Journal of Enterprise Strategy & Management Innovation
Volume I, Issue 1, February 2026
https://journal.ijhba.com/index.php/jesmi
https://slsipress.com

IT Infrastructure and Data Privacy Practices in Manufacturing Companies

Lionell Somono[1], Dr. Marc Joseph Ian A. Generoso II, PhD[1]
[1]Lyceum of the Philippines University – Batangas
Corresponding Author: [1]lionellsomono@lpubatangas.edu.ph

Abstract

This study assessed the perceived IT infrastructure and data privacy practices of manufacturing companies in Batangas, and examined the association between IT infrastructure assessment and data privacy practices. A descriptive, cross-sectional survey design was employed, using a purposive sample of 200 owners, managers, or designated Data Protection Officers from Batangas-based manufacturing companies involved in personal data processing and in the application process for the National Privacy Commission Seal of Registration. A self-made questionnaire using a four-point Likert scale measured IT infrastructure in terms of scalability and performance, security and compliance, and cost and efficiency, and measured data privacy practices in terms of scope of application, rights of data subjects, and accountabilities of controllers. Reliability testing yielded acceptable to excellent internal consistency across subscales (Cronbach's alpha range: 0.714–0.923). Descriptive statistics (weighted mean and rank) indicated strong agreement across IT infrastructure dimensions (overall mean = 3.57) and across data privacy practices dimensions (overall mean = 3.62). Normality testing (Shapiro–Wilk) indicated non-normal distributions; thus, Spearman rho was used to test relationships. Results showed statistically significant positive associations between IT infrastructure dimensions and data privacy practices (rho = .531 to .821), indicating that higher IT infrastructure assessments were associated with stronger data privacy practice assessments. Findings support a focused action plan emphasizing scalable capacity, strengthened security controls, and cost-efficient optimization aligned with sustained privacy practice implementation.

Keywords: *IT infrastructure; data privacy practices; manufacturing companies; Batangas province; descriptive survey; Spearman rho; Data Protection Officer; data privacy compliance*

1. Introduction

Manufacturing companies increasingly depend on information systems to support production planning, inventory control, supply chain coordination, quality monitoring, customer servicing, and internal administration. As these systems expand, organizations also process larger volumes of personal information relating to employees, customers, suppliers, and other stakeholders. This operational reality places a dual requirement on firms: ensuring that IT infrastructure is sufficiently capable to sustain business operations, and ensuring that data privacy practices are implemented in a consistent and auditable manner.

In the Philippine context, organizational accountability for personal data processing has become a routine governance expectation rather than a purely technical concern. Data privacy practice implementation typically involves defined policies, role assignments, and control mechanisms such as access restriction, secure storage, retention and disposal procedures, monitoring, and breach preparedness. These requirements are not implemented in isolation. They depend on enabling conditions inside the organization, particularly the availability of infrastructure resources and security capabilities that support the effective execution of privacy-related controls. Where infrastructure capacity is constrained or uneven, privacy practices may be difficult to institutionalize; conversely, where infrastructure capability is strong, privacy practices may be more consistently implemented as part of normal operations.

This study is situated in Batangas province, where manufacturing firms operate within increasingly digitalized environments shaped by industrial clustering and data-dependent processes. As manufacturing organizations strengthen their digital operations, the managerial issue is no longer limited to whether information technology is used, but whether infrastructure capability aligns with the requirements of sustained privacy practice implementation. From a practical standpoint, this alignment matters for operational continuity, organizational risk control, and compliance readiness. From a research standpoint, it is useful to clarify whether infrastructure capability and privacy practice implementation move together in organizational assessments within this local manufacturing setting.

Prior organizational assessments often treat IT infrastructure performance and data privacy practices as separate concerns—one framed as operations and efficiency, and the other framed as compliance and governance. However, the two domains plausibly interact: privacy practice implementation tends to require reliable infrastructure capacity and security controls, while privacy obligations may also drive firms to improve monitoring, access management, and documentation. Establishing whether these domains are empirically associated in manufacturing companies provides an evidence base for prioritizing capability-building and for designing improvement plans that are traceable to measured organizational conditions.

Accordingly, the study examined manufacturing companies in Batangas province by assessing IT infrastructure in terms of scalability and performance, security and compliance, and cost and efficiency; determining data privacy practices in terms of scope of application, rights of data subjects, and accountabilities of controllers; and testing whether IT infrastructure assessment is associated with data privacy practice assessment among the participating firms.

2. Review of Related Literature

Digitalization in manufacturing increasingly depends on IT infrastructures that can sustain continuous operations while meeting governance expectations for responsible data handling. In practice, manufacturing firms manage interconnected systems—networks, servers, endpoints, applications, and cloud services—that support both operational workflows and the processing of personal information. Within this context, IT infrastructure can be conceptually examined through (a) scalability and performance, (b) security and compliance, and (c) cost and efficiency, while data privacy practices can be examined through (a) scope of application, (b) rights of data subjects, and (c) the accountabilities of controllers. The literature reviewed below develops four thematic strands: infrastructure readiness as capability, security and compliance as control capacity, privacy governance as organizational practice, and the infrastructure–privacy alignment as a socio-technical relationship that plausibly shapes privacy practice implementation (Liu & Li, 2024; Tehrani et al., 2024; Tang, 2024).

2.1 IT Infrastructure Readiness: Scalability and Performance as Capability Conditions

IT infrastructure readiness is commonly treated as a capability condition that enables organizations to deliver reliable digital services and to adapt when operational loads increase or fluctuate. Scalability, in particular, is frequently associated with the capacity to accommodate growth in users, transactions, and data volume without degradation in service quality, while performance is linked to responsiveness, throughput, and system stability under varying workloads (Liu & Li, 2024; Zhou et al., 2024). Within manufacturing settings, these requirements may be heightened because infrastructure supports time-sensitive processes such as production monitoring, inventory updates, procurement coordination, and quality documentation. When infrastructure cannot scale effectively, firms may experience bottlenecks that compromise data availability and integrity—conditions that also complicate controlled processing of personal information in routine operations (Balakrishnan et al., 2024).

Recent scholarship also frames infrastructure capability as an organizational resource whose value depends on architectural design and governance. Studies discussing modernization and digital transformation emphasize that scalable capacity is typically not achieved through simple expansion of hardware alone; rather, it is facilitated by modular architectures, virtualization, and cloud-based elasticity that allow resources to be provisioned and reconfigured as needs change (Assaye et al., 2024; Sumrit, 2024). This perspective implies that performance is not merely a technical outcome but a managed property arising from capacity planning, monitoring, and continuous improvement. Organizational analyses similarly highlight that infrastructure investments yield operational value when aligned with workflow design, user behavior, and managerial oversight, indicating that capability is distributed across technical systems and organizational routines (Chwiłkowska-Kubala et al., 2023), and strategic evaluation of firms (Costa & Atento, 2025; Mangubat & Atento, 2025).

From the standpoint of privacy practice implementation, scalability and performance are relevant because privacy controls often require stable and timely processing of data flows. For example, access controls, logging, encryption processes, and retention workflows add computational and administrative loads that must be sustained without disrupting operations. Consequently, infrastructure capacity that is designed to perform reliably under load can be interpreted as an enabling condition for consistent governance execution, including privacy-related processes that require timely retrieval, controlled modification, and secure storage of personal information (Liu & Li, 2024; Zhou et al., 2024).

2.2 Security and Compliance: Control Strength and Organizational Resilience

Security is widely discussed as a foundational dimension of IT infrastructure because it determines the extent to which systems can resist unauthorized access, protect sensitive information, and maintain operational continuity. Infrastructural security commonly involves layered technical controls—such as identity and access management, network segmentation, encryption, monitoring, and secure configuration—implemented alongside administrative policies and role assignments (Awodele et al., 2024; Wang et al., 2024). These controls are frequently framed as necessary not only for preventing breaches but also for strengthening organizational resilience, given that modern threats include both external intrusion and internal misuse.

Compliance, in turn, is typically discussed as a governance dimension that connects security controls to formal organizational obligations, standards, and accountability expectations. Rather than being reducible to "having security tools," compliance emphasizes the consistent application of security practices, the existence of documentation and auditability, and the alignment of technical controls with organizational policies and oversight mechanisms (Li & Huang, 2024; Tehrani et al., 2024). This conceptualization matters because privacy practice implementation depends heavily on whether security is managed as a routine organizational practice rather than treated as an episodic technical fix. Scholarship has also emphasized that compliance-oriented practices often require structured procedures for risk assessment, incident response preparation, and the periodic validation of controls—activities that connect infrastructure to broader risk management systems (Jayarao et al., 2024).

For manufacturing firms, security and compliance challenges can be amplified by heterogeneous systems and distributed operations, where legacy equipment, multiple access points, and third-party integration increase attack surfaces. In such environments, the maturity of security controls and the strength of compliance routines are likely to shape whether data governance is consistently implemented. Recent studies addressing organizational security practice highlight that effective security is typically achieved when technical safeguards are complemented by governance routines, including role clarity, monitoring, and continuous improvement, rather than relying on ad hoc responses to incidents (Awodele et al., 2024; Tehrani et al., 2024). This orientation underscores why "security and compliance" can be treated as an infrastructure dimension that plausibly supports privacy practice execution through enforceable access policies, secure storage, traceable transactions, and incident preparedness (Wang et al., 2024).

2.3 Data Privacy Governance: Scope, Rights of Data Subjects, and Controller Accountabilities

Data privacy practices are frequently conceptualized as a governance domain that regulates how personal information is collected, processed, stored, shared, retained, and disposed of in organizational settings. The scope of application is central because privacy practices must first determine the boundaries of coverage: which data are treated as personal or sensitive, which processing activities are covered, and which organizational units and partners are included within governance procedures (Tang, 2024). Scholarship addressing privacy governance emphasizes that scope is not merely definitional; it functions as an operational boundary that guides policy applicability, resource allocation, role assignments, and the prioritization of controls across the organization (Saura et al., 2024).

A second foundational dimension concerns the rights of data subjects, which represent normative and procedural expectations regarding transparency and individual control over personal data. Studies on privacy governance commonly discuss rights-related practices through themes such as notice and transparency mechanisms, accessible channels for requests, and procedural safeguards for handling access, correction, objection, and related requests within appropriate timeframes (Rai et al., 2024; Tang, 2024). In organizational practice, the feasibility of upholding such rights is shaped by the extent to which firms maintain traceable records, structured workflows, and clear ownership of responsibilities. Accordingly, rights-related implementation can be treated as a practical test of governance maturity: organizations that can respond consistently to requests tend to exhibit stronger documentation and clearer operationalization of privacy routines (Holden & Harsh, 2024).

Third, privacy governance requires explicit attention to the accountabilities of controllers—those entities responsible for deciding how and why personal data are processed. This accountability dimension commonly includes the establishment of policies, the designation of responsible roles, the management of third-party processors, risk assessment routines, and incident response preparedness (Alkamli & Alabduljabbar, 2024; Holden & Harsh, 2024). The literature suggests that accountability is operationally expressed through traceability: firms must be able to demonstrate that privacy practices are implemented, monitored, and improved over time, and that governance responsibilities are embedded in organizational systems rather than remaining purely aspirational (Saura et al., 2024). By aligning privacy practice implementation with broader governance concerns, this framing emphasizes that privacy is sustained through systems and routines rather than formal policies, a systemic view echoed in integrated analytics frameworks that stress clear scope and governance as prerequisites for dual outcomes like operational efficiency and compliance in complex data environments (Atento et al, 2025).

2.4 Infrastructure–Privacy Alignment: Socio-Technical Enablers of Consistent Practice

A recurring view in recent scholarship is that privacy practices are socio-technical: they require both technical capacity (infrastructure and controls) and organizational capacity (roles, procedures, and compliance routines). From this perspective, privacy governance cannot be sustained if the infrastructure cannot reliably implement access restrictions, logging, secure storage, segmentation, or monitoring—functions that translate governance policies into enforceable controls (Li & Huang, 2024; Tehrani et al., 2024). Conversely, even sophisticated infrastructure may fail to support privacy practices if governance routines are absent or weak, indicating that alignment involves both technical readiness and organizational management.

Studies of digital transformation and organizational capability building frequently note that infrastructure modernization is most effective when paired with governance mechanisms that ensure consistent execution and accountability. This includes structured oversight of configuration, continuous monitoring, standard operating procedures, and the institutionalization of risk management practices (Cheng et al., 2024; He, Xin, & Yang, 2024). Related work has also emphasized that data-related governance challenges are intensified as organizations adopt more complex digital ecosystems, thereby increasing the need for aligned infrastructure and policy mechanisms that can scale with operational complexity (Almeida & Bacao, 2024; Li, Yang, & Lu, 2024). In these accounts, infrastructure does not function as a neutral technical substrate; it shapes and constrains what governance can practically accomplish.

The infrastructure–privacy alignment is also discussed in terms of continuous improvement. Organizations often operate under evolving threat environments and changing operational demands; thus, both infrastructure capability and privacy practices must be maintained rather than treated as one-time implementations. Scholarship on organizational resilience implies that effective governance requires iterative evaluation of controls, learning from incidents, and adapting practices to new conditions—activities that require both system-level monitoring and managerial commitment (Jayarao et al., 2024; Pramanik et al., 2024; Atento & Atento, 2025). Furthermore, some studies emphasize that organizational readiness in digital initiatives may depend on the alignment of technical resources with decision-making structures and leadership support, indicating that governance outcomes such as privacy practice implementation can reflect deeper organizational capability patterns (Freddi & Wasenden, 2024; Heo & Doh, 2024).

Importantly, the alignment theme supports a conceptual expectation of association—rather than a deterministic causal claim—between infrastructure assessments and privacy practice assessments. Where infrastructure is evaluated as scalable, secure, and cost-efficient, organizations may be more capable of operationalizing privacy practices consistently because core enabling conditions (e.g., access control enforcement, monitoring, reliable storage, and procedural traceability) are more likely to be present (Li & Huang, 2024; Tehrani et al., 2024). Where infrastructure capability is weaker, privacy practices may remain unevenly implemented due to operational constraints, resource limitations, or insufficient system-level support for governance processes (Tang, 2024; Zhou et al., 2024). This conceptual logic provides a coherent basis for empirically testing whether perceived infrastructure capability is associated with perceived privacy practice implementation in specific organizational settings.

2.5 Synthesis and Gaps

The reviewed literature indicates that IT infrastructure capability and data privacy practices are conceptually intertwined. Infrastructure readiness—particularly scalability/performance and security/compliance—forms part of the enabling conditions required for governance practices that depend on enforceable controls, documentation, and resilience (Liu & Li, 2024; Tehrani et al., 2024). Meanwhile, privacy governance emphasizes scope definition, rights implementation, and controller accountability, all of which require organizational routines and systems that can support traceable and consistent execution (Tang, 2024; Holden & Harsh, 2024). Taken together, prior scholarship suggests that infrastructure and privacy operate as a coupled socio-technical system rather than as independent domains.

However, two gaps are salient for the present study. First, much of the literature tends to examine infrastructure capability or privacy governance separately, leaving limited empirical work that tests whether these domains are associated at the level of organizational assessment in localized manufacturing contexts. Second, even when linkages are conceptually implied, organizational evidence often lacks a multidimensional operationalization that maps infrastructure and privacy into specific dimensions suitable for targeted improvement planning. Addressing these gaps requires local empirical assessment that measures IT infrastructure across capability dimensions and privacy practices across governance dimensions, and then tests whether infrastructure assessments and privacy practice assessments move together in manufacturing organizations. This focus supports evidence-informed prioritization of infrastructure investments and governance enhancements without presuming causality beyond what correlational evidence can justify.

3. Methods

3.1 Research Design

A descriptive, cross-sectional research design was employed to assess perceived IT infrastructure and perceived data privacy practices among manufacturing companies in Batangas. The design was appropriate for describing the prevailing assessments across the measured dimensions and for examining the association between the two major variable sets.

3.2 Participants and Setting

The study utilized a purposive sample of 200 respondents drawn from manufacturing companies located in Batangas province. Respondents were owners, managers, or designated Data Protection Officers (DPOs), selected based on their direct involvement in company data processing activities and their engagement in the application process for the Seal of Registration of the National Privacy Commission.

3.3 Instrumentation

Data were collected using a self-made questionnaire composed of two parts, with items expressed as descriptive statements. Responses were recorded on a four-point Likert scale with the following interpretation guide: 3.50–4.00 = Strongly Agree; 2.50–3.49 = Agree; 1.50–2.49 = Disagree; 1.00–1.49 = Strongly Disagree.

Part I (IT Infrastructure Assessment) measured three dimensions with five items per dimension:

a. Scalability and Performance;

b. Security and Compliance; and

c. Cost and Efficiency.

Part II (Data Privacy Practices) measured three dimensions with five items per dimension:

a. Scope of Application;

b. Rights of Data Subjects; and

c. Accountabilities of Controllers.

A pilot test involving 30 respondents was conducted, and reliability was assessed using Cronbach's alpha in SPSS 28. Internal consistency ranged from acceptable to excellent across dimensions ($\alpha = 0.714–0.923$). For IT Infrastructure Assessment, scalability and performance yielded $\alpha = 0.747$, security and compliance $\alpha = 0.813$, cost and efficiency $\alpha = 0.849$, and the overall IT scale (15 items) $\alpha = 0.923$. For Data Privacy Practices, scope of application yielded $\alpha = 0.806$, rights of data subjects $\alpha = 0.826$, accountabilities of controllers $\alpha = 0.714$, and the overall privacy scale (15 items) $\alpha = 0.917$. These values indicated that the instrument was sufficiently reliable for the intended analyses.

3.4 Data Collection Procedure

Prior to data collection, approvals were secured from participating companies, and respondent consent was obtained. Ethical and confidentiality protocols were communicated to participants. The questionnaire—refined through expert validation and pilot testing—was administered using multiple channels to improve coverage and response rate, including Messenger, email, and Google Forms. Responses from the different administration modes were consolidated and recorded systematically, with routine checks implemented to support completeness and data quality.

3.5 Data Analysis

For descriptive assessment, weighted mean and rank were used to summarize the IT infrastructure and data privacy practice dimensions. A Shapiro–Wilk normality test indicated that all variable p-values were less than 0.05, indicating non-normal distributions. Accordingly, Spearman rho was used to test the association between IT infrastructure assessments and data privacy practice assessments. All analyses were performed using SPSS version 28.

3.6 Ethical Considerations

Ethical safeguards were observed to ensure that information collected was used for research purposes only. Company consent was sought through formal communication, and participation was voluntary. Confidentiality and anonymity were maintained by not collecting respondent names, and care was taken to avoid any harm to participants during the conduct of the study.

4. Results and Discussion

This section presents the study findings in line with the study objectives, summarizing the descriptive and correlational results that address the study questions.

4.1 IT Infrastructure Assessment (Scalability and Performance; Security and Compliance; Cost and Efficiency)

Overall, respondents assessed the IT infrastructure of manufacturing companies in Batangas province at a Strongly Agree level across all three dimensions. The overall composite mean for IT infrastructure was 3.57, indicating consistently high perceived readiness.

Scalability and Performance. Respondents reported a strong assessment of scalability and performance, with a composite mean of 3.53 (Strongly Agree). This indicates that, from the respondents' perspective, the firms' systems were viewed as capable of supporting operational demands and adapting to workload changes. *(See Table 1)*

Security and Compliance. Security and compliance received the highest assessment among the three IT infrastructure dimensions, with a composite mean of 3.61 (Strongly Agree). This suggests that respondents perceived security measures and compliance-related controls as strongly evident in their organizations. *(See Table 2)*

Cost and Efficiency. Cost and efficiency was likewise assessed at a Strongly Agree level, with a composite mean of 3.57. This indicates that respondents perceived their IT resources and processes as cost-conscious and operationally efficient. *(See Table 3)*

A consolidated summary of the IT infrastructure dimension means supports the conclusion that all three dimensions were evaluated positively, with security and compliance ranking highest, followed by cost and efficiency, and then scalability and performance, although differences were modest. *(See Table 4)*

4.2 Data Privacy Practices (Scope of Application; Rights of Data Subjects; Accountabilities of Controllers)

Data privacy practices were also assessed at a Strongly Agree level across all measured dimensions. The overall composite mean for data privacy practices was 3.62, reflecting consistently strong perceived implementation of privacy-related practices among the participating manufacturing companies.

Scope of Application. The scope of application dimension achieved a composite mean of 3.63 (Strongly Agree), indicating that respondents generally perceived privacy policies and procedures as widely applicable and consistently observed across relevant organizational activities. *(See Table 5)*

Rights of Data Subjects. The rights of data subjects dimension obtained a composite mean of

3.62 (Strongly Agree), reflecting strong perceived observance of data subject rights-related processes and practices. *(See Table 6)*

Accountabilities of Controllers. Accountabilities of controllers yielded a composite mean of 3.60 (Strongly Agree), indicating that governance responsibilities and accountability practices were perceived to be strongly present. *(See Table 7)*

A consolidated summary of privacy practice dimension means shows consistently high ratings across all three domains, with scope of application ranked highest, followed by rights of data subjects, and then accountabilities of controllers, again with relatively small differences. *(See Table 8)*

4.3 Relationship Between IT Infrastructure Assessment and Data Privacy Practices

Normality testing indicated non-normal distributions; therefore, Spearman rho was used to test associations between IT infrastructure and data privacy practices. Results showed statistically significant positive associations between each IT infrastructure dimension and each data privacy practice dimension, as well as between overall IT infrastructure and overall data privacy practices. Reported rho values ranged from .531 to .821, with all associations significant at p < .001 (reported as .000 in SPSS output), indicating that higher IT infrastructure assessments were associated with stronger data privacy practice assessments.

At the dimension level, the following associations were observed:

Scalability and Performance demonstrated strong positive correlations with privacy practice dimensions, including scope of application (rho = .717), rights of data subjects (rho = .804), and accountabilities of controllers (rho = .768). It also exhibited the strongest association with overall data privacy practices (rho = .821).

Security and Compliance also exhibited strong positive correlations with scope of application (rho = .734), rights of data subjects (rho = .780), and accountabilities of controllers (rho = .784), and showed a strong association with overall data privacy practices (rho = .811).

Cost and Efficiency showed moderate to strong positive correlations with scope of application (rho = .531), rights of data subjects (rho = .673), and accountabilities of controllers (rho = .604), and was positively associated with overall data privacy practices (rho = .627).

Collectively, these results indicate that firms reporting stronger IT infrastructure assessments also reported stronger data privacy practice assessments. Importantly, the findings are interpreted as associations consistent with the study design and do not imply causality (see Table 9).

5. Conclusions and Recommendations

5.1 Conclusions

Based on the descriptive and correlational findings from manufacturing companies in Batangas province, the study draws the following conclusions:

1. The participating firms were assessed to have robust IT infrastructure, with strong ratings across scalability and performance, security and compliance, and cost and efficiency (overall mean = 3.57). Security and compliance emerged as the highest-rated infrastructure dimension, suggesting that baseline safeguards and compliance-oriented controls are perceived as strongly present.

2. Data privacy practices were likewise assessed at a strongly implemented level across scope of application, rights of data subjects, and accountabilities of controllers (overall mean = 3.62). This indicates that respondents generally perceived privacy practices as institutionalized through policies, procedures, and assigned responsibilities consistent with compliance expectations.

3. IT infrastructure capability and data privacy practices were strongly and positively associated. All correlations between infrastructure dimensions and privacy practice dimensions were statistically significant (rho = .531 to .821; p < .001), indicating that firms reporting stronger infrastructure capability also reported stronger privacy practice implementation.

4. The strongest relationships were observed for scalability and performance and overall IT infrastructure when linked with overall data privacy practice assessment (rho up to .821). This pattern is consistent with the view that privacy practice implementation is supported by infrastructure maturity; however, the cross-sectional design supports associational interpretation and does not establish causality.

5.2 Recommendations

The recommendations below translate the findings into a focused action plan for manufacturing firms seeking to sustain privacy practice implementation while maintaining infrastructure readiness:

1. Institutionalize privacy-by-design in IT planning and scaling. Infrastructure expansion plans (e.g., cloud migration, additional storage, higher network capacity) should embed data minimization, access control, logging, and secure configuration standards so that growth does not create privacy-control gaps.

2. Strengthen security and compliance controls as a continuous program. Maintain routine patch management, endpoint protection, network security controls (e.g., firewalls and segmentation), and role-based access management, and align these controls with documented privacy policies and the organization's incident response plan.

3. Formalize governance and accountability mechanisms. Ensure an empowered Data Protection Officer (or equivalent), maintain an updated inventory of personal data processing activities, conduct privacy impact assessments for new systems or process changes, and implement contractual safeguards and audits for third-party processors.

4. Standardize and monitor data subject rights workflows. Develop clear procedures and service-level targets for access, rectification, objection/erasure or blocking (where applicable), and consent withdrawal, with documentation trails that support internal audits and external regulatory inquiries.

5. Protect privacy investments through cost-efficient optimization. Treat privacy and cybersecurity controls as core operational requirements, not discretionary costs. Use cost reviews to prioritize high-impact controls (e.g., identity and access management, monitoring, and training) while managing total cost of ownership and reducing avoidable downtime or breach-related losses.

5.3 Implications of Research Findings

Managerial and operational implications. The results suggest that IT infrastructure readiness and data privacy practice implementation co-occur in organizational assessments. For manufacturing firms, privacy compliance should be managed as an integrated capability that links infrastructure planning, cybersecurity operations, and governance routines rather than as a stand-alone compliance function.

Policy and compliance implications. The strong associations observed across dimensions indicate that compliance readiness depends on both procedural and technical capacity. Organizations pursuing National Privacy Commission registration-related requirements may benefit from aligning their compliance roadmaps with measurable infrastructure capability improvements, particularly in scaling plans and security control maturity.

Research implications. The study used a cross-sectional, self-report design and a purposive sample within Batangas province; therefore, generalization should be made cautiously. Future studies may strengthen inference by expanding samples across regions and manufacturing sub-sectors, incorporating objective infrastructure and compliance indicators (e.g., audit outcomes, incident records, maturity assessments), and using longitudinal designs to test whether infrastructure investments precede improvements in privacy practice implementation.

6. References

Alkamli, S., & Alabduljabbar, R. (2024). Understanding privacy concerns in ChatGPT: A data-driven approach with LDA topic modeling. *Heliyon*, 10(20), e39087. https://doi.org/10.1016/J.HELIYON.2024.E39087

Almeida, G., & Bacao, F. (2024). UMAP-SMOTENC: A simple, efficient, and consistent alternative for privacy-aware synthetic data generation. Knowledge-Based Systems, 300, 112174. https://doi.org/10.1016/J.KNOSYS.2024.112174

Assaye, B. T., Endalew, B., Tadele, M. M., hailiye Teferie, G., Teym, A., Melese, Y. hune, senishaw, A. fentahun, Wubante, S. M., Ngusie, H. S., & Haimanot, A. B. (2024). Readiness of big health data analytics by technology-organization-environment (TOE) framework in Ethiopian health sectors. *Heliyon*, 10(19), e38570.

https://doi.org/10.1016/J.HELIYON.2024.E38570

Atento, A. G., & Atento, R. G. (2025). A Case Study of Mercury Drug Corporation: Strategic Adaptation to Universal Healthcare and Digital Disruption in the Philippines. *International Journal of Health & Business Analytics*, *1*(1). https://doi.org/10.65166/zhw7dd39

Atento, R. G., Quinto, L., Espelita, C. A. M., & Castaneda, C. (2025). Integrating Business and Health Analytics: A Conceptual Framework for Dual Outcomes in Healthcare. *International Journal of Health & Business Analytics*, *1*(1). https://doi.org/10.65166/04pdc866

Awodele, I. A., Mewomo, M. C., Municio, A. M. G., Chan, A. P. C., Darko, A., Taiwo, R., Olatunde, N. A., Eze, E. C., & Awodele, O. A. (2024). Awareness, adoption readiness and challenges of railway 4.0 technologies in a developing economy. *Heliyon*, *10*(4), e25934. https://doi.org/10.1016/J.HELIYON.2024.E25934

Balakrishnan, S., Jin, L., Cassottana, B., Costa, A., & Sansavini, G. (2024). Developing resilience pathways for interdependent infrastructure networks: A simulation-based approach with consideration to risk preferences of decision-makers. *Sustainable Cities and Society*, 115, 105795. https://doi.org/10.1016/J.SCS.2024.105795

Cheng, Z., Liu, Y., Wu, C., Pan, Y., Zhao, L., Deng, X., & Zhu, C. (2024). Decentralized IoT data sharing: A blockchain-based federated learning approach with joint optimizations for efficiency and privacy. *Future Generation Computer Systems*, 160, 547–563. https://doi.org/10.1016/J.FUTURE.2024.06.035

Chwiłkowska-Kubala, A., Cyfert, S., Malewska, K., Mierzejewska, K., & Szumowski, W. (2023). The impact of resources on digital transformation in energy sector companies. The role of readiness for digital transformation. *Technology in Society*, 74, 102315. https://doi.org/10.1016/J.TECHSOC.2023.102315

Costa, V. D., & Atento, R. G. (2025). Financial performance and market viability of Globe Telecom, Inc.: An integrated fundamental–technical analysis. *International Journal of Health & Business Analytics*, *1*(1). https://doi.org/10.65166/v5x9d097

Freddi, E., & Wasenden, O. C. (2024). Privacy during pandemics: Attitudes to public use of personal data. *Journal of Behavioral and Experimental Economics*, 113, 102304. https://doi.org/10.1016/J.SOCEC.2024.102304

He, P., Xin, Y., & Yang, Y. (2024). PARE: Privacy-Preserving Data Reliability Evaluation for Spatial Crowdsourcing in Internet of Things. Computers, *Materials and Continua*, 80(2), 3067–3084. https://doi.org/10.32604/CMC.2024.054777

Heo, G., & Doh, I. (2024). Blockchain and differential privacy-based data processing system for data security and privacy in urban computing. *Computer Communications*, 222, 161–176. https://doi.org/10.1016/J.COMCOM.2024.04.027

Holden, K., & Harsh, M. (2024). On pipelines, readiness and annotative labour: Political geographies of AI and data infrastructures in Africa. *Political Geography*, 113, 103150. https://doi.org/10.1016/J.POLGEO.2024.103150

Jayarao, G. B., Ray, S., & Panigrahi, P. K. (2024). Information security threats and organizational readiness in nWFH scenarios. *Computers & Security*, 140, 103745. https://doi.org/10.1016/J.COSE.2024.103745

Li, W., & Huang, Q. (2024). A hybrid encryption algorithm based approach for secure privacy protection of big data in hospitals. *Egyptian Informatics Journal*, 28, 100569. https://doi.org/10.1016/J.EIJ.2024.100569

Li, Y., Yang, R., & Lu, Y. (2024). A privacy risk identification framework of open government data: A mixed-method study in China. *Government Information Quarterly*, 41(1), 101916. https://doi.org/10.1016/J.GIQ.2024.101916

Liu, J., & Li, F. (2024). Rural revitalization driven by digital infrastructure: Mechanisms and empirical verification. *Journal of Digital Economy*, 3, 103–116. https://doi.org/10.1016/J.JDEC.2025.01.002

Mangubat, M., & Atento, R. G. (2025). Integrated Fundamental–Technical Evaluation of Jollibee Foods Corporation: Financial Performance, Market Behavior, and Investment Outlook. *International Journal of Health & Business Analytics*, *1*(2). https://doi.org/10.65166/azkk2x82

Pramanik, P., Jana, R. K., & Ghosh, I. (2024). AI readiness enablers in developed and developing economies: Findings from the XGBoost regression and explainable AI framework. *Technological Forecasting and Social Change*, 205, 123482. https://doi.org/10.1016/J.TECHFORE.2024.123482

Rai, H. M., Shukla, K. K., Tightiz, L., & Padmanaban, S. (2024). Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies. *Heliyon*, *10*(19), e38917. https://doi.org/10.1016/J.HELIYON.2024.E38917

Saura, J. R., Škare, V., & Dosen, D. O. (2024). Is AI-based digital marketing ethical? Assessing a new data privacy paradox. *Journal of Innovation & Knowledge*, *9*(4), 100597. https://doi.org/10.1016/J.JIK.2024.100597

Sumrit, D. (2024). Enhancing readiness degree for Industrial Internet of Things adoption in manufacturing enterprises: An integrated Pythagorean fuzzy approach. *Heliyon*, *10*(20), e39007. https://doi.org/10.1016/J.HELIYON.2024.E39007

Tang, Y. (2024). Privacy protection framework for open data: Constructing and assessing an effective approach. *Library & Information Science Research*, *46*(3), 101312. https://doi.org/10.1016/J.LISR.2024.101312

Tehrani, A. N., Ray, S., Roy, S. K., Gruner, R. L., & Appio, F. P. (2024). Decoding AI readiness: An in-depth analysis of key dimensions in multinational corporations. *Technovation*, 131, 102948. https://doi.org/10.1016/J.TECHNOVATION.2023.102948

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, 147, 104051. https://doi.org/10.1016/J.COSE.2024.104051

Zhou, F., Li, L., & Wen, H. (2024). Regional digital infrastructure and carbon neutrality: A technology–structure–efficiency perspective. *Energy Strategy Reviews*, 56, 101583. https://doi.org/10.1016/J.ESR.2024.101583

7. Tables

Table 1
IT Infrastructure Assessment (Scalability and Performance)

Indicators	**Weighted Mean**	**Verbal Interpretation**	**Rank**
1. Our current IT systems (e.g., servers, network, software) can easily handle increases in customer data and transaction volumes without significant slowdowns.	3.53	*Strongly Agree*	3
2. When our business experiences peak usage times (e.g., promotional periods, busy seasons), our IT infrastructure consistently maintains fast and reliable performance for employees and customers	3.49	*Agree*	5
3. We regularly assess our IT infrastructure's capacity to ensure it can support our projected business growth over the next 1-3 years without needing major overhauls.	3.56	*Strongly Agree*	2
4. Our existing software applications and online platforms load quickly and respond efficiently, minimizing delays for users within our company.	3.51	*Strongly Agree*	4
5. We have a clear strategy or plan in place to scale our IT infrastructure (e.g., adding more storage, upgrading internet speed, migrating to cloud services) if our data processing needs significantly increase.	3.57	*Strongly Agree*	1
COMPOSITE MEAN	**3.53**	Strongly Agree	

Legend: 1.0 – 1.49 (Strongly Disagree), 1.5 – 2.49 (Disagree), 2.5 – 3.49 (Agree) and 3.5 – 4.00 (Strongly Agree)

Table 2
IT Infrastructure Assessment (Security and Compliance)

Indicators	**Weighted Mean**	**Verbal Interpretation**	**Rank**
1. Our company has clearly defined security policies and procedures in place to protect personal data from unauthorized access, loss, or damage.	3.61	*Strongly Agree*	3
2. We regularly conduct employee training and awareness programs to educate our staff on data privacy best practices and how to identify cybersecurity threats (e.g., phishing).	3.58	*Strongly Agree*	4
3. Our IT infrastructure uses essential security tools such as firewalls, antivirus software, and regular software updates to protect against cyberattacks.	3.65	*Strongly Agree*	1
4. We have a documented incident response plan that outlines the steps our company will take in the event of a data breach, including notification procedures to affected individuals and the NPC.	3.56	*Strongly Agree*	5
5. Our company's data processing activities (collection, storage, use, sharing) are fully compliant with the requirements of the Data Privacy Act of 2012 (RA 10173) and its Implementing Rules and Regulations.	3.64	*Strongly Agree*	2
COMPOSITE MEAN	**3.61**	Strongly Agree	

Table 3
IT Infrastructure Assessment (Cost and Efficiency)

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Our company's current IT infrastructure helps us reduce operational costs (e.g., paper usage, manual processes, utilities) rather than increasing them.	3.56	*Strongly Agree*	3
2. We regularly review our IT expenses (e.g., software subscriptions, hardware maintenance, internet services) to identify areas where we can achieve better value or savings.	3.55	*Strongly Agree*	4
3. Our IT systems effectively automate routine tasks, allowing our employees to focus on more productive and strategic activities for the business.	3.53	*Strongly Agree*	5
4. We are confident that our IT infrastructure investments provide a good return for our business, contributing positively to our overall efficiency and profitability.	3.59	*Strongly Agree*	2
5. Our company has a clear understanding of the total cost of owning and maintaining our IT infrastructure, including hidden costs like downtime or security incidents.	3.60	*Strongly Agree*	1
COMPOSITE MEAN	**3.57**	**Strongly Agree**	

Table 4
Summary Table on IT Infrastructure Assessment

Indicators	Weighted Mean	Verbal Interpretation	Rank
Scalability and Performance	3.53	*Strongly Agree*	2
Security and Compliance	3.61	*Strongly Agree*	1
Cost and Efficiency	3.57	*Strongly Agree*	3
OVERALL MEAN	**3.57**	**Strongly Agree**	

Table 5
Data Privacy Practices (Scope of Application)

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Our company has a clear understanding of what constitutes "personal information" and "sensitive personal information" as defined by the Data Privacy Act (DPA).	3.70	*Strongly Agree*	1
2. We are confident that all types of personal information our organization collects, whether from customers, employees, or other sources, fall under the scope of the DPA.	3.65	*Strongly Agree*	2
3. Our company has assessed whether the DPA applies to our data processing activities even if they involve individuals or systems outside the Philippines (e.g., online transactions with international customers, use of foreign cloud servers).	3.62	*Strongly Agree*	3.5
4. We have determined that our company is classified as a "Personal Information Controller" (PIC) or "Personal Information Processor" (PIP) under the DPA, and we understand the implications of this classification.	3.62	*Strongly Agree*	3.5

5. Our company has identified any specific types of personal data or processing activities that might be exempt from certain DPA provisions and has legal guidance on such exemptions.	3.58	*Strongly Agree*	5
COMPOSITE MEAN	**3.63**	Strongly Agree	

Table 6
Data Privacy Practices (Rights of Data Subjects)

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Our company provides clear and accessible information to individuals about how their personal data is collected, used, stored, and shared (Right to be Informed).	3.65	*Strongly Agree*	1
2. We have a defined process that allows individuals to request and receive a copy of the personal data our organization holds about them (Right to Access)	3.60	*Strongly Agree*	4
3. Our company has a system in place for individuals to dispute inaccuracies in their personal data and request for its correction or update (Right to Rectification).	3.62	*Strongly Agree*	2
4. We provide options for individuals to object to the processing of their personal data (e.g., for direct marketing) or request its erasure or blocking under the conditions allowed by the DPA (Right to Object; Right to Erasure or Blocking).	3.59	*Strongly Agree*	5
5. Our company ensures that individuals can easily withdraw their consent for the processing of their personal data, and we have procedures to act on such withdrawals promptly.	3.61	*Strongly Agree*	3
COMPOSITE MEAN	**3.62**	Strongly Agree	

Table 7
Data Privacy Practices (Accountabilities of Controllers)

Indicators	**Weighted Mean**	**Verbal Interpretation**	**Rank**
1. Our company has officially designated a Data Protection Officer (DPO) or an equivalent individual responsible for overseeing our compliance with the Data Privacy Act.	3.59	*Strongly Agree*	4
2. We have documented our data processing activities, including details on what personal information we collect, why we collect it, and how it is managed throughout its lifecycle.	3.60	*Strongly Agree*	3
3. Our company conducts regular privacy impact assessments (PIAs) when introducing new projects or systems that involve the processing of personal data to identify and mitigate privacy risks.	3.57	*Strongly Agree*	5
4. We ensure that any third-party service providers or partners who process personal data on our behalf are contractually bound to comply with the Data Privacy Act.	3.61	*Strongly Agree*	1.5
5. Our company has a clear process for reporting personal data breaches to the National Privacy Commission (NPC) and affected data subjects within the required timeframe.	3.61	*Strongly Agree*	1.5
COMPOSITE MEAN	3.60	Strongly Agree	

Table 8
Summary Table on Data Privacy Practices

Indicators	**Weighted Mean**	**Verbal Interpretation**	**Rank**
Scope of Application	3.63	*Strongly Agree*	1
Rights of Data Subjects	3.62	*Strongly Agree*	2
Accountabilities of Controllers	3.60	*Strongly Agree*	3
OVERALL MEAN	**3.62**	Strongly Agree	

Table 9
Relationship between IT Infrastructure Assessment and Data Privacy Practices

Variables	***Spearman-rho***	**p-Value**	**Interpretation**
Scalability and Performance			
Scope of Application	.717**	< .001	Significant
Rights of Data Subjects	.804**	< .001	Significant
Accountabilities of Controllers	.768**	< .001	Significant
OVERALL MEAN	.821**	< .001	
Security and Compliance			
Scope of Application	.734**	< .001	Significant
Rights of Data Subjects	.780**	< .001	Significant
Accountabilities of Controllers	.784**	< .001	Significant
OVERALL MEAN	.811**	< .001	
Cost and Efficiency			
Scope of Application	.531**	< .001	Significant
Rights of Data Subjects	.673**	< .001	Significant
Accountabilities of Controllers	.604**	< .001	Significant
OVERALL MEAN	.627**	< .001	
OVERALL IT Infrastructure Assessment			

Scope of Application	.714**	< .001	Significant
Rights of Data Subjects	.810**	< .001	Significant
Accountabilities of Controllers	.772**	< .001	Significant
OVERALL MEAN	.812**	< .001	