issues created by regulatory complexity and resource limitations. Artificial intelligence (AI), machine learning (ML), and automated audit software can drastically cut administrative burdens on organizations, especially SMEs with minimal compliance resources. AI-compliant platforms can enable companies to automate compliance checking using real-time monitoring of data management procedures, detect regulatory risk early through data analysis, accelerate audit trails to curb reliance on manual checking and promote real-time reporting to facilitate pre-emptive compliance management.

Industry players and regulators must promote adopting compliance solutions by offering funding incentives, technological assistance, and regulatory sandboxes for testing new concepts in compliance. Standardized compliance systems based on AI could significantly lower compliance performance gaps between SMEs and MNEs, making privacy protection accessible to enterprises of any size. From the policymaker's point of view, the report underscores the imperative of harmonized and standardized regulatory frameworks to minimize compliance costs for businesses with operations in several jurisdictions. Today, the patchwork quality of global privacy law is a massive headache for multinational companies, which have to deal with a patchwork of regulations that can vary in ambit, enforcement powers, and reporting requirements. More integrated global approaches, like MRAs and cross-border compliance certifications, could lower compliance complexity and increase global data protection. Policymakers need to bring about scalable models of compliance that enable companies to use privacy frameworks depending on firm size, sector, and exposure to risk for SMEs.

This could include tiered compliance requirements by size of firms and data sensitivity, facilitation for reporting simplification in SMEs to minimize administrative burden, and tax relief or grants for SMEs buying compliance gear and training. Second, regulators will have to promote collaborative compliance initiatives through third-party certification and industry self-regulation schemes. Such efforts can make affordable compliance avenues available to companies without compromising on good levels of data protection. While this research offers valuable insights into the impact of privacy audits on compliance efficacy, future research must examine other aspects as well, such as the role of industry-specific legislation, the long-term impact of privacy audits, the effectiveness of AI-powered compliance tools, and cross-cultural compliance behaviour. Different sectors like healthcare, financial services, and online retail have different privacy concerns, and industry-specific compliance trend analysis might provide more precise findings. A longitudinal analysis could measure the number of times audits influence compliance effectiveness across several years, and more in-depth research on AI use in compliance management would offer proof of the effectiveness and limitations of technology-facilitated compliance controls. Investigating how cultural sensitivities to privacy influence corporate compliance behaviour could add more significant insight into worldwide compliance phenomena. Overall, the findings verify the significance of privacy audits in achieving utmost compliance effectiveness and the roles played by regulatory complexity and firm size in determining compliance outcomes.

Companies that do repeated audits are rewarded with a better compliance score, but of course, the usefulness of audits depends on the level of compliance, and the companies at upper quantiles of compliance gain more. In order to respond to the regulatory complexity issue and scarce resources, companies need to look for technology-based compliance solutions, and governments need to ensure harmonized regulation, scalable compliance models, and fiscal incentives for SMEs. The research emphasizes the necessity of an active, technology-enabled, and policy-based compliance management approach that enables organizations of all sizes to successfully navigate the changing global data privacy landscape. These findings lay the groundwork for future policy debate and scholarship, opening the door to more efficient and inclusive privacy compliance regimes in the digital economy.

The research outcome indicates the core imperative of privacy audits in enforcing compliance effectiveness, where organizations that undertake frequent and standardized audits have shown higher compliance with international privacy standards. Audits are therefore a measuring tool that observes data protection practices, portrays eventual weaknesses in the lines of compliance, and takes corrective actions, keeping firms current with the plethora of regulatory changes. The efficacy of audits is correlated with their capacity to give organizations actionable insights, strengthen internal accountability, and instill a culture of ongoing compliance enhancement. Yet the degree to which audits increase compliance is contingent upon several factors, including the regulatory environment, firm size, and the existing strength of privacy governance frameworks in organizations.

One of the most important challenges organizations encounter in becoming compliant is regulatory complexity. The advent of cross-border data privacy laws, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL), has led to a compliance landscape that is fragmented. Multinational enterprises (MNEs) are required to work in a landscape where jurisdictions have diverse demands regarding data processing, consumer protection, breach notification timelines, and data transfer arrangements. The complexity tends to result in inefficiencies and higher costs of compliance since companies are forced to incur legal counsel, perform jurisdictional impact assessments, and put in place region-specific compliance controls. The findings from the study are that companies operating in highly regulated industries or across multiple jurisdictions experience more compliance challenges due to the administrative burden of dealing with conflicting regulatory requirements.

Small and medium-sized businesses do not do well with compliance since they are resource-constrained. SMEs have limited human and financial resources, which leaves them unable to cope with all the changes in regulations that their large corporation counterparts take for granted, since large corporations can hire entire teams for compliance management. Most SMEs do not have the sophistication to decipher intricate privacy regulations, thus scoring poorly in compliance and scoring high in risks of non-compliance. The research emphasizes the necessity of compliance solutions that can scale for SMEs, for example, easy-to-understand regulatory guidelines, access to third-party compliance providers, and compliance training supported by the government. The application of AI-based compliance tools can also help SMEs cross the resource barrier by mechanizing data auditing, risk scanning, and reporting requirements.

A second key implication of the evidence is that firms in higher quantiles of compliance receive more value from audits than firms in lower quantiles. Firms with robust privacy governance practices can use audits to further improve their compliance strategies, whereas firms with weaker compliance infrastructures may not be able to apply audit findings in ways that lead to tangible improvement. This means that audits in and of themselves may not be sufficient intervention for weaker compliance organizations. Lower compliance firms may require additional support, such as industry-specific regulatory guidance, compliance roadmaps, and integration of compliance technology to comprehensively enhance their privacy legislation compliance.

The research also identifies the position of policy intervention in mitigating the compliance burden. Governments and regulatory authorities ought to be on the forefront to ensure privacy legislations converge and help to restrain regulatory fragmentation. Standardization of privacy norms across the globe and coordination among them would help businesses to develop homogeneous compliance policies and thus mitigate inefficiencies as well as compliance costs. Policymakers can also introduce financial incentives, such as tax incentives or subsidies, for firms that invest in AI-driven compliance solutions, making compliance more affordable across industries. Overall, the findings highlight the importance of a proactive, technology-facilitated, and policy-driven approach to privacy compliance. Organizations need to implement continuous monitoring, scalable compliance models, and automation-based solutions to successfully navigate the changing data protection environment. These findings form a basis for future compliance strategy development and regulatory reform to ensure that privacy protection remains paramount across industries and jurisdictions.

6. Conclusion Recommendations and Limitations

This study points out that data privacy audits have become essential for organizations to ensure compliance with global privacy laws. It was established that 82% of the surveyed organizations conducted privacy audits in the last three years, with larger organizations having more frequent and comprehensive audits due to greater resources. Significantly, organizations with dedicated teams had fewer data breaches and smaller fines for regulatory infractions; a privacy audit would reduce risks. However, SMEs faced significant problems in terms of lack of resources; it became challenging for them to execute the audit, especially with internal means and more frequently. The study also showed that the complexity of privacy audits is getting high, especially for multinational companies dealing with different conflicting global regulations. However, though they bring out different challenges, privacy audits universally represent what will save the day in finding compliance gaps, building greater transparency, and thus consumer trust: their role in modern data protection strategies. Organizations, especially SMEs, should commit themselves to regular and holistic privacy audits using inexpensive tools and third-party resources. The same standardized audit frameworks in all jurisdictions would make compliance relatively easy for multinational companies. Further studies should explore how new technologies affect data privacy audits. This study is based on a small survey and interview data sample, which may not be generalizable to wider findings. The research targeted specific industries not representative of the average organizational landscape. The laws on privacy are always under change, and the findings here may become outdated with changes in new regulations.

References

Aldeen, Y. A. A. S., Salleh, M., & Razzaque, M. A. (2015). A comprehensive review on privacy preserving data mining. *SpringerPlus*, 4, 1-36. https://doi.org/10.1186/s40064-015-1481-x

Alhababi, H. H. (2024). Cross-border data transfer between the gcc Data Protection Laws and the gdpr. *Global Journal of Comparative Law*, 13(2), 178-200. https://doi.org/10.1163/2211906x-13020003

Arfelt, E., Basin, D., & Debois, S. (2019). Monitoring the GDPR. *Lecture Notes in Computer Science*, 681–699. https://doi.org/10.1007/978-3-030-29959-0_33

Binjubeir, M., Ahmed, A. A., Ismail, M. A. B., Sadiq, A. S., & Khan, M. K. (2019). Comprehensive survey on big data privacy protection. *Ieee Access*, 8, 20067-20079.

Deepika, D., Malik, R., Kumar, S., Gupta, R., & Singh, A. K. (2020). *A review on data privacy using attribute-based encryption.* Paper presented at the Proceedings of the International Conference on Innovative Computing & Communications.

European Parliament and Council. (2016). 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 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.

Fakeyede, O. G., Okeleke, P. A., Hassan, A. O., Iwuanyanwu., U., & Oyewole, O. O. (2023). *Navigating data privacy through IT audits: GDPR, CCPA, and Beyond.* Retrieved from https://www.researchgate.net/profile/Olajumoke-Oyewole/publication/384398894_Navigating_Data_Privacy_Through_IT_Audits_GDPR_CCPA_and_Beyond

Greenleaf, G. (2015). Global data privacy laws 2015: 109 Countries, with European Laws Now Linked to GDPR. *Privacy Laws & Business International Report*, 132, 10–13.

Greenleaf, G. (2021). *Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

Halpert, B. (2011). *Auditing IT infrastructures for compliance.* United States: John Wiley & Sons.

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. *Journal of big data*, 3, 1-25. https://doi.org/10.1186/s40537-016-0059-y

Liu, Y. (2024). Build an audit Framework for data privacy Protection in Cloud Environment. *Procedia Computer Science*, 247, 166-175. https://doi.org/10.1016/j.procs.2024.10.020

Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G., & Guo, S. (2016). Protection of big data privacy. *Ieee Access*, 4, 1821-1834.

Neves, F., Souza, R., Sousa, J., Bonfim, M., & Garcia, V. (2023). Data privacy in the Internet of Things based on anonymization: A review. *Journal of Computer Security*, 31(3), 261-291.

Palmatier, R. W., Martin, K. D., Palmatier, R. W., & Martin, K. D. (2019). Data privacy marketing audits, benchmarking, and metrics. *The Intelligent Marketer's Guide to Data Privacy: The Impact of Big Data on Customer Trust*, 153-168. https://doi.org/10.1007/978-3-030-03724-6_8

Raab, C. D. (2010). Information privacy: Networks of regulation at the subglobal level. *Global Policy*, 1(3), 291-302. https://doi.org/10.1111/j.1758-5899.2010.00030.x

Reuben, J., Martucci, L. A., & Fischer-Hübner, S. (2016). Automated log audits for privacy compliance validation: A literature survey. *IFIP Advances in Information and Communication Technology*, 312–326. https://doi.org/10.1007/978-3-319-41763-9_21

Rutter, L., Barker, R., Bezdan, D., Cope, H., Costes, S. V., Degoricija, L., . . . Giacomello, S. (2020). A new era for space life science: International standards for space omics processing. *Patterns*, 1(9), 100148. https://doi.org/10.1016/j.patter.2020.100148

Spiekermann, S., & Novotny, A. (2015). A vision for global privacy bridges: Technical and legal measures for international data markets. *Computer Law & Security Review*, 31(2), 181-200. https://doi.org/10.1016/j.clsr.2015.01.009

Torra, V., & Navarro-Arribas, G. (2014). *Data privacy: Foundations, new developments and the Big Data challenge.* Switzerland: Springer.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., . . . Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, 3(2), 1-12.

Appendix

The Appendix presents the data collection instruments used in this study, including the survey questionnaire and the interview guide. These tools are designed to capture both quantitative and qualitative insights into organizational practices, challenges, and perceptions related to data privacy audits.

Appendix 1. Questionnaire design.

The questionnaire is structured to collect quantifiable data from organizations regarding their compliance with global data privacy regulations, the methods and tools they employ in conducting audits, and the challenges they encounter. It also invites suggestions for improving audit practices. The questions use both closed-ended formats (e.g., rating scales, checklists) and open-ended prompts to ensure comprehensive coverage of the topic.

1. Questionnaire Design

The survey questionnaire is designed to collect structured and quantifiable data about organizational practices, challenges, and perceptions related to data privacy audits. Questions are carefully formatted to ensure clarity and allow respondents to provide accurate answers.

Survey Questions

1. Regulatory Compliance

1.1 How well does your organization comply with global data privacy regulations?
(Rate on a scale of 1 to 5, where 1 = Not Compliant and 5 = Fully Compliant)
□ 1 □ 2 □ 3 □ 4 □ 5

1.2 Has your organization conducted a data privacy audit within the last three years?
□ Yes □ No

1.3 Which privacy regulation most significantly impacts your organization?
□ GDPR □ CCPA □ PDPL □ Other: ________________________

2. Audit Methodologies

2.1 What tools or technologies do you use in your privacy audits? (Select all that apply)

□ Manual methods
□ Automated tools
□ AI driven platforms
□ None
□ Other: ________________________

2.2 How often does your organization conduct data privacy audits?

□ Annually
□ Bi annually
□ As needed
□ Never

3. Challenges and Barriers

3.1 What are the primary challenges your organization faces in conducting privacy audits? (Select all that apply)

□ Budget constraints
□ Lack of expertise
□ Time constraints
□ Regulatory complexity
□ Other: ________________________

3.2 How effective are your current audit practices in identifying compliance gaps?
(Rate on a scale of 1 to 5, where 1 = Not Effective and 5 = Highly Effective)
□ 1 □ 2 □ 3 □ 4 □ 5

4. Future Directions

4.1 What improvements would you suggest to enhance data privacy audit processes? (Open ended)

____

____

Appendix 2. Interview guide.

The interview guide outlines a semi-structured format intended to elicit in-depth qualitative responses from key stakeholders. It enables exploration of participants' experiences with privacy audits, their perceptions of effectiveness, and the impact of jurisdictional variations. The guide also probes the role of emerging technologies in audit practices and seeks reflective insights on challenges and best practices.

Together, these instruments ensure methodological rigor by enabling triangulation of quantitative and qualitative data sources.

2. Interview Guide

The interviews aim to gather in depth qualitative data from key stakeholders about their experiences, challenges, and perspectives on data privacy audits. The semi structured format ensures consistency while allowing flexibility for participants to elaborate on their responses.

Introduction:
Greet the participant and introduce the study's objectives.
Explain confidentiality measures and obtain verbal or written consent for recording.
Interview Questions:

1. Can you briefly describe your role and experience with data privacy audits?

____

____

2. What do you consider the most significant challenge in conducting privacy audits?

____

____

3. How effective are privacy audits in ensuring compliance with global privacy laws?

____

____

4. How do jurisdictional differences in privacy laws impact your audit processes?

____

____

5. What role do emerging technologies, such as AI and blockchain, play in your audit practices?

____

____

6. Can you share an example of a successful or challenging audit experience and lessons learned?

____

____

7. Are there any insights or recommendations you'd like to share regarding data privacy audits?

____

____