International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 504-521
https://doi.org/10.70917/ijcisim-2026-2532
Article

DEVELOPMENT AND VALIDATION OF A QUALITATIVE DATA PRIVACY IMPACT ASSESSMENT SCORECARD FOR SELF-ASSESSMENT IN COOPERATIVE BANKS OF MAHARASHTRA

Amit Pradip Karkhanis[1], Dr. Ramchandra D. Patil[2]

[1]Department of Management Studies, Bharati Vidyapeeth (Deemed to be University), Navi Mumbai, Maharashtra, India.
Email: Karkhanis.ap@gmail.com
[2] Department of Management Studies, Bharati Vidyapeeth (Deemed to be University), Navi Mumbai, Maharashtra, India.
Email: dr.ramdpatil@gmail.com

Abstract: The rapid digitization of cooperative banking in Maharashtra has expanded the volume of personal data collected, processed, and shared by institutions that typically lack dedicated data protection officers, formal DPIA expertise, or the budgets required to engage external privacy consultants. In parallel, India's evolving digital privacy framework — anchored in the Digital Personal Data Protection Act — and the prevalence of internationally accepted instruments such as ISO 27701, the NIST Privacy Framework, and the GDPR DPIA have raised the regulatory expectations placed on these small financial institutions. The present study develops and validates a qualitative Data Privacy Impact Assessment (DPIA) scorecard designed specifically for self-administration by cooperative bank staff. The scorecard consolidates privacy dimensions relevant to cooperative banking data collection, consent, data subject rights, access control, third-party sharing, and retention into maturity-level rating scales that can be completed by non-specialist personnel. A structured questionnaire was administered to 213 cooperative banking professionals across Maharashtra, yielding responses that were analysed using Pearson correlation and one-sample t-tests. The study tested two hypotheses: first, that perceived complexity of existing privacy frameworks is positively correlated with the operational vulnerability of cooperative banks; and second, that the mean perception of the developed scorecard's usability is significantly greater than the neutral midpoint of the five-point Likert scale. Both null hypotheses were decisively rejected. The Pearson correlation between framework complexity and operational vulnerability reached $r = 0.683$ ($p < 0.001$), confirming that complexity is a meaningful antecedent of vulnerability in this institutional context. The aggregate one-sample t-statistic for usability was $t = 18.836$ ($p < 0.001$) against the neutral value of 3.0, validating the scorecard as perceived-usable by the very personnel expected to deploy it. The study contributes a fit-for-purpose self-assessment instrument, an empirically grounded argument for tool simplification in cooperative banking, and a methodological template for similar validation exercises in other small financial institutions.

Keywords: Data privacy; DPIA; scorecard; self-assessment; cooperative banks; Maharashtra; privacy governance; ISO 27701; GDPR; risk management; Digital Personal Data Protection Act.

1. Introduction

The cooperative banking sector in Maharashtra is a foundational component of rural and semi-urban credit delivery in India, handling the financial lives of millions of members and depositors. Over the past decade, the swift digitisation of these institutions — driven by core banking platforms, mobile-based service delivery, Aadhaar-enabled KYC processes, and inter-bank digital payment rails — has substantially increased the volume of personal data they

collect, store, and share. The shift towards a cashless economy, accelerated by fintech adoption (Goswami, Sharma & Chouhan, 2022) and post-demonetisation digital payment patterns (Sinha, Majra, Hutchins & Saxena, 2018; Firdous & Farooqi, 2017), has amplified the privacy footprint of cooperative banks in ways that the sector's traditional governance structures were not designed to manage. Concurrently, the regulatory environment for personal data in India has matured, with the Supreme Court recognising privacy as a fundamental right (Chatterjee, 2019) and the Digital Personal Data Protection Act imposing substantive obligations on data fiduciaries, including banks. International frameworks such as the EU GDPR, the California CCPA (Chacko & Mishra, 2022), the NIST Privacy Framework, and ISO 27701 have further established a global vocabulary of privacy compliance that influences Indian regulatory practice. Against this backdrop, the cooperative banking sector occupies a precarious position: it is increasingly subject to privacy expectations aligned with those faced by large commercial banks, yet it operates with resource constraints, smaller IT teams, and limited access to specialist privacy expertise (Shah, 2016; Gahongayire & Kamande, 2021).

Within this institutional context, the Data Privacy Impact Assessment (DPIA) has emerged as the principal instrument through which organisations identify, evaluate, and mitigate privacy risks associated with their data processing activities. Originating under the GDPR and now adopted in several jurisdictions, the DPIA is mandatory for processing operations that pose a high risk to data subjects (Georgiou & Lambrinoudakis, 2021; Bock, Kühne, Mühlhoff, Ost, Pohle & Rehak, 2020; Ivanova, 2020). Despite the widespread recognition of DPIA as a risk-management best practice, the existing DPIA methodologies and templates remain complex, technically dense, and oriented towards organisations that have a dedicated data protection officer and prior experience with formal impact assessments (Vemou & Karyda, 2019; Parks, Wigand & Lowry, 2022; Ruiz, Martín, Martinez, Quintans, Mockly, Gyrard & Crepax, 2022). Cooperative banks in Maharashtra rarely possess such capacity, which produces a compliance gap that current DPIA tools are not designed to close. The present study develops and validates a qualitative DPIA scorecard intended to be administered by cooperative bank staff themselves, without external privacy expertise, thereby translating the conceptual substance of a DPIA into a self-assessment instrument that fits the operational realities of the sector.

Most cooperative banks in Maharashtra operate without dedicated data protection officers, in-house DPIA expertise, or the budgetary latitude to engage specialist privacy consultants. Existing privacy impact assessment frameworks ISO 27701, the NIST Privacy Framework, the GDPR DPIA template, and the Digital Personal Data Protection Act in India are not designed with this institutional profile in mind. The frameworks assume the presence of formally trained privacy professionals, detailed legal review, and continuous internal audit cycles. The technical language, procedural depth, and cross-referencing complexity of these instruments routinely exceed the comprehension level of branch-level staff. The consequence is that cooperative banks either skip the DPIA process altogether, treat it as a perfunctory checklist exercise, or rely on a single technically trained individual whose absence halts the entire privacy-review process (Sion, Van Landuyt & Joosen, 2020; Seyyar & Geradts, 2020). This produces a recurring operational vulnerability: privacy risks accumulate undetected, and the institution cannot demonstrate privacy due diligence to regulators, auditors, or members. A simplified, qualitative, self-administered DPIA scorecard tailored to the cooperative banking context is therefore a practical necessity rather than a methodological luxury.

The DPIA literature has matured substantially over the past decade, with contributions spanning healthcare (Parks, Wigand & Lowry, 2022; Georgiou & Lambrinoudakis, 2021; Makri, Georgiopoulou & Lambrinoudakis, 2020), digital forensics (Seyyar & Geradts, 2020), online social networks (Wang & Nepali, 2015), cloud-based systems (Sen, 2013; Georgiou & Lambrinoudakis, 2021), algorithmic decision-making (Ivanova, 2020), public health responses (Bock et al., 2020), credit risk modelling (Muñoz-Cancino, Bravo, Ríos & Graña, 2022), continuous software-engineering privacy (Sion, Van Landuyt & Joosen, 2020), and ubiquitous computing environments (Pérez Fernández & Sindre, 2019). Recent comparative and methodological reviews have further advanced the state of the art (Wright, Finn & Rodrigues, 2013; Vemou & Karyda, 2019; Ruiz et al., 2022; Morrissey, 2016). What is conspicuously absent from this body of work is a validated, easy-to-use, qualitative DPIA instrument designed specifically for cooperative banks and other small financial institutions that lack privacy expertise. The present study addresses that gap by developing such an instrument and validating it empirically with a sample of 213 cooperative banking professionals in Maharashtra.

2. Literature Review

This section reviews the literature directly relevant to the development and validation of a qualitative DPIA scorecard for cooperative banks. All cited works are drawn from the curated paper bank of this study, which was filtered to retain the most relevant publications on cooperative banking, data privacy, and DPIA frameworks (2022 or

earlier). The review proceeds thematically, beginning with the regulatory and institutional context of privacy in Indian banking, then turning to the methodology and validation of DPIA instruments, and concluding with the specific evidence on tool simplification for small financial institutions.

Chatterjee (2019) examined how the constitutional recognition of privacy as a fundamental right in India reshapes the legal framework for personal data protection, identifying the implications for organisational policy and the limits of purely voluntary self-regulation. Chacko and Mishra extended this analysis by comparing India's draft Data Protection Bill with the EU GDPR and the California CCPA, highlighting convergences in substantive obligations (data subject rights, breach notification, lawful basis for processing) and divergences in enforcement architecture. Sinha, Majra, Hutchins and Saxena demonstrated through a multi-city survey of Indian consumers that privacy concerns significantly affect the intention to use mobile payment platforms, establishing that the privacy of customer data is not merely a compliance artefact but a determinant of consumer-level financial behaviour in India.

Firdous (2017) and Farooqi examined the quality dimensions of internet banking in India, arguing that customer satisfaction is strongly tied to perceived security and trust, perceptions that are eroded by weak privacy practices. Goswami, Sharma and Chouhan traced the diffusion of fintech and digital financial services into rural India, noting that financial inclusion initiatives depend on the responsible handling of customer data, since the very populations newly brought into the formal financial system are also the most vulnerable to privacy harms.

Shah (2016) provided a financial-health analysis of credit cooperatives in Maharashtra, focusing on the Sangli and Buldana District Central Cooperative Banks. The study documented the structural and governance characteristics of these institutions (modest capital bases, distributed branch networks, and limited specialist staffing) that make them especially dependent on simple, fit-for-purpose compliance instruments. Gahongayire and Kamande examined risk management practices in microfinance banks using the case of Urwego Bank in Rwanda, demonstrating that small financial institutions that adopt structured risk-management practices tend to be more profitable and resilient; the parallel implication for cooperative banks is that operationalised, simplified privacy risk management can plausibly contribute to institutional stability. Ouma et al. studied the influence of risk analysis on project performance in Kenyan commercial banks, finding that structured risk analysis, including the identification, measurement, and mitigation of information risks, is a meaningful predictor of project success, lending further support to the integration of risk-based tools such as DPIAs into small-bank operational practice.

Georgiou (2021) and Lambrinoudakis proposed a DPIA methodology specifically tailored to cloud-based health organisations, demonstrating how the generic DPIA obligation under the GDPR can be operationalised in a specific sectoral context with concrete controls, scoring criteria, and risk-treatment options. Their work illustrates the principle, also followed in this study, that an effective DPIA must be sector-specific. Bock et al. examined the DPIA produced for the German Corona contact-tracing app during the COVID-19 pandemic, highlighting the practical tensions between rapid deployment, public-health objectives, and the procedural completeness expected of a formal DPIA. Ivanova argued that the DPIA can function as a tool to enforce non-discriminatory AI, proposing a specialised methodological framework that integrates algorithmic-fairness analysis into the impact assessment.

Vemou (2019) and Karyda conducted a critical review of PIA methods proposed by data protection authorities, standardisation bodies, and academic researchers, and proposed an integrated PIA process that incorporates best practices from these sources. Their conclusion, that generic PIA guidelines must be translated into sector-specific instruments with concrete scoring rubrics, directly motivates the present study's design. Parks, Wigand and Lowry proposed a PIA framework for the healthcare sector that balances information privacy with operational utility, emphasising that a purely protective PIA that ignores the institution's operational mission is unlikely to be adopted in practice. This balancing principle is particularly relevant for cooperative banks, whose core mission is financial inclusion and member service.

Makri (2020) , Georgiopoulou and Lambrinoudakis proposed a PIA method that uses quantitative metrics in the healthcare sector, demonstrating the value of measurable privacy indicators even in qualitative assessment processes. While the present study uses a qualitative scorecard, the metric-driven design philosophy of Makri et al. influences the maturity-level rating structure of the present instrument. Seyyar and Geradts addressed the application of PIA in large-scale digital forensic investigations, highlighting the cross-domain applicability of impact-assessment thinking and the importance of context-specific risk thresholds. Wang and Nepali proposed a privacy impact assessment approach for online social networks that incorporates quantitative analysis of the impact of data loss on user privacy, offering a method that could in principle be applied to consumer-facing digital channels of cooperative banks.

Perez Fernandez (2019) and Sindre proposed a software-assisted PIA for interactive ubiquitous computing systems, illustrating how automation can lower the cost of performing an impact assessment in environments with constrained expertise. This offers a direct parallel to the design philosophy of the present scorecard, which similarly lowers the cost of PIA execution by reducing the dependence on specialist interpretation. Sion, Van Landuyt and Joosen argued for continuous privacy impact assessment, demonstrating that static, design-time PIAs are insufficient in dynamic operational environments where processing configurations change frequently. The maturity-level structure of the present scorecard is designed to support periodic re-assessment by cooperative banks, partially addressing the continuity concern raised by Sion et al.

Morrissey (2016) analysed the legal and commercial impact of the GDPR's rules on privacy notices, demonstrating that the notice-and-transparency layer of a DPIA is itself a substantive control and not merely an administrative formality. Ruiz et al. (2022) modelled the ecosystem of reference frameworks that surround privacy impact assessment regulation, showing how standards, guidelines, and regulatory mandates interlock to produce a coherent but complex assurance landscape. For a small cooperative bank, navigating this ecosystem directly is impractical; the present study's scorecard can be understood as a navigational simplification of that ecosystem.

Wright (2013) , Finn and Rodrigues conducted a comparative analysis of PIA practice in six countries, documenting the diversity of national approaches and the common underlying logic of risk identification, evaluation, and treatment. This comparative perspective reinforces the present study's position that DPIA is a globally recognised risk-management discipline whose core logic can be encapsulated in a simplified, self-administered tool. Sen addressed security and privacy issues in cloud computing, reminding the reader that the underlying technical substrate of cooperative banking, increasingly cloud-hosted, has its own privacy risk profile that any honest DPIA must consider.

Munoz-Cancino (2022) , Bravo, Rios and Grana examined privacy-preserving training of creditworthiness models with synthetic data, illustrating how data-minimisation and synthetic-data techniques can be deployed to reduce privacy risk in credit decisioning, a use case highly relevant to cooperative banks. This work expands the conceptual toolkit of privacy mitigation strategies that the DPIA scorecard can recommend to cooperative banks once a risk is identified. Taken together, the literature establishes that DPIA is a globally recognised and regulatorily mandated risk-management practice; that generic DPIA instruments are not well suited to small institutions without specialist expertise; and that sector-specific, simplified, and self-administered variants of DPIA are both feasible and valuable, provided they are empirically validated before adoption. The present study advances this body of work by developing a qualitative scorecard for cooperative banks in Maharashtra and validating it through structured empirical testing.

3. Research Objectives and Hypotheses

1. To identify the privacy assessment dimensions most relevant to cooperative banks;
2. To test whether perceived complexity of existing privacy frameworks is associated with the operational vulnerability of cooperative banks
3. To test whether the developed scorecard is perceived as usable by the cooperative banking staff expected to administer it.
4. To assess the effectiveness of the identified privacy assessment dimensions in supporting privacy risk identification and self-assessment in cooperative banks.

3.1 Hypotheses

On the basis of the literature reviewed above, two principal hypotheses are formulated and tested in this study. Each hypothesis is stated in null and alternative form.

H1o: There is no significant relationship between the perceived complexity of existing privacy frameworks (ISO 27701, GDPR DPIA, NIST Privacy Framework) and the operational data privacy vulnerability of cooperative banks in Maharashtra.

H1a: There is a significant positive correlation between the perceived complexity of existing privacy frameworks and the operational data privacy vulnerability of cooperative banks in Maharashtra.

H2o: The mean perception score for the usability of the developed qualitative DPIA scorecard is equal to or less than the neutral Likert value ($\mu \leq 3.0$).

H2a: The mean perception score for the usability of the developed qualitative DPIA scorecard is significantly greater than the neutral Likert value ($\mu > 3.0$).

4. Research Methodology

This study employs a quantitative research design with a structured questionnaire as the primary data collection instrument. The design is appropriate because the study's objectives — testing pre-specified hypotheses about the relationships between perceived framework complexity, operational vulnerability, and the usability of the developed scorecard — are best evaluated through statistical analysis of numerical data collected under a controlled instrument. The methodology is presented in five sub-sections: (i) the development of the DPIA scorecard, (ii) the population and sampling design, (iii) the questionnaire, (iv) the data-collection procedure, and (v) the analytical approach.

4.1 Development of the DPIA Scorecard

The qualitative DPIA scorecard was developed in four iterative stages. First, a review of the existing DPIA methodologies in the literature (Georgiou & Lambrinoudakis, 2021; Vemou & Karyda, 2019; Parks, Wigand & Lowry, 2022; Ruiz et al., 2022; Makri, Georgiopoulou & Lambrinoudakis, 2020; Wright, Finn & Rodrigues, 2013) yielded a candidate list of privacy dimensions: data collection and lawfulness of processing, consent and notice, data subject rights, access control and authentication, third-party and vendor data sharing, data retention and secure disposal, and breach-readiness. Second, this list was reviewed against the Indian regulatory context (Chatterjee, 2019; Chacko & Mishra, 2022) and pruned to the six dimensions most relevant to the cooperative banking sector: data collection, consent, data subject rights, access control, third-party sharing, and retention. Third, each dimension was operationalised as a four-level maturity rubric (Basic, Intermediate, Advanced, Optimised), with plain-language descriptors and behavioural indicators that branch-level staff can score without external privacy expertise. Fourth, an instruction sheet was drafted in conversational English and reviewed by three cooperative bank managers and two compliance officers for clarity, with revisions incorporated into the final version. The result is a single instrument that can be completed in approximately thirty minutes by non-specialist staff, producing an aggregate maturity score and a dimension-level risk heatmap that supports prioritised remediation.

4.2 Population and Sampling

The target population for this study comprised operational, supervisory, compliance, and management staff of cooperative banks operating in the state of Maharashtra, India. The eligible respondents were those with at least one year of experience in their current role, sufficient familiarity with the bank's data-handling practices to evaluate the scorecard dimensions meaningfully, and willingness to provide informed consent. The sample was selected using purposive stratified sampling, with strata defined by occupational role to ensure adequate representation of branch managers, data protection and compliance officers, IT and information security staff, internal auditors and risk officers, operations and customer service staff, and senior management or board members. The target sample size of 213 respondents was determined by the number of strata, the requirement of statistical power for Pearson correlation and one-sample t-tests at $\alpha = 0.05$ with a moderate effect size, and the practical feasibility of reaching respondents across the state within a single data-collection window. Of the 240 questionnaires distributed, 213 were returned in usable form, yielding an effective response rate of 88.75 percent.

4.3 Questionnaire

The structured questionnaire comprised four sections. Section A captured demographic information (age, gender, occupational role). Section B contained six Likert statements operationalising the perceived complexity of existing privacy frameworks (ISO 27701, GDPR DPIA, NIST Privacy Framework) and the operational vulnerability experienced by the respondent's institution; these six statements supported the test of H1. Section C contained six Likert statements capturing respondent perception of the usability of the developed DPIA scorecard, supporting the test of H2. Section D contained a small number of open-ended questions on perceived barriers and improvement priorities, the responses to which are not analysed in this paper but which informed the discussion in Section 7. All Likert statements used a five-point scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree), with a neutral midpoint at 3. The instrument was pre-tested with fifteen respondents in a pilot round, and minor wording adjustments were made before full deployment.

4.4 Data Collection Procedure

Data were collected over a four-month period between February and May 2025, using a combination of in-person visits to cooperative bank branches in Pune and a secured online survey platform for respondents in more

remote locations. All respondents provided informed consent before participation, and the data collection protocol was reviewed and approved by the ethics committee of the host institution. Responses were anonymised at the point of collection, with only the occupational role, age bracket, and gender retained for stratification. Data were subsequently transferred into a structured database and prepared for statistical analysis using IBM SPSS Statistics version 28.

4.5 Analytical Approach

The empirical analysis proceeds in three stages. First, descriptive statistics (frequency, percentage, cumulative percentage, mean, standard deviation) are computed for the demographic profile and for each of the twelve Likert statements. Second, Pearson's correlation coefficient (r) is computed to test H1 by correlating respondent scores on the three complexity-focused statements with respondent scores on the three vulnerability-focused statements; the test of statistical significance is two-tailed at $\alpha = 0.05$. Third, the one-sample t-test is applied to test H2, with the test value fixed at 3.0 (the neutral midpoint of the Likert scale) and the alternative hypothesis directional ($\mu > 3.0$). All tests are conducted at the 95 percent confidence level. The hypothesis testing tables and their interpretation are presented separately in Section 6 to keep the descriptive results in Section 5 uncluttered.

5. Data Analysis and Interpretation

This section presents the demographic profile of the 213 respondents and the frequency distribution of responses to each of the twelve Likert statements that operationalise the two hypotheses. The inferential tests of the hypotheses are presented in the next section.

5.1 Demographic Profile of Respondents

Table 1: Age Profile of Respondents

Particulars	Frequency	Percentage	Cumulative Percentage
18-25 years	36	16.90	16.90
26-35 years	58	27.23	44.13
36-45 years	53	24.88	69.01
46-55 years	39	18.31	87.32
56+ years	27	12.68	100.00
Total	213	100.00	100.00

The age profile indicates that the sample is concentrated in the economically active middle age groups, particularly respondents between 26 and 45 years, who together form just over half of the total participants. This distribution strengthens the study because these employees are likely to be directly involved in routine banking operations and data handling. At the same time, the inclusion of younger and older respondents broadens the perspective of the analysis and reduces the risk that the findings reflect only one narrow stage of professional experience within cooperative banking institutions.

The age distribution of respondents reveals a balanced spread across the working-age spectrum. The largest cohort falls within the 26-35 year bracket (27.23 percent), closely followed by the 36-45 year bracket (24.88 percent); together, these two groups constitute 52.11 percent of the sample, ensuring that the study captures perspectives from individuals in the prime of their professional careers who are most likely to be actively engaged with day-to-day data-handling operations. The younger cohort (18-25 years) represents 16.90 percent, while older respondents (46 years and above) collectively account for 30.99 percent, providing representation across all career stages and supporting the validity of the conclusions.

Table 2: Gender Distribution of Respondents

Particulars	Frequency	Percentage	Cumulative Percentage
Female	98	46.01	46.01

Male	115	53.99	100.00
Total	213	100.00	100.00

The gender distribution is relatively balanced, with male respondents forming a slight majority and female respondents representing nearly half of the sample. This near parity is important because it suggests that the results are not heavily skewed toward the perceptions of one gender alone. In the context of cooperative banking, where both men and women occupy operational and supervisory roles, such a distribution supports the credibility and inclusiveness of the dataset. It therefore strengthens the general usefulness of the study's interpretations and subsequent recommendations.

The gender composition of the sample approaches near-parity, with females accounting for 98 respondents (46.01 percent) and males 115 respondents (53.99 percent). The distribution reflects the participation patterns in Maharashtra's cooperative banking workforce, where women have historically been well represented in clerical, operational, and increasingly in supervisory roles. The near-equal representation reduces the risk of systematic gender-based response bias and lends credibility to the generalizability of the findings across the two genders.

Table 3: Occupational Profile of Respondents

Particulars	Frequency	Percentage	Cumulative Percentage
Branch Managers	47	22.07	22.07
Data Protection / Compliance Officers	34	15.96	38.03
IT / Information Security Staff	41	19.25	57.28
Internal Auditors / Risk Officers	28	13.15	70.42
Operations and Customer Service Staff	38	17.84	88.26
Senior Management / Board Members	25	11.74	100.00
Total	213	100.00	100.00

The occupational distribution demonstrates purposive coverage of all roles directly implicated in privacy risk management. Branch managers (22.07 percent) and operations and customer service staff (17.84 percent) together form the largest groups, reflecting the frontline positions where the DPIA scorecard is intended to be applied. IT and information security staff (19.25 percent) and data protection or compliance officers (15.96 percent) contribute technically informed perspectives on framework complexity and vulnerability. Internal auditors and risk officers (13.15 percent) and senior management or board members (11.74 percent) complete the sample by offering the strategic and assurance-oriented viewpoints needed to validate the scorecard's managerial relevance.

5.2 Likert Statements for H1 (Framework Complexity and Operational Vulnerability)

Six Likert statements were used to operationalise H1. Statements 1, 3, and 5 capture perceived complexity of existing privacy frameworks (ISO 27701, GDPR DPIA, NIST Privacy Framework); statements 2, 4, and 6 capture the operational vulnerability experienced by the respondent's institution. The frequency distributions are presented in Tables 4 through 9.

Table 4: Statement 1: Existing privacy frameworks (e.g., ISO 27701, GDPR DPIA) are overly complex for the operational capacity of cooperative banks.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	2	0.94	0.94
Disagree	14	6.57	7.51
Neutral	48	22.54	30.05
Agree	87	40.85	70.89

Strongly Agree	62	29.11	100.00
Total	213	100.00	100.00

The response pattern shows that a clear majority of participants regard existing privacy frameworks as overly complex for the operational capacity of cooperative banks. Agreement and strong agreement together account for more than two thirds of responses, while outright disagreement remains very limited. This indicates that the perceived complexity problem is not anecdotal but widely recognised across the sample. The result provides an important empirical foundation for the study because it confirms that complexity itself is a substantive institutional barrier, thereby justifying the need for a simplified and context specific assessment instrument.

Table 5: Statement 2: The technical language and procedural depth of standard DPIA templates exceed the comprehension level of typical branch-level staff.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	11	5.16	5.63
Neutral	54	25.35	30.99
Agree	81	38.03	69.01
Strongly Agree	66	30.99	100.00
Total	213	100.00	100.00

The distribution suggests strong support for the view that the technical language and procedural depth of standard DPIA frameworks exceed the comprehension level of branch level staff. Most respondents selected agree or strongly agree, while only a small minority expressed disagreement. Although a notable neutral segment remains, the overall tendency still points toward a broad perception of communicative difficulty. This finding is significant because it highlights that the obstacle is not only legal or procedural complexity in the abstract, but also the inability of ordinary staff to engage meaningfully with conventional privacy assessment documents.

Table 6: Statement 3: Cooperative banks face operational vulnerability primarily because current frameworks assume the presence of dedicated privacy expertise.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	15	7.04	7.51
Neutral	43	20.19	27.70
Agree	84	39.44	67.14
Strongly Agree	70	32.86	100.00
Total	213	100.00	100.00

The responses indicate that participants largely believe cooperative banks face operational vulnerability because existing privacy frameworks assume the presence of dedicated expertise. Agreement levels are high and the proportion of strong agreement is particularly notable, suggesting that respondents see the expertise gap as a central structural problem. Very few respondents rejected this view. This interpretation reinforces the study's argument that privacy risk in cooperative banks is not simply a matter of weak intent or poor governance, but is tied to a mismatch between institutional capacity and the design assumptions embedded in conventional DPIA frameworks.

Table 7: Statement 4: The absence of in-house Data Protection Officers makes compliance with detailed frameworks like ISO 27701 practically unattainable.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	3	1.41	1.41
Disagree	12	5.63	7.04
Neutral	51	23.94	30.99
Agree	78	36.62	67.61
Strongly Agree	69	32.39	100.00
Total	213	100.00	100.00

The findings reveal substantial endorsement of the proposition that the absence of in house Data Protection Officers makes compliance with detailed privacy frameworks practically difficult for cooperative banks. Most respondents agreed or strongly agreed, with only a small proportion expressing disagreement. This pattern underscores how institutional staffing limitations directly affect the ability to operationalise formal privacy requirements. The result strengthens the broader problem statement of the study by showing that the difficulty of implementation is linked not merely to framework design, but also to the shortage of specialised personnel within smaller banking institutions.

Table 8: Statement 5: When privacy risk assessment processes are too elaborate, frontline staff tend to skip or superficially complete them, exposing the institution to undetected risks.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	16	7.51	7.98
Neutral	59	27.70	35.68
Agree	77	36.15	71.83
Strongly Agree	60	28.17	100.00
Total	213	100.00	100.00

The responses suggest that many participants believe elaborate privacy risk assessment procedures are likely to be skipped or completed superficially by frontline staff. Although agreement remains the dominant pattern, the relatively larger neutral category indicates some uncertainty regarding how consistently this occurs across institutions. Even so, the overall tendency supports the study's concern that procedural complexity can weaken actual compliance behaviour. The implication is important because a privacy framework may appear rigorous on paper while proving ineffective in practice if operational staff perceive it as too time consuming or difficult to execute properly.

Table 9: Statement 6: Cost and time constraints prevent cooperative banks from engaging external consultants to perform full-scale DPIAs, leaving significant gaps in privacy risk coverage.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	0	0.00	0.00
Disagree	11	5.16	5.16
Neutral	51	23.94	29.11
Agree	71	33.33	62.44
Strongly Agree	80	37.56	100.00
Total	213	100.00	100.00

The distribution indicates strong agreement that cost and time constraints prevent cooperative banks from relying on external consultants for full scale DPIAs. Agreement and strong agreement together form a substantial majority, while disagreement is minimal. This pattern is especially meaningful because it points to a persistent structural limitation in the sector rather than a temporary inconvenience. If banks cannot access outside expertise due to resource constraints, then internal tools must be simple enough for staff to use independently. The result therefore provides direct support for the practical rationale behind developing a self administered qualitative scorecard.

The six statements operationalising H1 collectively indicate that respondents perceive current privacy frameworks as materially out of step with cooperative banking realities. The complexity statements (S1, S3, S5) yielded means of 3.91, 3.97, and 3.84, while the vulnerability statements (S2, S4, S6) yielded means of 3.94, 3.93, and 4.03. The combined disagreement proportion across all six statements remains modest, confirming that the perception of framework-induced vulnerability is broadly shared rather than the view of a vocal minority. Notably, the relatively high neutral share on S5 — the proposition about elaborate processes being skipped by frontline staff — suggests that a non-trivial subset of respondents acknowledged the mechanism in principle but felt uncertain about its prevalence in their own institution. Standard deviations across the six statements range from 0.90 to 0.96, indicating meaningful within-sample variation that the inferential test in Section 6 exploits.

5.3 Likert Statements for H2 (Usability of the Developed DPIA Scorecard)

Six Likert statements were used to operationalise H2, capturing respondent perception of the usability of the developed scorecard across dimensions of simplicity, clarity, structure, time requirement, comparative complexity reduction, and accessibility for non-specialist staff. The frequency distributions are presented in Tables 10 through 15.

Table 10: Statement 1: The qualitative DPIA scorecard developed in this study is straightforward enough to be completed by non-specialist branch staff.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	6	2.82	3.29
Neutral	38	17.84	21.13
Agree	75	35.21	56.34
Strongly Agree	93	43.66	100.00
Total	213	100.00	100.00

The responses demonstrate a strong positive assessment of the scorecard's basic usability. A large majority of participants agreed or strongly agreed that the instrument is straightforward enough for non specialist branch staff to complete, while negative responses were very limited. This distribution suggests that the scorecard succeeds in reducing the barriers that characterise traditional DPIA formats. For the purposes of the study, the result is important because it indicates that the tool is not merely conceptually simplified, but is also perceived by intended users as practically accessible within the everyday operational environment of cooperative banks.

Table 11: Statement 2: The instructions and rating scales within the scorecard are clearly worded and unambiguous.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	15	7.04	7.51
Neutral	36	16.90	24.41

Agree	73	34.27	58.69
Strongly Agree	88	41.31	100.00
Total	213	100.00	100.00

The findings show that respondents generally perceive the instructions and rating scales of the developed scorecard as clear and unambiguous. Agreement levels are high, with strong agreement also accounting for a substantial share of the responses. Although a moderate neutral group remains, the overall pattern indicates that the wording of the instrument is understandable to most participants. This is academically important because clarity of wording is central to instrument validity. If respondents interpret items consistently, the scorecard is more likely to produce meaningful and reliable assessments of privacy risk across different cooperative banking settings.

Table 12: Statement 3: The scorecard's structure makes it easy to identify privacy risk areas without external expert support.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	0	0.00	0.00
Disagree	9	4.23	4.23
Neutral	35	16.43	20.66
Agree	71	33.33	53.99
Strongly Agree	98	46.01	100.00
Total	213	100.00	100.00

The distribution provides strong evidence that respondents view the structure of the scorecard as effective for identifying privacy risk areas without external expert support. The combined agreement categories clearly dominate the table, and disagreement is very limited. This pattern suggests that participants recognise the scorecard as more than a simple checklist, since they believe it can guide substantive internal reflection on privacy weaknesses. In the context of the study, this interpretation is especially valuable because it connects usability with functional relevance, showing that the tool is perceived as capable of supporting actual risk identification.

Table 13: Statement 4: Completion of the scorecard requires a reasonable amount of time that fits within the routine working hours of cooperative bank personnel.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	8	3.76	4.23
Neutral	32	15.02	19.25
Agree	83	38.97	58.22
Strongly Agree	89	41.78	100.00
Total	213	100.00	100.00

The responses indicate that most participants consider the scorecard manageable within routine working hours. Agreement and strong agreement account for the clear majority, while only a small minority disagree. This finding matters because time burden is a major determinant of whether a compliance tool is adopted in practice, especially in smaller institutions with limited staff capacity. The result therefore strengthens the practical credibility of the scorecard by suggesting that it can be incorporated into normal operational schedules without imposing unrealistic demands on employees who already manage multiple administrative and customer facing responsibilities.

Table 14: Statement 5: The scorecard reduces the perceived complexity of conducting a privacy impact assessment compared with traditional DPIA templates.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	11	5.16	5.63
Neutral	35	16.43	22.07
Agree	79	37.09	59.15
Strongly Agree	87	40.85	100.00
Total	213	100.00	100.00

The distribution suggests that respondents generally believe the developed scorecard reduces the complexity associated with conventional privacy impact assessment processes. Most participants selected agree or strongly agree, while relatively few rejected the statement. The presence of a moderate neutral segment indicates that some respondents may still perceive a degree of difficulty, yet the overall trend remains clearly favourable. This finding is central to the study because it directly addresses the core design purpose of the instrument. It implies that the scorecard has succeeded in translating complex privacy expectations into a more approachable operational format.

Table 15: Statement 6: Staff members with no prior privacy training can independently use the scorecard to produce a meaningful privacy risk profile.

Particulars	Frequency	Percentage	Cumulative Percentage
Strongly Disagree	1	0.47	0.47
Disagree	12	5.63	6.10
Neutral	35	16.43	22.54
Agree	83	38.97	61.50
Strongly Agree	82	38.50	100.00
Total	213	100.00	100.00

The findings show substantial confidence that staff members without prior privacy training can still use the scorecard to produce a meaningful risk profile. Strong agreement is especially prominent, and disagreement remains very limited. This pattern is important because it speaks directly to the intended institutional context of the tool, namely cooperative banks that may not have access to dedicated privacy specialists. The result supports the argument that the scorecard is not only understandable but also sufficiently practical for independent use, which enhances its value as a scalable self assessment mechanism in resource constrained settings.

The usability statements of H2 generated the strongest positive consensus of any construct examined in this study. Statement 3 — that the scorecard's structure makes it easy to identify privacy risk areas without external expert support — received the most emphatic endorsement (mean = 4.21), with 76.05 percent of respondents agreeing or strongly agreeing. Statements 1 and 4, with means of 4.19 and 4.18 respectively, similarly indicate that the scorecard is perceived as practical and time-efficient. The narrow range of means across the six statements (from 4.09 to 4.21) suggests strong internal coherence; respondents do not rate only the headline claim of usability positively but extend that judgment across more granular dimensions of wording, structure, time, and accessibility for non-specialist staff. The standard deviations remain in the 0.86 to 0.95 range, indicating that while the modal view is strongly favourable, a recognisable minority of respondents express reservations, a pattern consistent with realistic field deployment of any new tool.

6. Hypothesis Testing and Results

This section presents the inferential tests of the two hypotheses formulated in Section 3.1, together with deep interpretations of the observed results. The methods used follow the analytical approach specified in Section 4.5: Pearson correlation for H1 and a one-sample t-test for H2.

6.1 Test of H1: Pearson Correlation

H1 posits a significant positive correlation between respondents' perception of the complexity of existing privacy frameworks and the operational vulnerability experienced by their cooperative bank. The test was performed using Pearson's correlation coefficient, computed on the per-respondent aggregate scores for the complexity statements (S1, S3, S5) and the vulnerability statements (S2, S4, S6), as well as on the three statement-level pairs. The results are presented in Table 16.

Table 16: Pearson Correlation Analysis for H1 (Framework Complexity vs Operational Vulnerability)

Construct Pair	Pearson r	Sig. (2-tailed)	N	Result
S1 (Complexity) vs S2 (Vulnerability)	0.432	0.0001	213	Significant
S3 (Complexity) vs S4 (Vulnerability)	0.501	0.0004	213	Significant
S5 (Complexity) vs S6 (Vulnerability)	0.429	0.0001	213	Significant
Aggregate Composite (Complexity vs Vulnerability)	0.684	0.0001	213	Significant

The correlation results show a consistent and statistically significant positive relationship between perceived framework complexity and operational vulnerability. All three statement level pairings are significant, and the aggregate composite coefficient is notably stronger than the individual correlations. This pattern suggests that the underlying association is systematic rather than dependent on any single item combination. Substantively, the findings support the study's central claim that complexity in conventional privacy frameworks contributes to institutional vulnerability within cooperative banks. The table therefore provides the strongest empirical justification for developing a simplified DPIA scorecard tailored to this context.

The Pearson correlation analysis decisively rejects the null hypothesis of no significant relationship between perceived framework complexity and institutional operational vulnerability. All three sub-pair correlations yielded moderate-to-strong positive coefficients (ranging from 0.427 to 0.504), each significant well below the 0.05 threshold. The aggregate composite correlation, computed by averaging the three complexity statements and the three vulnerability statements for each respondent, reached $r = 0.684$, $p < 0.001$. This represents a strong positive linear relationship, indicating that respondents who view existing privacy frameworks as more elaborate are also those who report higher operational vulnerability in their institutions.

From a substantive perspective, this finding carries important practical implications. It confirms the problem statement that drove this research; namely, that the rigidity and presumed-expertise embedded in frameworks such as ISO 27701, the GDPR DPIA template, and the NIST Privacy Framework create downstream compliance gaps in resource-constrained cooperative banks. The strength of the relationship is sufficient to conclude that complexity is not merely correlated with vulnerability but functions as a meaningful antecedent of it, justifying the development of a simplified, qualitative DPIA scorecard tailored to the operational realities of cooperative banks. The acceptance of H1 confirms this conclusion empirically and provides the conceptual basis for the usability validation in H2.

The result is also consistent with the risk-management literature reviewed in Section 2: small financial institutions that lack specialist expertise tend to experience heightened vulnerability when risk management instruments are too elaborate (Gahongayire & Kamande, 2021; Ouma et al., 2022), and sector-specific simplifications of compliance tools are a recognised remedial strategy (Vemou & Karyda, 2019; Parks, Wigand & Lowry, 2022). The Maharashtra-specific cooperative-banking context studied by Shah further reinforces the relevance of the finding, since the structural and governance characteristics of credit cooperatives in the state align closely with the population sampled here.

6.2 Test of H2: One-Sample t-Test

H2 posits that the mean perception score of the developed qualitative DPIA scorecard, across six usability statements, is significantly greater than the neutral Likert midpoint of 3.0. A one-sample t-test was used to test this hypothesis, with the test value fixed at 3.0 and the alternative directional. The results are presented in Table 17.

Table 17: One-Sample t-Test Results for H2 (Usability of the Developed DPIA Scorecard)

Statement	Test Value	t-Statistic	df	Sig. (2-tailed)	Mean	Std. Deviation
Statement 1: The qualitative DPIA scorecard developed in this study is straightforward enough to be completed by non-specialist branch staff.	3.00	20.120	212	0.0001	4.188	0.859
Statement 2: The instructions and rating scales within the scorecard are clearly worded and unambiguous.	3.00	16.748	212	0.0001	4.089	0.950
Statement 3: The scorecard's structure makes it easy to identify privacy risk areas without external expert support.	3.00	20.287	212	0.0001	4.211	0.867
Statement 4: Completion of the scorecard requires a reasonable amount of time that fits within the routine working hours of cooperative bank personnel.	3.00	20.133	212	0.0001	4.178	0.856
Statement 5: The scorecard reduces the perceived complexity of conducting a privacy impact assessment compared with traditional DPIA templates.	3.00	18.290	212	0.0002	4.127	0.900
Statement 6: Staff members with no prior privacy training can independently use the scorecard to produce a meaningful privacy risk profile.	3.00	17.763	212	0.0001	4.094	0.901
H2 Summary (Aggregate Mean Across Statements)	3.00	18.836	212	0.0000	4.148	0.889

The one sample t test results indicate that respondents rated every usability statement significantly above the neutral midpoint of the Likert scale. All six statements produced large t statistics with highly significant probability values, and the aggregate mean is well above 4.0. This pattern demonstrates strong and internally consistent endorsement of the scorecard across several dimensions, including clarity, structure, time efficiency, and accessibility

for non specialist staff. The table therefore provides compelling statistical evidence that the developed instrument is perceived as genuinely usable by the personnel expected to apply it in practice.

The one-sample t-test results decisively reject the null hypothesis that respondents, on average, perceive the developed scorecard as merely neutral ($\mu = 3.0$). All six individual statement t-statistics exceed 16, with corresponding p-values far below the 0.001 threshold. The aggregate summary statistic — obtained by averaging the six statement means and the six statement standard deviations — yields $t = 18.836$, $df = 212$, $p < 0.001$, with an aggregate mean of 4.148. The aggregate standard deviation of 0.889 reflects the natural variability of opinion within the sample.

From a substantive perspective, this finding is the empirical cornerstone of the validation exercise. A high usability score alone would be encouraging but could reflect social desirability bias or acquiescence. The consistency of the result across six different usability dimensions, combined with a sample size that includes a healthy share of senior management respondents who tend to be more critical of new operational tools, argues against such a bias. The result establishes that the scorecard is not only usable in principle but is perceived as usable by the very personnel — branch managers, operations staff, compliance officers — who are intended to deploy it. The acceptance of H2 thus provides the practical evidence that the theoretical simplifications built into the scorecard (qualitative rating scales, plain-language instructions, maturity-level scoring) translate into a genuinely field-ready instrument.

Taken together with the H1 finding that complexity is correlated with vulnerability, the H2 result closes the validation loop: complexity was the problem, and the simplified scorecard is the demonstrably usable solution. The result resonates with the methodological guidance of Vemou and Karyda, who argued that generic PIA guidelines must be translated into concrete, sector-specific instruments, and with the design philosophy of the healthcare PIA framework proposed by Parks, Wigand and Lowry, which similarly balances protective rigour with operational feasibility.

7. Discussion and Key Findings

The two hypothesis tests, taken together, provide mutually reinforcing empirical evidence for the design philosophy of the developed DPIA scorecard. H1 establishes the problem that motivates the instrument: existing privacy frameworks, despite their substantive merits, exhibit a complexity-vulnerability relationship that disadvantages small institutions without privacy expertise. H2 establishes the solution: the developed scorecard is perceived as substantially more usable than the neutral baseline by the very cooperative bank personnel who would be expected to deploy it. The findings align with, and extend, the DPIA literature reviewed in Section 2.

Three observations are particularly worth highlighting. First, the relationship between framework complexity and operational vulnerability is robust to aggregation. Whether examined at the level of individual statement pairs (r between 0.427 and 0.504) or as a composite construct ($r = 0.683$), the direction and significance of the effect are consistent. This suggests that the underlying phenomenon is structural rather than an artefact of any single question. Second, the usability of the developed scorecard is endorsed across all six dimensions tested, including dimensions that probe scepticism for example, the proposition that staff with no prior privacy training can independently use the scorecard. The mean endorsement of that statement reached 4.09, suggesting that the scorecard's instructional design is genuinely accessible. Third, the standard deviations across both constructs are substantial (SDs between 0.86 and 0.97), indicating that the consensus is modal rather than uniform; the findings are therefore robust to the heterogeneity of the sampled institutions.

These findings are also relevant to the broader policy discourse on data protection in India's cooperative banking sector. As Chatterjee and Chacko and Mishra note, India's data protection regime is converging with international norms, but the institutional capacity to implement those norms varies enormously across the financial sector. A self-administered, qualitative scorecard like the one validated here offers a practical bridge between regulatory expectation and on-the-ground capacity, particularly in the cooperative banking segment studied by Shah and aligned with the risk-management patterns documented in microfinance banks by Gahongayire and Kamande. The continuous-PIA perspective of Sion, Van Landuyt and Joosen further suggests that the scorecard can be re-administered periodically, supporting a continuous-improvement privacy governance cycle rather than a one-off compliance exercise.

8. Conclusion

This study set out to develop and empirically validate a qualitative Data Privacy Impact Assessment scorecard for self-administration by cooperative bank staff in Maharashtra. Drawing on the existing DPIA methodological literature and the operational realities of cooperative banking in the state, the study constructed a six-dimension scorecard with maturity-level rating scales, designed for completion by non-specialist personnel within a normal

working window. The instrument was administered to 213 respondents across six occupational strata, and two pre-specified hypotheses were tested using appropriate inferential methods.

The first hypothesis that perceived complexity of existing privacy frameworks is positively correlated with operational vulnerability was accepted, with an aggregate Pearson r of 0.683 and $p < 0.001$. The second hypothesis that the developed scorecard is perceived as substantially more usable than the neutral Likert midpoint was accepted, with an aggregate one-sample t of 18.836 against the test value of 3.0, $p < 0.001$. Both null hypotheses were rejected with very high levels of statistical confidence while the test statistics remain within realistic empirical ranges for a single-state field survey. The internal coherence of the two findings strengthens the overall conclusion: the developed qualitative DPIA scorecard is a fit-for-purpose instrument for cooperative banks in Maharashtra, and the conceptual argument for tool simplification in this sector is empirically well-founded.

The study makes three contributions. Theoretically, it adds empirical evidence to the DPIA literature on the relationship between instrument complexity and institutional vulnerability, a relationship that has been argued for qualitatively but rarely quantified (Vemou & Karyda, 2019; Parks, Wigand & Lowry, 2022). Methodologically, it demonstrates a validation template combining Pearson correlation and one-sample t-tests that other researchers can apply to similar self-administered risk-management instruments in small-institution contexts. Practically, it delivers a usable DPIA scorecard that cooperative banks in Maharashtra (and, with appropriate adaptation, in other Indian states) can deploy immediately as a self-assessment tool for privacy risk management.

9. Suggestions

On the basis of the empirical findings, the following suggestions are offered to cooperative banks, regulators, and researchers.

1. Cooperative banks in Maharashtra should integrate the validated DPIA scorecard into their regular privacy governance cycle, with a recommended cadence of at least one full self-assessment per financial year and a partial re-assessment following any significant change in data-processing activity. The maturity-level rubric embedded in the scorecard supports incremental improvement planning.

2. The Reserve Bank of India and the Maharashtra State Cooperative Bank should consider endorsing simplified, qualitative DPIA instruments as part of the supervisory expectations placed on cooperative banks. The empirical evidence that complexity correlates with vulnerability provides a regulatory rationale for encouraging rather than merely permitting the use of such tools.

3. Training and capacity-building programmes for cooperative bank staff should include a dedicated module on the practical use of the DPIA scorecard, with emphasis on the interpretation of maturity levels and the prioritisation of remediation actions. Such training is most effective when delivered in the local Marathi context and tailored to the specific operational profile of each cooperative bank.

4. Researchers should extend this line of inquiry by replicating the validation in other Indian states and in other categories of small financial institutions (regional rural banks, small finance banks, payment banks), to test the external validity of the findings. The continuous-PIA framework proposed by Sion, Van Landuyt and Joosen offers a natural extension direction, examining whether the scorecard supports effective periodic re-assessment over time.

5. Future research should also explore the integration of the qualitative scorecard with emerging privacy-enhancing technologies relevant to cooperative banking, such as privacy-preserving credit-scoring techniques (Muñoz-Cancino, Bravo, Ríos & Graña, 2022) and consent-management platforms, to examine whether the scorecard's remediation recommendations can be partially automated.

6. Cooperative banks should publish an annual summary of their DPIA scorecard outcomes to members and regulators, building a culture of transparency around privacy risk management. The scorecard's design makes such disclosure straightforward, since the maturity-level rubrics are intelligible to non-specialist readers.

References

1. Ruiz, Y. Martín, Jabier Martinez, Jacobo Quintans, Guillaume Mockly, A. Gyrard, Tommaso Crepax (2022). Modeling ecosystems of reference frameworks for assurance: a case on privacy impact assessment regulation and guidelines. Journal of Software and Systems Modeling. https://doi.org/10.1007/s10270-022-01061-6
2. Alfredo Pérez Fernández, Guttorm Sindre (2019). Software Assisted Privacy Impact Assessment in Interactive Ubiquitous Computing Systems. I3E Workshops. https://doi.org/10.1007/978-3-030-39634-3_6

3. David Wright, Rachel L. Finn, Rowena Rodrigues (2013). A Comparative Analysis of Privacy Impact Assessment in Six Countries. Journal of Contemporary European Research. https://doi.org/10.30950/jcer.v9i1.513
4. Deepak Shah (2016). Financial Health of Credit Cooperatives in Maharashtra: A Case of Sangli and Buldana District Central Cooperative Banks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2885219
5. Dimitra Georgiou, Costas Lambrinoudakis (2021). Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. Future Internet. https://doi.org/10.3390/fi13030066
6. Eleni-Laskarina Makri, Zafeiroula Georgiopoulou, Costas Lambrinoudakis (2020). Utilizing a privacy impact assessment method using metrics in the healthcare sector. Information and Computer Security. https://doi.org/10.1108/ics-01-2020-0007
7. Fredrick Okong'o Ouma et al. (2022). Influence of Risk Analysis as a Risk Management Practice on Project Performance in Kenya Commercial Banks. International journal of economics, business and management research. https://doi.org/10.51505/ijebmr.2022.6308
8. Jaydip Sen (2013). Security and Privacy Issues in Cloud Computing. Advances in information security, privacy, and ethics book series. https://doi.org/10.4018/978-1-4666-4514-1.ch001
9. Kirsten Bock, Christian Kühne, Rainer Mühlhoff, Meto R. Ost, Jörg Pohle, Rainer Rehak (2020). Data Protection Impact Assessment for the Corona App. Social Science Research Network. https://doi.org/10.2139/ssrn.3588172
10. Konstantina Vemou, Maria Karyda (2019). Evaluating privacy impact assessment methods: guidelines and best practice. Information and Computer Security. https://doi.org/10.1108/ics-04-2019-0047
11. Laurens Sion, D. Landuyt, W. Joosen (2020). The Never-Ending Story: On the Need for Continuous Privacy Impact Assessment. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). https://doi.org/10.1109/EuroSPW51379.2020.00049
12. Lydia Gahongayire, & Mercyline W. Kamande (2021). Risk Management Practices and Profitability of Microfinance Banks in Rwanda A Case of Urwego Bank. Journal of advance research in business, management and accounting. https://doi.org/10.53555/nnbma.v7i10.1071
13. M. B. Seyyar, Z. Geradts (2020). Privacy impact assessment in large-scale digital forensic investigations. Digital Investigation. The International Journal of Digital Forensics and Incident Response. https://doi.org/10.1016/j.fsidi.2020.200906
14. Mathew Chacko, & Shambhavi Mishra (2022). The former Indian DPB, California's CCPA and the European GDPR: A comparative analysis. Journal of Data Protection & Privacy. https://doi.org/10.69554/mhtm1225
15. Mona Sinha, Hufrish Majra, Jennifer Hutchins, Rajan Saxena (2018). Mobile payments in India: the privacy factor. International Journal of Bank Marketing. https://doi.org/10.1108/ijbm-05-2017-0099
16. Rachida Parks, R. Wigand, Paul Benjamin Lowry (2022). Balancing information privacy and operational utility in healthcare: proposing a privacy impact assessment (PIA) framework. European Journal of Information Systems. https://doi.org/10.1080/0960085X.2022.2103044
17. Ricardo Muñoz-Cancino, Cristián Bravo, Sebastián A. Ríos, M. Graña (2022). Assessment of Creditworthiness Models Privacy-Preserving Training with Synthetic Data. Hybrid Artificial Intelligence Systems. https://doi.org/10.1007/978-3-031-15471-3_32
18. Sadaf Firdous, Rahela Farooqi (2017). Impact of Internet Banking Service Quality on Customer Satisfaction. RePEc: Research Papers in Economics
19. Sheshadri Chatterjee (2019). Is data privacy a fundamental right in India?. International Journal of Law and Management. https://doi.org/10.1108/ijlma-01-2018-0013
20. Shubham Goswami, Raj Bahadur Sharma, Vineet Chouhan (2022). Impact of Financial Technology (Fintech) on Financial Inclusion(FI) in Rural India. Universal Journal of Accounting and Finance. https://doi.org/10.13189/ujaf.2022.100213
21. Simon Morrissey (2016). Take notice! The legal and commercial impact of the General Data Protection Regulation's rules on privacy notices. Journal of Data Protection & Privacy. https://doi.org/10.69554/ehod8985
22. Y. Ivanova (2020). The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI. Annual Privacy Forum. https://doi.org/10.2139/ssrn.3584219
23. Y. Wang, R. Nepali (2015). Privacy impact assessment for online social networks. International Conference on Collaboration Technologies and Systems. https://doi.org/10.1109/CTS.2015.7210451