Cybersecurity readiness and data privacy compliance in local government: Basis for contextualized plan

Antonio L. Adille IV

aadilleiv@gmail.com
Laguna State Polytechnic University, Sta. Cruz Campus, Laguna, Philippines, 4009

Abstract

This study aimed to assess the level of cybersecurity readiness and data privacy compliance among Local Government Units (LGUs), focusing on key areas such as technological resources, organizational resources and competencies, and environmental mandates, as well as technical preparedness, policy and regulatory compliance, employee awareness, and organizational resilience. The study was conducted during the academic year 2025–2026. It also sought to determine whether a significant relationship exists between cybersecurity readiness and data privacy compliance using statistical tools such as frequency, percentage, mean, standard deviation, and Pearson correlation coefficient. A quantitative descriptive–correlational research design was utilized in this study. The respondents consisted of selected LGU personnel who were purposively selected based on their roles in information and communication technology and data handling. Data were gathered through a structured survey questionnaire designed to measure the variables of the study. The collected data were analyzed using appropriate statistical methods to describe the levels of cybersecurity readiness and data privacy compliance and to examine the relationships between them. The results revealed that LGUs demonstrate a moderate to high level of cybersecurity readiness and data privacy compliance across all indicators. The study concludes that strengthening technological capabilities, enhancing organizational competencies, and ensuring compliance with regulatory mandates are essential. It is therefore recommended that LGUs invest in continuous training, improve policy implementation, and upgrade cybersecurity infrastructure to further enhance data privacy compliance.

Keywords: Cybersecurity readiness, data privacy compliance, local government units, information security, organizational resilience

1. Introduction

The rapid growth of information and communication technology (ICT) has greatly changed how governments deliver public services. Many government institutions now depend on digital systems to improve efficiency, transparency, and accessibility for citizens. While digitalization has enhanced public administration, it has also created serious challenges for cybersecurity and data privacy, especially since government agencies handle large volumes of sensitive personal information.

As cyber threats continue to increase in frequency and complexity, government institutions face risks that may disrupt public services and weaken public trust. Because trust is essential in effective governance, protecting information systems and personal data has become an important responsibility of public institutions. In response, the Philippine government enacted the Data Privacy Act of 2012 (Republic Act No. 10173), which requires all government agencies, including Local Government Units (LGUs), to implement measures that ensure the protection of personal data and information systems.

Despite these national policies, the implementation of cybersecurity and data privacy measures remains inconsistent among public institutions (OECD, 2021). Differences in organizational capacity, leadership, funding, technical expertise, and administrative competence affect how policies are enforced at the local level. Since LGUs provide essential public services such as civil registration, healthcare, social welfare,

and taxation, their increasing reliance on digital technologies has also increased their exposure to cyber risks and potential data breaches.

Several studies and government reports revealed that many LGUs continue to face challenges such as limited cybersecurity infrastructure, lack of trained personnel, insufficient funding, and low awareness of data privacy responsibilities. Reports from the National Privacy Commission and the Department of Information and Communications Technology further emphasized that cybersecurity readiness among LGUs remains uneven, particularly in smaller municipalities. International studies also support these findings, noting that budget limitations, lack of awareness, and shortages of cybersecurity professionals are common barriers in the public sector. These challenges highlight the need for stronger cybersecurity readiness and improved data privacy compliance among LGUs to ensure the protection of public information and maintain citizens' trust in government services.

1.1. Background of the Study

The rapid digital transformation of public administration has significantly changed the way local governments deliver services and perform their daily operations. Local Government Units (LGUs) now rely heavily on information and communication technology (ICT) systems to manage essential public services such as civil registration, healthcare, social welfare, taxation, disaster response, education, and public records management. Through digitalization, government transactions have become faster, more accessible, and more efficient, allowing LGUs to improve the quality of service provided to citizens. This shift toward digital governance reflects the growing need for modernization in public administration and highlights the important role of technology in promoting transparency, accountability, and effective public service delivery.

However, while digital transformation offers many benefits, it also exposes local governments to increasing cybersecurity threats and data privacy risks. As LGUs become more dependent on digital systems and online platforms, they also become more vulnerable to cyberattacks such as hacking, phishing, ransomware, malware infections, unauthorized access, and data breaches. In recent years, cyberattacks targeting government institutions have increased both in frequency and sophistication, disrupting operations and threatening the confidentiality and integrity of sensitive information. Many local governments are often considered vulnerable or "soft targets" because of limited cybersecurity infrastructure, outdated systems, insufficient funding, and lack of trained cybersecurity professionals. These challenges make it difficult for LGUs to effectively detect, prevent, and respond to cyber threats.

At the same time, the amount of personal and sensitive data collected by local governments has grown significantly due to the expansion of digital services. LGUs regularly handle confidential information such as birth records, voter registration details, healthcare information, financial records, educational data, and social welfare documents. If these data are improperly managed, leaked, or compromised, citizens may face serious consequences such as identity theft, financial fraud, privacy violations, and misuse of personal information. More importantly, incidents involving data breaches can weaken public trust and confidence in government institutions. Because trust is a fundamental element of effective governance, protecting citizens' information has become both a legal responsibility and an ethical obligation for LGUs.

Despite the implementation of laws and national policies related to cybersecurity and data privacy, many LGUs continue to experience difficulties in fully complying with established standards and regulations. Existing studies commonly focus on cybersecurity issues in national agencies or large organizations, while limited attention has been given to the actual cybersecurity readiness and data privacy compliance of local government units, particularly in smaller municipalities. There is also a lack of localized studies examining how technological resources, organizational competencies, environmental mandates, employee awareness, and institutional preparedness influence data privacy compliance within LGUs. Furthermore, previous studies often discuss cybersecurity and data privacy separately, creating a gap in understanding the relationship between cybersecurity readiness and data privacy compliance in local government settings.

This study seeks to address these gaps by examining the level of cybersecurity readiness and data privacy compliance among LGUs and determining the relationship between these variables. Specifically, the study aims to provide a clearer understanding of how technological capabilities, organizational resources, policy implementation, and employee awareness contribute to the protection of sensitive government data and information systems. By identifying existing strengths and weaknesses, the study hopes to contribute to the improvement of cybersecurity practices, policy implementation, and data privacy protection in local government institutions. Ultimately, the study emphasizes the importance of strengthening cybersecurity readiness not only to protect information systems but also to preserve public trust, ensure continuity of public services, and support the long-term success of digital governance initiatives.

1.2. Theoretical Framework

This study is grounded on three interrelated theoretical and regulatory lenses: Institutional Theory**,** the Technology–Organization–Environment (TOE) Framework, and the General Data Protection Regulation (GDPR) Framework**.** Together, these frameworks provide a comprehensive basis for examining the readiness and compliance of local government units (LGUs) in implementing cybersecurity and data privacy practices. Institutional Theory explains the external and internal pressures that shape LGUs' compliance behavior, the TOE Framework clarifies the contextual determinants of cybersecurity adoption, and the GDPR Framework provides a global benchmark for evaluating the robustness of LGUs' data privacy practices.

1.2.1. Institutional Theory

Institutional Theory (DiMaggio & Powell, 1983; Scott, 2004) posits that organizations are influenced by forces and expectations from their institutional environment. These external pressures compel organizations to adopt structures, behaviors, and technologies that maintain legitimacy and public trust. In relation to data protection and cybersecurity implementation in LGUs, Institutional Theory highlights three key institutional pressures:

1.2.2. Coercive Pressures

These arise legal mandates and regulatory requirements. The Data Privacy Act of 2012 (Republic Act No. 10173) requires LGUs to adopt technical and administrative measures to protect personal data. Like the GDPR, the DPA institutionalizes data protection principles such as transparency, accountability, data minimization, and breach reporting. Compliance with these requirements is therefore not optional but a legal imperative that exerts coercive pressure on LGUs.

1.2.3. Normative Pressures

Normative pressures stem from the increasing professionalization of IT and digital governance practices. The expanding role of Data Protection Officers, privacy training programs, and internationally recognized standards many of which are inspired by the GDPR shape expectations on how LGUs should manage data and cybersecurity risks. These norms promote the adoption of best practices and reinforce institutional expectations related to digital responsibility, ethical data handling, and public sector accountability.

1.2.4. Mimetic Pressures

Under conditions of uncertainty, organizations emulate the practices of highly compliant or successful peers. LGUs often look to other more digitally advanced agencies or localities for models of cybersecurity implementation. The widespread global adoption of GDPR aligned privacy frameworks further strengthens mimetic pressures, encouraging LGUs to adopt similar measures to remain credible, competitive, and aligned with recognized international standards.

Institutional Theory therefore explains why LGUs pursue cybersecurity and data privacy initiatives: to conform to legal mandates, professional standards, and the practices of leading institutions, thereby maintaining legitimacy within the public governance landscape.

1.2.5. Technology–Organization–Environment (TOE) Framework

The Technology–Organization–Environment (TOE) Framework (Tornatzky & Fleischer, 1990) provides a multidimensional lens for understanding the factors that influence an organization's adoption of technological innovations, such as cybersecurity systems and data protection mechanisms. The framework encompasses three contexts:

1.2.6. Technological Context

This refers to the availability, sophistication, and suitability of technological infrastructure within the LGU. Components include cybersecurity tools, IT architecture, data encryption systems, network security protocols, and digital platforms used for service delivery. LGUs with more advanced technological environments are more capable of complying with the standards set by the Data Privacy Act and the GDPR, such as data integrity, confidentiality, and breach prevention.

1.2.7. Organizational Context

Organizational factors include leadership commitment, staff competencies, financial resources, internal policies, and organizational culture. Effective data protection requires trained personnel (e.g., DPOs), clear governance structures, and adequate budget allocation for cybersecurity programs. An organizational culture that prioritizes data protection, risk management, and ethical data handling strengthens LGUs' ability to adopt and sustain compliant cybersecurity practices.

1.2. 8. Environmental Context

This dimension captures external factors that shape cybersecurity readiness, including cyber threat landscapes, inter-organizational collaborations, citizens' expectations for secure public services, and national regulatory frameworks such as the DPA and its implementing rules. The GDPR also exerts global influence by setting high standards for data protection that serve as reference points even for organizations outside Europe. These environmental forces pressure LGUs to enhance their cybersecurity posture and align with national and international best practices.

The TOE Framework explains how and under what conditions LGUs are able to implement cybersecurity and data privacy measures, emphasizing readiness and capacity.

1.2.9. General Data Protection Regulation (GDPR) Framework

Although the GDPR is a European Union regulation, it has become the global benchmark for data protection standards. Its principles lawful, fair, and transparent processing; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability parallel and reinforce the requirements of

the Data Privacy Act of 2012. The GDPR also institutionalizes organizational measures that guide LGUs in building strong data protection frameworks. Among these measures are the concept of privacy by design and by default, which encourage organizations to integrate privacy and security considerations into systems and processes from the beginning. The regulation also promotes the conduct of Data Protection Impact Assessments (DPIAs) to identify and minimize potential privacy risks associated with data processing activities. In addition, the GDPR highlights the importance of protecting the rights of data subjects, implementing mandatory breach notification procedures, maintaining proper documentation of data processing activities, and ensuring accountability and demonstrable compliance within organizations.

By integrating GDPR principles, LGUs can evaluate whether their data protection measures meet internationally recognized standards. The GDPR framework thus functions as a normative and technical reference point, strengthening both Institutional and TOE analyses by specifying what robust data protection should look like in practice.

1.2.10. Synthesis of Frameworks

The integration of Institutional Theory, the TOE Framework, and the GDPR Framework provides a comprehensive theoretical foundation for examining LGU compliance with cybersecurity and data privacy practices:

Institutional Theory explains the pressures that drive LGUs to comply with data protection mandates.

TOE Framework explains the readiness conditions that determine how effectively LGUs can implement cybersecurity and privacy mechanisms.

GDPR Framework offers a global standard that guides and evaluates the quality, rigor, and completeness of LGU data protection measures.

Together, these frameworks illuminate the interplay between legitimacy pressures, organizational capability, environmental conditions, and global best practices. This combined perspective enables a deeper understanding of how LGUs can achieve secure, resilient, and citizen-centered digital governance.

1.3. Conceptual Framework

The conceptual framework is presented in the form of the paradigm below. The paradigm is an application of system analysis from descriptive research, where it provides the independent variable, mediating variables and the dependent variable of the study.

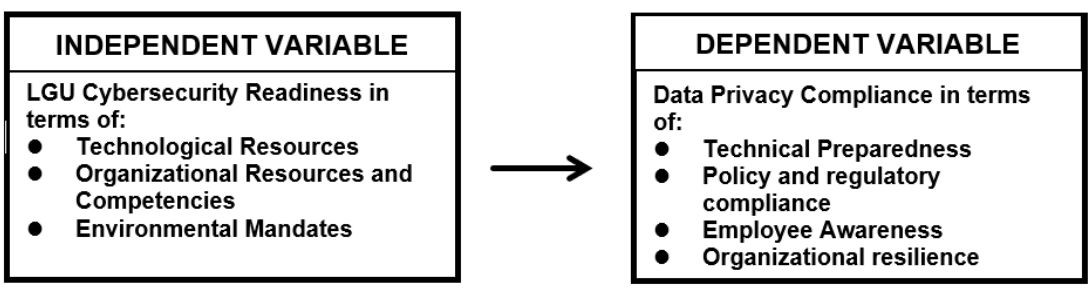

Figure 1. Relationship Among Variables

This study adopts a conceptual framework that examines how technological, organizational, and environmental conditions influence the cybersecurity and data privacy readiness of Local Government Units

(LGUs). It also considers the mediating mechanisms that translate LGU resources and leadership commitment into effective cybersecurity practices. The model posits that Independent Variables (IVs) influence the Mediating Variables (MVs), which in turn affect the Dependent Variable (DV).

The independent variables in this study capture the internal and external conditions that influence a local government unit's (LGU's) capacity and motivation to adopt cybersecurity and data privacy measures. Guided by the Technology–Organization–Environment (TOE) framework and institutional perspectives, these factors include the technological, organizational, and environmental elements that shape an LGU's readiness for digital security.

First, technological resources refer to the availability of essential hardware, software, and secure network infrastructures that enable LGUs to implement cybersecurity solutions. Without adequate technological tools, even well-designed policies or trained personnel cannot effectively safeguard information assets.

Second, organizational resources and competencies encompass the internal capacities that support cybersecurity implementation. These include the allocation of skilled personnel, sufficient budget, and reliable IT support infrastructure. Organizational competence also reflects how well LGU staff understand cyber risks, threats, and vulnerabilities—an area that underscores the importance of digital literacy and threat awareness. Additionally, leadership commitment plays a critical role; when leaders prioritize cybersecurity through policy directives, proper funding, governance structures, and strategic planning, they reinforce the organization's ability to institutionalize secure practices.

Third, environmental mandates pertain to the external pressures that influence LGUs to comply with cybersecurity and data privacy requirements. Regulatory frameworks most notably the Data Privacy Act of 2012 serve as compelling forces that shape LGU behavior and drive adherence to national standards on data protection and cybersecurity.

Together, these independent variables form the foundational readiness conditions that either enable or constrain an LGU's ability to advance its cybersecurity posture.

The dependent variable**,** cybersecurity and data privacy readiness, reflects the overall extent to which LGUs are prepared and capable of meeting cybersecurity standards and complying with legal and regulatory requirements. This readiness includes their technical capability, policy adherence, employee awareness, and overall organizational resilience. It represents the culmination of technological resources, organizational capacities, environmental obligations, and the effectiveness of internal mechanisms that support secure and privacy-aligned governance.

1.4. Statement of the Problem

This study aimed to assess the level of cybersecurity readiness and data privacy compliance in local government unit. It also seeks to answer the following queries:

1. What is the demographic profile of respondents in terms of;
    - 1.1 Years of service
    - 1.2 Highest educational attainment
    - 1.3 ICT Training background
    - 1.4 LGU type
2. What is the level of cybersecurity readiness of LGU in terms of:
    - 2.1 Technological Resources;
    - 2.2 Organizational Resources and Competencies; and
    - 2.3 Environmental Mandates?
3. What is the level of Data Privacy Compliance in terms of:
    - 2.1. Technical preparedness;
    - 2.2. Policy and regulatory compliance;

2.3. Employee awareness; and
2.4. Organizational resilience?

4. Is there a significant relationship between the level of cybersecurity readiness and data privacy compliance, and with respect to the demographic profile of the respondent?
5. What action plan may be proposed based on the findings of the study

1.5. Research Hypothesis

Based on the questions stated above, the hypotheses will be proposed:
There is no significant relationship between the level of cybersecurity readiness and data privacy compliance with respect to the demographic profile of the respondents.

1.6. Significance of the Study

This study is significant because it addresses the growing need for secure, reliable, and privacy-focused digital governance in local government units (LGUs). As LGUs increasingly adopt digital systems to deliver public services, they also face rising threats of cyberattacks, data breaches, and unauthorized access to sensitive information. Examining their current cybersecurity practices, assessing their readiness against cyber threats, and evaluating their compliance with national and international regulations is therefore both timely and essential. This research responds to these challenges by identifying the existing capacities, gaps, and vulnerabilities of LGUs, while highlighting best practices that can guide improvements in cybersecurity governance and data protection.

The findings of this study will be most beneficial to LGUs themselves, as they are at the forefront of implementing cybersecurity measures and ensuring the security of government information systems. By providing a clear picture of their current technological infrastructure, organizational capacity, and compliance levels, this study will help LGUs recognize areas where improvements are needed. The insights generated will support them in strengthening their cybersecurity frameworks, enhancing staff training, allocating resources more effectively, and developing strategies to protect the personal data of citizens who depend on their services.

Local government officials, information technology personnel, and Data Protection Officers (DPOs) will also benefit greatly from this study. These individuals play a direct role in managing cybersecurity operations and enforcing data privacy policies. The study will offer them practical guidance on implementing effective internal practices, such as incident response planning, risk management, and continuous capacity building. By learning from the strengths and weaknesses identified across LGUs, they can adopt improved approaches that ensure better compliance with the Data Privacy Act of 2012 and related regulatory requirements.

National government agencies including the Department of Information and Communications Technology (DICT), National Privacy Commission (NPC), and the Department of the Interior and Local Government (DILG) will likewise gain valuable information from this research. The assessment of LGU readiness and compliance can guide these agencies in formulating more targeted policies, designing capacity building programs, and providing technical support tailored to the needs of local governments. The data will also help them identify common challenges faced by LGUs, enabling them to allocate resources more strategically and reinforce cybersecurity standards nationwide.

Citizens and local communities form another important group that stands to benefit from this study. As the primary users of government services, citizens entrust LGUs with their personal information, expecting it to be protected from misuse or unauthorized disclosure. By contributing to the enhancement of cybersecurity and data privacy measures, this research indirectly promotes the safety and security of citizen

data. Stronger cybersecurity practices will also foster greater trust in digital government services, encouraging more people to participate in online governance initiatives.

The study also has implications for policymakers and legislators, who may use the results to strengthen existing regulations or propose new measures designed to enhance cybersecurity readiness at the local level. The findings can serve as evidence in crafting policies that support greater investments in cybersecurity infrastructure, standardized training programs, and the institutionalization of privacy management practices across all LGUs.

Finally, this study will serve as a valuable reference for future researchers. As cybersecurity in local governance is still an emerging field in the Philippines, the results of this research provide a foundation for further academic inquiry. Future researchers may build upon the findings by conducting comparative studies between regions, developing models for assessing cybersecurity maturity, or exploring specialized topics such as artificial intelligence in public administration or the intersection of digital governance and citizen trust. By doing so, future studies can deepen the understanding of cybersecurity challenges and contribute to the continuous improvement of data protection practices in the public sector.

Overall, the significance of this study lies in its potential to inform policy, strengthen institutional capacity, enhance public trust, and advance academic knowledge. Its timely examination of cybersecurity and data privacy practices offers practical solutions to existing problems and presents meaningful implications for both local and national governance.

1.7. Scope and Limitations of the Study

This study centers on assessing the readiness and compliance of selected local government units (LGUs) in implementing and institutionalizing cybersecurity and data privacy practices within the evolving landscape of digital governance. As public institutions increasingly adopt digital systems for service delivery, communication, and information management, cybersecurity and data protection have become critical elements of local administration. The study, therefore, aims to evaluate how prepared LGUs are to protect sensitive information and ensure compliance with the Data Privacy Act of 2012 (Republic Act No. 10173) and other relevant national policies that mandate the secure handling of data in public sector operations.

The scope of the study includes an in-depth examination of several core areas that collectively determine LGU readiness and compliance: technological infrastructure, organizational capacity, policy formulation and enforcement, staff competence and training, and risk management systems. Each of these dimensions is essential to understanding the overall cybersecurity posture of LGUs.

The study explores the availability, functionality, and reliability of IT assets and digital systems used within LGUs, including hardware, software, network security, and data protection tools. This component assesses whether existing technological infrastructure is adequate to support the secure storage, processing, and transmission of information.

This aspect examines the institutional readiness of LGUs to implement cybersecurity and data privacy measures. It involves analyzing governance structures, leadership commitment, budget allocation, and the existence of dedicated units or personnel (such as data protection officers or IT departments) tasked with managing cybersecurity initiatives.

The study evaluates the presence and enforcement of cybersecurity and data privacy policies, as well as the mechanisms used to monitor and ensure compliance with national laws and local regulations. This includes assessing whether LGUs have implemented internal guidelines aligned with the standards set by the National Privacy Commission (NPC) and whether such policies are consistently observed in practice.

Recognizing that effective cybersecurity implementation depends on human behavior as much as on technology, the study examines the level of awareness, technical skill, and professional development of personnel handling sensitive data. The research will consider training programs, seminars, and other capacity-building initiatives that aim to strengthen the cybersecurity competence of LGU employees.

The study also looks into the strategies and protocols LGUs employ to identify, prevent, and respond to potential cyber threats, breaches, or data loss incidents. This includes examining risk assessment procedures, response mechanisms, and the presence of contingency plans to ensure operational continuity and public trust.

In addition to these internal factors, the study considers the influence of legal and regulatory pressures that shape LGUs' behavior and priorities in cybersecurity and data privacy management. Compliance with national mandates, adherence to privacy standards, and the need to maintain institutional legitimacy all form part of the external environment driving LGUs to strengthen their digital governance systems.

The participants in this study will include individuals directly involved in the formulation, implementation, and monitoring of cybersecurity and data privacy policies within the selected LGUs. These include, but are not limited to, Information Technology (IT) officers, Data Protection Officers (DPOs), administrative heads, and other key personnel responsible for data management and information security. Their insights and experiences will provide a comprehensive understanding of how cybersecurity and privacy measures are operationalized at the local level.

The study is limited to specific LGU, which are purposely chosen based on their accessibility, relevance, and representatives in terms of size, location, and digital maturity. As such, the findings may not fully represent all LGUs nationwide but are expected to offer meaningful insights into trends, challenges, and best practices applicable to similarly situated local governments. The scope does not extend to national agencies, private corporations, or non-governmental organizations, except when their interactions directly impact the cybersecurity operations of the participating LGUs. It is also important to note that the study's outcomes depend significantly on the cooperation, honesty, and transparency of the respondents. The quality of data gathered from surveys, interviews, and document reviews will be influenced by the willingness of LGU personnel to provide accurate and complete information regarding their cybersecurity and data privacy policies. Limitations such as restricted access to internal documents, confidentiality constraints, or differing interpretations of compliance standards may affect the depth of the analysis.

Furthermore, the study does not aim to conduct a technical audit or penetration testing of LGU systems. Instead, it focuses on an organizational and policy-oriented assessment, emphasizing governance processes, institutional readiness, and compliance behavior rather than detailed technical evaluations of network security or software performance. The study is descriptive and diagnostic in nature, seeking to understand the current state of cybersecurity and data privacy practices and the factors influencing their implementation.

In terms of timeframe, the study covers the period from 2023 to 2025, reflecting the most recent developments in LGU digital transformation efforts. This period captures the ongoing digitalization of public services, the strengthening of national cybersecurity directives, and the continuous adaptation of LGUs to new technologies and emerging threats.

In summary, this study is confined to evaluating how selected LGUs prepare for and comply with cybersecurity and data privacy requirements in the digital age. It provides an analytical view of the interplay between technology, policy, and organizational capacity at the local level while recognizing inherent limitations related to scope, access, and respondent cooperation. Through this defined scope and set of limitations, the study aims to generate practical insights that can inform policy decisions, improve institutional readiness, and contribute to the development of a secure and privacy-conscious local governance framework in the Philippines.

1.8. Definition of Terms

The following definitions of terms are provided to ensure clarity and a common understanding of key concepts used throughout the study. These terms establish the operational meanings adopted by the researcher,

helping readers interpret the study's findings and discussions within the appropriate technical and contextual framework.

Cybersecurity – In this study, cybersecurity refers to the set of technologies, processes, and practices implemented by local government units (LGUs) to protect their digital systems, networks, and data from cyber threats such as hacking, malware, ransomware, and unauthorized access.

Cybersecurity Readiness – This term refers to the overall level of preparedness of LGUs in preventing, detecting, responding to, and recovering from cyberattacks. It includes technological infrastructure, policy implementation, personnel capability, and internal security practices.

Data Privacy – Data privacy refers to the protection of personal and sensitive information collected, processed, and stored by LGUs. It involves ensuring that such data is handled lawfully, securely, and in accordance with the Data Privacy Act of 2012 and related regulations.

Data Privacy Compliance – This term describes the degree to which LGUs adhere to the requirements of the Data Privacy Act of 2012, including the appointment of a Data Protection Officer (DPO), conducting Privacy Impact Assessments, maintaining a Privacy Manual, and implementing breach response procedures.

Data Protection Officer (DPO) – In this study, the DPO is the LGU official responsible for managing data protection programs, monitoring compliance with privacy regulations, and ensuring that personal information is handled securely within the organization.

Technological Infrastructure – Technological infrastructure refers to the hardware, software, network systems, security tools, and digital platforms used by LGUs to deliver services and protect organizational data. It includes computers, servers, cybersecurity software, firewalls, and information systems.

Organizational Capacity – This term refers to the internal resources of LGUs—including available personnel, technical skills, leadership support, and structural capability that enable them to implement effective cybersecurity and data privacy measures.

Cybersecurity Policies and Initiatives – These are formal guidelines, programs, and activities established by LGUs to govern cybersecurity practices. Examples include information security policies, data protection programs, cybersecurity awareness campaigns, and compliance procedures.

Internal Practices – Internal practices refer to the day-to-day operational measures and routines carried out within LGUs to support cybersecurity and data privacy. These include staff training, risk assessments, incident reporting, and policy enforcement.

Risk Management – Risk management refers to the process of identifying, evaluating, and addressing cybersecurity risks within the LGU. It includes vulnerability assessments, threat analysis, and the development of mitigation strategies to reduce potential security breaches.

Cyber Threats – Cyber threats are digital attacks or malicious activities that target IT systems and data. Examples include phishing, malware, unauthorized system access, ransomware attacks, and network intrusions affecting LGU operations.

Local Government Units (LGUs) – LGUs refer to local administrative units in the Philippines such as provinces, cities, municipalities, and barangays. For this study, LGUs serve as the primary research respondents and units of analysis regarding cybersecurity and privacy practices.

Compliance Level – Compliance level refers to the extent to which LGUs follow mandated cybersecurity and data privacy standards. Compliance is measured through the presence of policies, designated personnel, training programs, and documentation required by regulators.

Challenges and Barriers – These terms refer to the various difficulties encountered by LGUs in implementing cybersecurity and privacy measures, such as limited budget, lack of trained personnel, political turnover, outdated technologies, and insufficient awareness.

Demographic Factors – In this study, demographic factors include the LGU's size, income classification, budget capacity, and geographic location—variables used to determine variations in cybersecurity readiness and compliance levels.

1.9. Review of Related Literature and Study

The rapid digitalization of government services has amplified global concerns about cybersecurity and data privacy, particularly within local government units (LGUs). As public institutions increasingly depend on digital platforms to provide essential services, they simultaneously expose themselves to vulnerabilities that can compromise both government operations and citizen data. Literature from various countries illustrates that while digital advancement has improved administrative efficiency, it has also heightened exposure to cyberattacks. Duggan and Doyle (2020) note that local governments worldwide remain highly susceptible to cyber threats due to outdated infrastructure, insufficient budgets, and bureaucratic challenges that hinder modernization. This international perspective reflects a growing consensus that cybersecurity readiness has become a central issue in modern governance.

Foreign literature emphasizes that the foundation of cybersecurity lies in the robustness of an organization's technological infrastructure. Massey et al. (2020) explain that governments with modern, secure networks and updated software demonstrate stronger defenses against cyberattacks, while those relying on legacy systems tend to be more vulnerable. These challenges extend beyond technology, as the availability of trained personnel and strong organizational capacity also influence cybersecurity performance. Anderson and Kim (2019) point out that staffing shortages in cybersecurity roles remain common among local governments globally, often resulting from budget limitations and the competitive nature of the ICT labor market.

Cybersecurity policies and governance frameworks further shape organizational readiness. Reeves (2019) highlights that many developing nations struggle to adopt international frameworks such as ISO/IEC 27001 or the NIST Cybersecurity Framework due to financial and technical limitations. Even in countries where such policies exist, their effectiveness largely depends on political will and administrative commitment. Wright and Marshall (2022) note that cybersecurity policies often fail when leadership does not prioritize implementation or allocate sufficient resources.

Internal organizational practices, including staff training, policy enforcement, and risk management, also emerge as crucial factors in enhancing cybersecurity resilience. Velasco and Tan (2021) emphasize that frequent training and awareness-building help reduce incidents caused by human error, one of the most common sources of data breaches worldwide. Lopez and Chen (2020) add that routinely conducting risk assessments and updating incident response plans significantly improves readiness. Nevertheless, studies show that many local governments internationally are unable to maintain regular training or update internal protocols due to resource constraints (Williams, 2022).

Local literature reflects similar concerns within the Philippine context. Panganiban (2021) observes that as LGUs increasingly shift to electronic governance, many still lack the necessary technological infrastructure to secure their systems effectively. Reports from the Department of Information and Communications Technology (DICT, 2020) emphasize the uneven distribution of digital resources across the country, with urban LGUs generally possessing more advanced infrastructure than their rural counterparts. Santos and Cruz (2021) further illustrate that organizational capacity varies widely among LGUs; while national policies require the appointment of Data Protection Officers (DPOs), many LGUs struggle to comply due to the scarcity of trained personnel and limited institutional support.

The implementation of cybersecurity and data privacy policies in the Philippines also faces significant challenges. Although the Data Privacy Act of 2012 provides a legal foundation for safeguarding personal information, De la Cruz (2022) found that many LGUs fail to implement its key requirements, such as conducting privacy impact assessments or creating incident response protocols. These shortcomings are often linked to inconsistent leadership priorities, insufficient budgets, and limited technical knowledge among staff.

Internal cybersecurity practices within LGUs also remain underdeveloped. Domingo (2021) notes that many LGUs do not regularly conduct cybersecurity training or risk assessments. Instead, their approach

tends to be reactive, responding to issues after they arise rather than preventing them proactively. This pattern undermines the establishment of a consistent cybersecurity culture within local government offices.

Several local authors discuss the challenges and barriers that hinder the improvement of LGU cybersecurity. Delos Reyes (2020) reports that frequent political turnover, limited financial resources, lack of IT personnel, and insufficient technological literacy contribute to the slow advancement of cybersecurity initiatives. These challenges are compounded by bureaucratic delays and competing administrative demands that deprioritize cybersecurity.

Foreign studies further reinforce the global nature of these issues. Peterson and Lawrence (2020) found that the majority of local governments in the United States lack formal cybersecurity strategies, leaving them vulnerable to increasingly sophisticated attacks. In Europe, Steed and Rhodes (2019) discovered that municipalities often fail to meet basic cybersecurity standards due to fragmented ICT systems and insufficient coordination among departments. Brighton and Evans (2021) demonstrated that the presence of cybersecurity specialists significantly improves compliance with information security regulations, suggesting that human capital plays a pivotal role in cybersecurity governance.

Local studies similarly highlight vulnerabilities in Philippine LGUs. Ilagan and Montelibano (2020) reported that only a minority of LGUs showed full compliance with the Data Privacy Act, noting that many lacked privacy manuals, breach protocols, and functional committees dedicated to data protection. Marquez and Bautista (2020) identified major disparities in readiness across LGUs in Luzon, with larger, higher-income LGUs demonstrating superior infrastructure and cybersecurity programs compared to their smaller counterparts. Pascual and Reganit (2021) revealed that staff training and leadership support were strong predictors of cybersecurity readiness in provincial governments, underscoring the importance of internal organizational practices.

Synthesizing these findings reveals consistent themes across international and local contexts. Weak technological infrastructure, inconsistent organizational capacity, and limited policy implementation continue to undermine cybersecurity readiness. Internal practices such as training and risk management are often insufficient, and LGUs face numerous barriers including budget constraints, leadership turnover, and limited technical expertise. Demographic differences such as income level, size, and location further influence disparities in cybersecurity readiness.

Despite the breadth of existing literature, several gaps remain. First, few studies provide a holistic assessment that integrates technological, organizational, policy, and demographic variables to evaluate LGU cybersecurity readiness. Second, limited research explores how internal practices mediate the relationship between organizational capacity and compliance. Third, comparative analyses across different types of LGUs urban versus rural, small versus large, low income versus high income are scarce. These gaps highlight the need for a comprehensive study that examines cybersecurity readiness and data privacy compliance among LGUs, identifies their challenges, and offers evidence-based recommendations for improving cybersecurity governance in the Philippines.

Scholarly literature highlights that organizational mechanisms play a vital mediating role in strengthening cybersecurity readiness within local governments. Effective policy implementation ensures that cybersecurity frameworks and data privacy laws are translated into actual organizational practices. For instance, Reeves (2019) and Wright and Marshall (2022) emphasize that even when cybersecurity policies exist, their effectiveness depends largely on leadership commitment and administrative enforcement. Similarly, capacity-building initiatives, such as continuous staff training and awareness programs, are identified as critical factors that enhance employee competence and reduce vulnerabilities caused by human error (Velasco & Tan, 2021; Pascual & Reganit, 2021). Additionally, robust risk management systems, including regular risk assessments and updated incident response protocols, significantly strengthen an LGU's ability to prepare for and respond to cyber threats (Lopez & Chen, 2020; Domingo, 2021). These findings indicate that organizational mechanisms do not simply accompany readiness; they bridge the gap between

available resources and actual cybersecurity performance, making them essential mediating variables in assessing LGU cybersecurity and data privacy readiness.

2. Methodology

This chapter presents the methods and procedures used to conduct the study entitled *"Cybersecurity Readiness and Data Privacy Compliance in Local Government: Basis for Contextualized Plan."* It describes the research design, respondents of the study, sampling techniques, research instruments, data gathering procedures, and the statistical treatment of data. Each step in the methodology was structured to ensure that the objectives of the study to assess the readiness and compliance of local government units (LGUs) in implementing cybersecurity and data privacy measures were adequately achieved.

2.1. Research Design

The study employed a descriptive-correlational quantitative research design, which is highly suitable for investigating the cybersecurity and data privacy practices of local government units (LGUs). The descriptive component of the design allows the researcher to systematically examine and present the current state of cybersecurity readiness and data privacy compliance among selected LGUs. Specifically, it enables the study to describe the level of implementation of policies, the adequacy of technological infrastructure, personnel awareness, and the effectiveness of data protection mechanisms. By employing descriptive measures, the study can provide a clear and structured overview of existing practices, identify strengths and weaknesses, and highlight areas that require improvement.

The correlational component complements the descriptive aspect by exploring potential relationships between variables, in this case, between cybersecurity readiness and compliance with data privacy standards. This design is appropriate because it allows the researcher to quantify the degree of association between organizational preparedness and the level of adherence to regulations such as the Data Privacy Act of 2012 and related government issuances. Understanding these relationships is crucial for identifying whether higher organizational capacity, better technological infrastructure, or enhanced internal practices are linked to stronger compliance outcomes, thereby providing empirical insights into effective cybersecurity governance.

Additionally, the use of quantitative data collection through structured survey questionnaires ensures that measurable and comparable data can be gathered across multiple LGUs, enabling statistical analysis and generalizable findings. To enrich the quantitative findings, qualitative insights were also obtained through brief follow-up interviews with key personnel, including IT officers and Data Protection Officers (DPOs), for triangulation purposes. This mixed approach strengthens the study's validity by confirming and contextualizing survey responses, while still maintaining the structured, objective framework of a quantitative study.

Overall, the descriptive-correlational design is well-suited to this research because it not only captures the current status of cybersecurity and data privacy practices but also identifies meaningful associations between organizational readiness and compliance. This dual focus enables the study to generate actionable recommendations that can inform policy, strengthen LGU cybersecurity governance, and enhance compliance with data protection standards.

2.2. Respondents of the Study

The respondents of the study consisted of local government employees directly involved in managing digital information systems, IT infrastructure, and data privacy compliance. These included Information Technology Officers / MIS Personnel, Data Protection Officers (DPOs), Records Officers / Administrative Officers, Department Heads or Supervisors handling digital records and systems.

The study covered five (5) local government units within the Province of Laguna, representing city and municipal categories. A total of 25 respondents will participate in the study and will be distributed across the LGUs based on their staffing complement and department size.

The inclusion criteria required that respondents have at least one year of experience handling information systems, cybersecurity, or data privacy-related tasks. This ensured that participants could provide informed perspectives relevant to the study objectives.

2.3. Sampling Technique

The study used a purposive sampling technique, a non-probability sampling method appropriate for selecting respondents with specific knowledge and responsibilities related to the research focus. Although non-probability sampling may limit the generalizability of the findings, it remains effective in examining the relationships among the study variables within the organization.

Given the technical nature of cybersecurity and data privacy, only personnel occupying ICT-related and administrative positions were selected. This approach ensured the reliability and relevance of responses regarding institutional readiness and compliance practices.

To further ensure representation, the number of participants from each LGU was determined proportionally to its population size and organizational structure.

2.4. Research Instrument

Data were collected using a structured survey questionnaire developed by the researcher and validated by experts in information technology, public administration, and research methodology. The questionnaire was divided into four major sections:

1. **Profile of Respondents** – demographic and professional information such as position, years of service, and ICT training background.
2. **Cybersecurity Readiness** – measured using indicators adapted from the *NIST Cybersecurity Framework* and *Department of Information and Communications Technology (DICT) Cyber Resilience Model*. Indicators covered policy existence, infrastructure, employee awareness, and incident response preparedness.
3. **Data Privacy Compliance** – assessed based on compliance with the *National Privacy Commission's (NPC)* core privacy principles and circulars (lawful processing, data protection measures, and accountability mechanisms).
4. **Challenges and Recommendations** – included both Likert-scale and open-ended questions regarding barriers and suggested improvements.

2.5. Research Procedure

1. **Preparation Phase** The researcher first secured approval from the academic adviser. Letters of permission were then sent to the offices of the selected LGUs, explaining the purpose of the study and requesting participation.
2. **Instrument Validation** The survey questionnaire underwent expert validation specialists from cybersecurity management. Their feedback led to minor revisions to improve clarity and content relevance.
3. **Data Collection** Upon approval, the questionnaires were distributed in printed form for LGUs. Respondents were briefed about the study's objectives, confidentiality assurance, and voluntary participation. Data collection lasted for three weeks.

4. **Data Organization** Collected responses were encoded and cleaned using Microsoft Excel before being imported into SPSS (Statistical Package for the Social Sciences) for analysis.
5. **Follow-Up Interviews (Optional Triangulation)** To complement survey data, short semi-structured interviews were conducted with selected IT officers and DPOs to gather deeper insights on institutional challenges and compliance experiences.
6. **Data Analysis and Interpretation** Statistical analyses were conducted to describe and interpret the findings in relation to the study's objectives.

2.6. Statistical Treatment

The following statistical tools were employed in analyzing the collected data:

1. **Frequency and Percentage Distribution** – used to present the demographic profile of respondents and categorical variables related to cybersecurity policies and data privacy compliance.
2. **Weighted Mean and Standard Deviation** – used to determine the average level of readiness and compliance based on Likert-scale responses.
3. **Pearson's Correlation Coefficient (r)** – used to determine the relationship between cybersecurity readiness and data privacy compliance.

The strength of the relationship was interpreted using Guilford's Rule of Thumb (1956), as shown below:

Table 1. *Interpretation of Correlation Coefficient Based on Guilford's Rule of Thumb*

Correlation Coefficient (*r*)	**Interpretation**
0.00 – 0.20	Slight / Negligible
0.21 – 0.40	Low Correlation
0.41 – 0.70	Moderate Correlation
0.71 – 0.90	High Correlation
0.91 – 1.00	Very High Correlation

Note. Interpretation based on Guilford (1956).

A significance level of $p < .05$ was used to determine statistical significance, while the strength of relationships was interpreted using Guilford's Rule of Thumb (1956).

Table 2. *Likert Scale*

Weighted Mean Range	Descriptive Equivalent	Interpretation
3.21 – 4.00	Strongly Agree	Very High
2.41 – 3.20	Agree	Moderately High
1.61 – 2.40	Disagree	Low
1.00 – 1.60	Strongly Disagree	Very Low

2.7. Ethical Considerations

All research procedures adhered to ethical standards for human participation. Respondents were informed of their rights, including voluntary participation, confidentiality of responses, and data anonymity. No personally identifiable information was disclosed in the results, and all collected data were used solely for academic purposes.

3. Results and Discussion

This chapter presents, analyzes, and interprets the data gathered in the study. The results are organized according to the statement of the problem.

3.1. Demographic Profile of Respondents

Table 3. *Demographic Profile of the Respondents in terms of Years of Service, Educational Attainment, ICT Training, and LGU type.*

Demographic Profile	Frequency	Percent	Rank
Years of Service			
Less than 1 year	8	32.0	2
1-5 years	10	40.0	1
6-10 years	4	16.0	3
11-15 years	2	8.0	4
26 years and above	1	4.0	5
Educational Attainment			
College Graduate	22	88.0	1
Masters	3	12.0	2
ICT Training			
None	2	8.0	3
Basic ICT Training	16	64.0	1
Advanced ICT Training	6	24.0	2
Cybersecurity-specific training	1	4.0	4
LGU Type			
City	10	40.0	2
Municipality	15	60.0	1
TOTAL	**25**	**100.0**	

The demographic profile of the respondents presents important insights into their background in terms of years of service, educational attainment, ICT training, and LGU type.

In terms of years of service, the majority of respondents have 1–5 years of experience (f = 10, 40.0%), ranking first. This is followed by those with less than 1 year of service (f = 8, 32.0%), indicating that a large portion of the workforce is relatively new. Respondents with 6–10 years of service (f = 4, 16.0%) rank third, while those with 11–15 years (f = 2, 8.0%) and 26 years and above (f = 1, 4.0%) comprise the smallest groups. This distribution suggests that the LGU workforce is composed largely of early-career employees, which may have implications for experience and institutional knowledge (Smith, 2020).

In terms of educational attainment, the majority of respondents are college graduates (f = 22, 88.0%), ranking first, while a smaller portion holds master's degrees (f = 3, 12.0%). This indicates that most employees have attained a basic level of higher education, but relatively few have pursued advanced academic qualifications (Garcia & Reyes, 2019).

With regard to ICT training, most respondents have basic ICT training (f = 16, 64.0%), ranking first. This is followed by those with advanced ICT training (f = 6, 24.0%), while a smaller number have no ICT training (f = 2, 8.0%) or cybersecurity-specific training (f = 1, 4.0%). This suggests that while general ICT knowledge is common, specialized cybersecurity training is limited among employees, which may affect organizational cybersecurity readiness (Almeida et al., 2021).

In terms of LGU type, the majority of respondents come from municipalities (f = 15, 60.0%), ranking first, while the remaining respondents are from cities (f = 10, 40.0%). This indicates that the study primarily reflects the context and practices of municipal LGUs (Department of the Interior and Local Government [DILG], 2018).

Overall, the data show that respondents are mostly early-career, college-educated individuals with basic ICT training, and are primarily from municipal LGUs. These characteristics may influence their level of

cybersecurity awareness, skills, and implementation of data privacy practices within their respective organizations (National Privacy Commission, 2020).

3.2. Level of Cybersecurity Readiness

Table 4. *Level of Cybersecurity Readiness in terms of Technological Resources*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Our LGU uses updated hardware and software for secure operations.	3.24	0.52	Very High	Fully Implemented
2. Firewalls, antivirus programs, and encryption tools are properly implemented.	3.12	0.44	Moderately High	Mostly Implemented
3. IT systems and software are regularly updated and patched.	3.16	0.62	Moderately High	Mostly Implemented
4. Secure servers or cloud services are used to store LGU data.	3.28	0.84	Very High	Fully Implemented
5. Endpoint devices are centrally managed and secured.	3.28	0.54	Very High	Fully Implemented
Overall Weighted Mean	**3.22**	**0.50**	**Very High**	**Fully Implemented**

Table 3 shows that the overall mean of 3.22 (*SD* = 0.50), verbally interpreted as Very High, indicates that LGUs possess a strong level of technological resources necessary for cybersecurity. This suggests that systems and tools are not only available but are fully implemented and compliant, reflecting a high degree of readiness in terms of technical infrastructure.

Individual indicators, with mean scores ranging from 3.12 to 3.28 and standard deviations between 0.44 and 0.84, further support the overall finding of a very high level of implementation. Specifically, the indicators "Secure servers or cloud services are used to store LGU data" (*M* = 3.28, *SD* = 0.84) and "Endpoint devices are centrally managed and secured" (*M* = 3.28, *SD* = 0.54) obtained the highest mean scores, both interpreted as Very High, indicating that these practices are fully implemented and compliant. This is followed by "Our LGU uses updated hardware and software for secure operations" (*M* = 3.24, *SD* = 0.52), which also reflects a very high level of implementation.

Meanwhile, "IT systems and software are regularly updated and patched" (*M* = 3.16, *SD* = 0.62) and "Firewalls, antivirus programs, and encryption tools are properly implemented" (*M* = 3.12, *SD* = 0.44) are interpreted as Moderately High, indicating that these measures are mostly implemented or largely compliant. Although these areas demonstrate strong performance, they are slightly lower compared to other indicators, suggesting opportunities for further strengthening and consistency.

Overall, the findings indicate that LGUs demonstrate full implementation and compliance in most aspects of technological cybersecurity readiness, particularly in data storage and endpoint security. However, minor improvements may still be needed in system updating and core security tools to achieve uniform excellence across all areas.

According to the National Institute of Standards and Technology Cybersecurity Framework (2018), technological readiness requires not only the availability of tools but also their proper integration, maintenance, and continuous monitoring. Furthermore, Neil Hadlington (2017) emphasizes that insufficient or outdated technological resources can increase vulnerability to cyberattacks, even when basic systems are already in place.

Table 5. Level of Cybersecurity Readiness in terms of Organizational Resources and Competencies

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Regular system backups and recovery mechanisms are in place.	3.32	0.75	Very High	Fully Implemented
2. Employees receive regular training on cybersecurity best practices.	2.72	1.02	Moderately High	Mostly Implemented
3. Awareness campaigns on phishing and social engineering attacks are conducted.	2.92	0.81	Moderately High	Mostly Implemented
4. There is formal incident response plan for cybersecurity breaches.	2.76	0.88	Moderately High	Mostly Implemented
5. Regular drills or simulations are conducted to prepare for cyber incidents.	2.56	0.87	Moderately High	Mostly Implemented
Overall Weighted Mean	**2.86**	**0.72**	**Moderately High**	**Mostly Implemented**

The table shows that the indicators of cybersecurity preparedness range from moderately high to very high, based on their mean scores. The highest-rated indicator is the implementation of regular system backups and recovery mechanisms (M = 3.32, SD = 0.75), interpreted as Very High, with a remark of Fully Implemented/Fully Compliant. This suggests that LGUs are highly consistent in ensuring data protection and system recovery measures, reflecting strong technical resilience in maintaining business continuity and data integrity.

Next are several indicators interpreted as Moderately High, including awareness campaigns on phishing and social engineering attacks (M = 2.92, SD = 0.81), presence of a formal incident response plan (M = 2.76, SD = 0.88), employees receiving regular cybersecurity training (M = 2.72, SD = 1.02), and conduct of regular drills or simulations (M = 2.56, SD = 0.87). These results indicate that these practices are mostly implemented or largely compliant, but not yet consistently executed across all LGUs.

Among these, awareness campaigns on phishing and social engineering attacks obtained the highest mean, suggesting that informational efforts are relatively more common compared to structured training and simulation activities. Meanwhile, regular drills or simulations recorded the lowest mean, indicating that practical preparedness exercises are the least prioritized component of cybersecurity readiness.

Overall, the weighted mean of 2.86 (SD = 0.72), interpreted as Moderately High, suggests that cybersecurity preparedness practices are generally mostly implemented and largely compliant, but still require improvement. While LGUs demonstrate strong performance in technical safeguards such as system backups, gaps remain in human-centered and organizational preparedness, particularly in training, awareness programs, incident response planning, and simulation exercises.

According to Parsons et al. (2017), human factors remain one of the weakest links in cybersecurity, as insufficient training and awareness significantly increase vulnerability to cyber threats. Furthermore, ISACA (2020) emphasizes that effective cybersecurity depends not only on technology but also on organizational culture, leadership commitment, and continuous capacity building.

Table 6. *Level of Cybersecurity Readiness in terms of Environmental Mandates*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Our LGU follows national cybersecurity guidelines.	3.08	0.86	Moderately High	Mostly Implemented
2. Cyber incidents are reported in accordance with government requirements.	2.80	0.91	Moderately High	Mostly Implemented
3. Cybersecurity mandates influence LGU IT decisions.	3.20	0.58	Moderately High	Mostly Implemented
4. Our LGU is aware of risks for non-compliance.	3.40	0.65	Very High	Fully Implemented
5. Cybersecurity is checked during external audits.	3.00	0.76	Moderately High	Mostly Implemented
Overall Weighted Mean	**3.10**	**0.56**	**Moderately High**	**Mostly Implemented**

The table shows that the indicators of cybersecurity compliance and regulatory adherence in the LGU range from moderately high to very high, based on their mean scores. The highest-rated indicator is the awareness of risks for non-compliance (M = 3.40, SD = 0.65), interpreted as Very High, with a remark of Fully Implemented/Fully Compliant. This indicates that LGUs have a strong understanding of the consequences of non-compliance, reflecting high awareness of cybersecurity risks and regulatory obligations.

This is followed by the influence of cybersecurity mandates on LGU IT decisions (M = 3.20, SD = 0.58), interpreted as Moderately High, with a remark of Mostly Implemented/Largely Compliant. This suggests that government policies and cybersecurity directives significantly guide IT-related decisions, although not yet at a fully standardized level across all units.

Next is the LGU's adherence to national cybersecurity guidelines (M = 3.08, SD = 0.86), also interpreted as Moderately High, indicating that compliance with national standards is generally practiced and largely compliant, but still shows some variability in implementation. Similarly, cybersecurity being checked during external audits (M = 3.00, SD = 0.76) is interpreted as Moderately High, reflecting that audit mechanisms are in place and contribute to monitoring compliance, though not consistently maximized across all processes.

The lowest indicator is cyber incident reporting in accordance with government requirements (M = 2.80, SD = 0.91), likewise interpreted as Moderately High, with a remark of Mostly Implemented. This suggests that while reporting mechanisms exist, they are not consistently followed, indicating a gap in formal compliance procedures and timely reporting of cyber incidents.

Overall, the weighted mean of 3.10 (SD = 0.56), interpreted as Moderately High, indicates that LGUs demonstrate a generally positive level of cybersecurity compliance and regulatory adherence. However, despite this overall strength, gaps remain particularly in cyber incident reporting practices, which may affect timely response, coordination, and escalation of cybersecurity incidents.

Under the Data Privacy Act of 2012 (Republic Act 10173), organizations are mandated to implement strict safeguards for the protection of personal data; however, compliance levels often vary depending on institutional capacity and enforcement. Greenleaf (2014) further emphasizes that regulatory compliance is often rule-based rather than culture-based, resulting in partial and inconsistent implementation across organizations.

Table 7. *Composite Table of the Level of Cybersecurity Readiness*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Technological Resources	3.22	0.50	Moderately High	Mostly Implemented
2. Organizational Resources and Competencies	2.86	0.72	Moderately High	Mostly Implemented
3. Environmental Mandates	3.10	0.56	Moderately High	Mostly Implemented
General Overall Weighted Mean	**3.06**	**0.59**	**Moderately High**	**Mostly Implemented**

Table 7 presents the overall level of cybersecurity readiness of the respondents across key indicators. Among the indicators, Technological Resources obtained the highest mean score (M = 3.22, SD = 0.50), interpreted as *Moderately High* with the remark *Mostly Implemented/Largely Compliant*. This indicates that the organization has relatively strong technological tools, systems, and infrastructure in place to support cybersecurity efforts. The low standard deviation further suggests consistency in responses, meaning most respondents share a similar perception regarding the adequacy of technological resources.

This is followed by Environmental Mandates (M = 3.10, SD = 0.56), also interpreted as *Moderately High*. This implies that external requirements such as policies, laws, and regulatory frameworks are generally observed and contribute positively to cybersecurity readiness. Compliance with external mandates reflects the organization's alignment with national and institutional cybersecurity standards.

Lastly, Organizational Resources and Competencies recorded the lowest mean (M = 2.86, SD = 0.72), although still within the *Moderately High* level. This suggests that while structures, skills, and internal capabilities are present, they may not be as strong or consistently developed compared to technological and regulatory aspects. The relatively higher standard deviation indicates more varied responses, pointing to inconsistencies in organizational capacity across respondents.

Overall, the General Weighted Mean of 3.06 (SD = 0.59) indicates a *Moderately High* level of cybersecurity readiness, described as *Mostly Implemented/Largely Compliant*. This means that while essential cybersecurity measures are in place, there is still room for improvement to achieve a fully optimized and consistently implemented cybersecurity framework.

These findings align with the study of Bada et al. (2019), which emphasizes that organizations often demonstrate stronger technological adoption compared to human and organizational capabilities, highlighting the need for continuous capacity building and skills development to enhance overall cybersecurity readiness.

3.3. Level of Data Privacy Compliance

The results show that the indicators of data protection and security practices in the LGU are consistently rated at a very high level based on their mean scores. This indicates that data protection measures are fully implemented and fully compliant, reflecting strong cybersecurity practices across all areas.

The highest-rated indicators are "Data is regularly backed up and secured" (M = 3.48, SD = 0.65) and "Unauthorized access is monitored" (M = 3.48, SD = 0.71), both interpreted as Very High. This suggests that LGUs place strong emphasis on ensuring data availability and security through regular backups and continuous monitoring systems, demonstrating robust implementation of core data protection controls.

Table 8. *Level of Data Privacy Compliance in terms of Technical Preparedness*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Our LGU has technical measures in place to protect personal data.	3.24	0.79	Very High	Fully Implemented
2. Access to sensitive information is controlled.	3.36	0.57	Very High	Fully Implemented
3. Data is regularly backed up and secured.	3.48	0.65	Very High	Fully Implemented
4. Systems are updated to keep data safe.	3.32	0.63	Very High	Fully Implemented
5. Unauthorized access is monitored.	3.48	0.71	Very High	Fully Implemented
Overall Weighted Mean	**3.38**	**0.53**	**Very High**	**Fully Implemented**

This is followed by "Access to sensitive information is controlled" (*M* = 3.36, *SD* = 0.57), also interpreted as Very High, indicating that access management systems are effectively implemented and consistently enforced to protect sensitive information. Similarly, "Systems are updated to keep data safe" (*M* = 3.32, *SD* = 0.63) is also rated Very High, reflecting regular system maintenance and updates that contribute to safeguarding data integrity and security.

The lowest-rated indicator is "The LGU has technical measures in place to protect personal data" (*M* = 3.24, *SD* = 0.79), likewise interpreted as Very High, suggesting that while technical safeguards are fully implemented, they are relatively less emphasized compared to operational controls such as backups and monitoring.

Overall, the weighted mean of 3.38 (*SD* = 0.53), interpreted as Very High, indicates that LGUs demonstrate a strong and well-established level of data protection and cybersecurity practices. This shows that essential security mechanisms such as backups, access control, system updates, and monitoring are fully implemented, contributing to a high level of data security resilience and compliance.

According to ISO/IEC 27001 (2013), technical controls are essential in ensuring the confidentiality, integrity, and availability of information systems. Likewise, Hashizume et al. (2013) emphasize that organizations commonly prioritize technical safeguards as a primary defense layer against cyber threats, reinforcing the importance of maintaining strong data protection mechanisms.

The results from Table 9 show that the indicators of cybersecurity policy and compliance in the LGU are consistently rated at a moderately high level based on their mean scores. This indicates that cybersecurity policies and compliance mechanisms are generally mostly implemented and largely compliant, although there are still areas that require strengthening to achieve full effectiveness.

The highest-rated indicator is "Compliance is monitored and enforced" (*M* = 3.00, *SD* = 0.76), interpreted as Moderately High, with a remark of Mostly Implemented/Largely Compliant. This suggests that monitoring mechanisms are in place to ensure adherence to cybersecurity policies; however, enforcement may still need improvement to ensure consistent application across all units.

Table 9. *Level of Data Privacy Compliance in terms of Policy and Regulatory Compliance*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Our LGU has clear cybersecurity policies.	2.72	0.98	Moderately High	Mostly Implemented
2. Policies are reviewed and updated regularly.	2.84	0.80	Moderately High	Mostly Implemented
3. Compliance is monitored and enforced.	3.00	0.76	Moderately High	Mostly Implemented
4. Cybersecurity incidents are reported according to rules.	2.72	0.98	Moderately High	Mostly Implemented
5. Management supports cybersecurity compliance in IT operations and projects.	2.96	0.68	Moderately High	Mostly Implemented
Overall Weighted Mean	**2.85**	**0.70**	**Moderately High**	**Mostly Implemented**

This is followed by "Management support for cybersecurity compliance in IT operations and projects" (M = 2.96, SD = 0.68), also interpreted as Moderately High, indicating that leadership support is present and contributes to compliance efforts, but may not yet be fully strong or consistently demonstrated across all initiatives.

Next is "Policies are reviewed and updated regularly" (M = 2.84, SD = 0.80), likewise interpreted as Moderately High, suggesting that policy updates are conducted but not frequently enough to fully address emerging cybersecurity threats and evolving risks.

Both "Our LGU has clear cybersecurity policies" (M = 2.72, SD = 0.98) and "Cybersecurity incidents are reported according to rules" (M = 2.72, SD = 0.98) obtained the lowest mean scores, still interpreted as Moderately High, indicating that while policies exist and reporting procedures are established, clarity and consistent implementation remain areas for improvement.

Overall, the weighted mean of 2.85 (SD = 0.70), interpreted as Moderately High, indicates that the LGU's cybersecurity policy and compliance framework is generally in place and functional. However, while monitoring and management support show relatively stronger implementation, improvements are still needed in policy clarity, regular updates, and consistent incident reporting to strengthen overall cybersecurity governance.

According to Siponen et al. (2014), the effectiveness of cybersecurity policies largely depends on proper enforcement and employee adherence, as weak implementation can lead to non-compliance and increased security risks.

Table 10 shows that the indicators of employee compliance and data privacy awareness in the LGU are consistently rated at a moderately high level based on their mean scores. This indicates that employee compliance and awareness are generally mostly implemented and largely compliant, although there are still areas that require strengthening to achieve a higher level of effectiveness.

The highest-rated indicator is "Employees follow proper procedures to protect personal and sensitive information" (M = 3.16, SD = 0.62), interpreted as Moderately High, with a remark of Mostly Implemented/Largely Compliant. This suggests that employees generally adhere to established procedures in handling personal and sensitive data, reflecting a relatively positive level of compliance in daily operations.

Table 10. *Level of Data Privacy Compliance in terms of Employee Awareness*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Employees follow proper procedures to protect personal and sensitive information.	3.16	0.62	Moderately High	Mostly Implemented
2. Regular training programs on data privacy are conducted.	2.92	0.76	Moderately High	Mostly Implemented
3. Employees understand their roles and responsibilities in handling personal data.	2.96	0.79	Moderately High	Mostly Implemented
4. Employees know how to identify and report potential data breaches.	2.88	0.88	Moderately High	Mostly Implemented
5. Employees are aware of the LGU's data privacy policies.	2.88	0.88	Moderately High	Mostly Implemented
Overall Weighted Mean	**2.96**	**0.67**	**Moderately High**	**Mostly Implemented**

This is followed by "Employees understand their roles and responsibilities in handling personal data" (M = 2.96, SD = 0.79), also interpreted as Moderately High, indicating that employees have a reasonable understanding of their responsibilities, although consistency and depth of understanding may still vary across personnel.

Next is "Regular training programs on data privacy are conducted" (M = 2.92, SD = 0.76), likewise interpreted as Moderately High, suggesting that training activities are implemented but not yet frequent or comprehensive enough to fully strengthen employee competencies in data privacy management.

Both "Employees know how to identify and report potential data breaches" (M = 2.88, SD = 0.88) and "Employees are aware of the LGU's data privacy policies" (M = 2.88, SD = 0.88) obtained the lowest mean scores, still interpreted as Moderately High, indicating that while awareness and reporting knowledge exist, they are not yet fully developed or consistently applied across all employees.

Overall, the weighted mean of 2.96 (SD = 0.67), interpreted as Moderately High, indicates that employee compliance and data privacy awareness in the LGU are generally in place and largely compliant. However, despite this positive result, gaps remain in training frequency, policy awareness, role clarity, and breach reporting, which may affect the overall effectiveness of data privacy protection practices.

According to Kruger and Kearney (2006), employee awareness is a critical component of information security management, as human error remains a leading cause of data breaches.

Table 11 results show that the indicators of cybersecurity incident response and data privacy resilience in the LGU are consistently rated at a moderately high level based on their mean scores. This indicates that incident response and resilience practices are generally mostly implemented and largely compliant, although there are still areas that require strengthening to achieve full effectiveness.

Table 11. *Level of Data Privacy Compliance in terms of Organizational Resilience*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Our LGU has plans to respond to cybersecurity incidents.	3.48	0.51	Very High	Fully Implemented
2. The LGU updates resilience strategies to address emerging threats to data privacy.	3.00	0.71	Moderately High	Mostly Implemented
3. Recovery procedures ensure that personal data is restored securely and without loss.	3.24	0.60	Very High	Fully Implemented
4. Recovery procedures ensure that personal data is restored securely and without loss.	2.92	0.70	Moderately High	Mostly Implemented
5. Employees are trained to handle data privacy breaches and protect sensitive information.	2.96	0.79	Moderately High	Mostly Implemented
Overall Weighted Mean	**3.12**	**0.52**	**Moderately High**	**Mostly Implemented**

The highest-rated indicator is "Our LGU has plans to respond to cybersecurity incidents" (M = 3.48, SD = 0.51), interpreted as Very High, with a remark of Fully Implemented/Fully Compliant. This suggests that the LGU has strong preparedness in terms of having established and well-defined response plans for cybersecurity incidents, reflecting a high level of organizational readiness.

This is followed by "Recovery procedures ensure that personal data is restored securely and without loss" (M = 3.24, SD = 0.60), also interpreted as Very High, indicating that recovery mechanisms are effectively implemented to ensure secure restoration of data after incidents.

Next is "The LGU updates resilience strategies to address emerging threats to data privacy" (M = 3.00, SD = 0.71), interpreted as Moderately High, suggesting that the LGU is moderately proactive in updating its strategies, although improvements are still needed to ensure consistent adaptation to evolving cyber threats.

Both "Employees are trained to handle data privacy breaches and protect sensitive information" (M = 2.96, SD = 0.79) and the second instance of "Recovery procedures ensure that personal data is restored securely and without loss" (M = 2.92, SD = 0.70) obtained the lowest mean scores, both interpreted as Moderately High, indicating that employee training and some aspects of recovery implementation still require strengthening to ensure consistency and full effectiveness.

Overall, the weighted mean of 3.12 (SD = 0.52), interpreted as Moderately High, indicates that the LGU demonstrates a generally positive level of cybersecurity incident response and data privacy resilience. However, while strong foundations exist in response planning and recovery systems, gaps remain in employee training and consistent implementation of recovery procedures, which may affect overall effectiveness in managing cybersecurity incidents.

According to Linkov et al. (2013), resilience in cybersecurity requires not only response capability but also preparedness, adaptability, and continuous improvement to effectively anticipate, absorb, recover from, and adapt to cyber threats.

Table 12. *Composite Table of the Level of Data Privacy Compliance*

Indicators	Mean	SD	Verbal Interpretation	Remarks
1. Technological Preparedness	3.38	0.53	Moderately High	Mostly Implemented
2. Policy and Regulatory Compliance	2.85	0.70	Moderately High	Mostly Implemented
3. Employee Awareness	2.96	0.67	Moderately High	Mostly Implemented
4. Organizational Resilience	3.12	0.52	Moderately High	Mostly Implemented
General Overall Weighted Mean	**3.08**	**0.49**	**Moderately High**	**Mostly Implemented**

Among the indicators, Technological Preparedness obtained the highest mean score (M = 3.38, SD = 0.53), interpreted as *Moderately High* with the remark *Mostly Implemented/Largely Compliant*. This indicates that the organization is well-equipped with the necessary technological systems and tools to support data privacy protection. The relatively low standard deviation suggests that respondents consistently perceive technological preparedness as adequately established.

This is followed by Organizational Resilience (M = 3.12, SD = 0.52), also interpreted as *Moderately High*. This suggests that the organization has the capacity to respond to, recover from, and adapt to data privacy risks and incidents. It reflects the presence of mechanisms that ensure continuity and protection of data despite potential threats.

Next is Employee Awareness (M = 2.96, SD = 0.67), which remains within the *Moderately High* level. This indicates that employees have a fair level of understanding and awareness of data privacy practices, although there may still be a need for continuous training and reinforcement to ensure consistent compliance across all personnel.

Lastly, Policy and Regulatory Compliance recorded the lowest mean (M = 2.85, SD = 0.70), though still interpreted as *Moderately High.* This implies that while policies and regulations are generally followed, there may be inconsistencies in implementation or gaps in fully aligning with all required standards. The higher standard deviation suggests varied responses, indicating differences in how policies are understood or applied within the organization.

Overall, the General Weighted Mean of 3.08 (SD = 0.49) indicates a *Moderately High* level of data privacy compliance, described as *Mostly Implemented/Largely Compliant*. This means that the organization has established key data privacy measures, but continuous improvement is necessary to achieve stronger and more consistent compliance.

These findings are supported by National Institute of Standards and Technology (2020), which highlights that organizations tend to prioritize technological controls, while policy enforcement and human factors such as awareness often require sustained effort and training to reach full compliance. Similarly, Bada et al. emphasize that employee awareness and organizational practices play a critical role in strengthening overall data privacy and security compliance.

3.4. Relationship Between Variables

Table 13. *Relationship Between Variables in terms of Demographic Profile and Data Privacy Compliance*

Demographic Profile		Data Privacy Compliance			
		Technical Preparedness	**Policy and Regulation Compliance**	**Employee Awareness**	**Organizational Resilience**
Years of Service	Pearson Correlation	0.169	0.051	0.000	0.082
	Sig. (2-tailed)	0.418	0.808	1.000	0.695
	N	25	25	25	25
Educational Attainment	Pearson Correlation	0.064	0.262	0.323	0.250
	Sig. (2-tailed)	0.760	0.206	0.115	0.228
	N	25	25	25	25
ICT Training	Pearson Correlation	0.349	0.046	-0.034	0.082
	Sig. (2-tailed)	0.087	0.827	0.872	0.698
	N	25	25	25	25
LGU type	Pearson Correlation	-0.101	0.200	.474*	0.351
	Sig. (2-tailed)	0.632	0.337	0.017	0.086
	N	25	25	25	25

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Table 13 shows that most demographic variables, such as years of service, educational attainment, and ICT training, have no significant relationship with data privacy compliance, as evidenced by their respective p-values exceeding the 0.05 level of significance. This indicates that individual characteristics alone do not substantially influence how respondents comply with data privacy requirements. In other words, regardless of experience, educational background, or prior ICT exposure, employees tend to exhibit similar levels of compliance, suggesting that compliance behavior may be shaped more by organizational systems and structures rather than personal attributes.

However, a notable exception is observed in the case of LGU type, which shows a significant relationship with employee awareness ($r = 0.474$, $p = 0.017$). This moderate positive correlation implies that the type of local government unit, whether city or municipality, has a meaningful influence on the level of awareness among employees regarding data privacy practices. Specifically, it can be inferred that respondents from one type of LGU (most likely cities) may demonstrate higher levels of awareness compared to those from municipalities, potentially due to better access to resources, infrastructure, and training programs.

This finding highlights the importance of organizational context in shaping cybersecurity and data privacy outcomes. Differences in budget allocation, availability of ICT infrastructure, leadership priorities, and exposure to national initiatives may contribute to variations in awareness levels across LGUs. For

instance, city LGUs are often more equipped with dedicated IT personnel, structured training programs, and stronger policy enforcement mechanisms, whereas municipal LGUs may face constraints in these areas.

The result is consistent with the study by Puhakainen and Siponen (2010), which emphasized that the organizational environment plays a critical role in shaping employees' security awareness and compliance behavior. They argue that effective awareness is not solely dependent on individual knowledge but is largely driven by organizational support, continuous training, and enforcement of security policies. Similarly, Parsons et al. (2017) noted that organizational culture and management support significantly affect how employees perceive and respond to cybersecurity responsibilities.

Moreover, this finding aligns with socio-technical systems theory, which posits that organizational outcomes, such as data privacy compliance, are shaped by the interaction among people, technology, and organizational structures. Even if employees possess similar qualifications or experience, differences in organizational environment can lead to varying levels of awareness and behavior.

Table 14 presents the relationship between cybersecurity readiness and data privacy compliance across four key areas: technical preparedness, policy and regulation compliance, employee awareness, and organizational resilience. Overall, the results show strong and significant positive relationships, meaning that as cybersecurity readiness improves, data privacy compliance also increases.

In terms of technological resources, the correlation values show a high positive relationship with technical preparedness (r = .712, p < .001), policy and regulation compliance (r = .657, p < .001), and organizational resilience (r = .720, p < .001), while a moderate positive relationship is observed with employee awareness (r = .596, p < .001). Based on Guilford's Rule of Thumb, these findings suggest that improvements in technological resources are strongly associated with enhanced data privacy compliance, particularly in system preparedness and organizational resilience.

Table 14. *Relationship Between Variables in terms of Cybersecurity Readiness and Data Privacy Compliance*

Cybersecurity Readiness		**Data Privacy Compliance**			
		Technical Preparedness	**Policy and Regulation Compliance**	**Employee Awareness**	**Organizational Resilience**
Technological Resources	Pearson Correlation	.712**	.657**	.596**	.720**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001
	N	25	25	25	25
Organizational Resources and Competencies	Pearson Correlation	.667**	.715**	.789**	.708**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001
	N	25	25	25	25
Environmental Mandates	Pearson Correlation	.625**	.665**	.674**	.693**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001
	N	25	25	25	25

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

For organizational resources and competencies, the results reveal a moderate to high positive relationship with technical preparedness ($r = .667$, $p < .001$), policy and regulation compliance ($r = .715$, $p < .001$), employee awareness ($r = .789$, $p < .001$), and organizational resilience ($r = .708$, $p < .001$). Notably, employee awareness demonstrates a high positive correlation, indicating that strengthening organizational capacity significantly contributes to improving employee understanding and adherence to data privacy practices.

Meanwhile, environmental mandates show a moderate positive relationship with technical preparedness ($r = .625$, $p < .001$), policy and regulation compliance ($r = .665$, $p < .001$), employee awareness ($r = .674$, $p < .001$), and organizational resilience ($r = .693$, $p < .001$). These results imply that external policies and regulatory requirements play an important role in influencing LGU compliance, although their impact is slightly less strong compared to technological and organizational factors.

Overall, all correlation values are statistically significant ($p < .001$), indicating strong evidence of relationships between variables. Using Guilford's Rule of Thumb, the findings confirm that cybersecurity readiness has a moderate to high positive correlation with data privacy compliance. This suggests that as LGUs improve their technological infrastructure, organizational capabilities, and adherence to environmental mandates, their level of data privacy compliance correspondingly increases.

4. Summary, Conclusions, Recommendations

4.1. Summary of Findings

This section presents the key findings of the study, highlighting the demographic profile of respondents, their level of cybersecurity readiness, data privacy compliance, and the relationship among variables.

First, the findings reveal that most respondents are early in their careers and possess only basic ICT training. A large proportion of participants have 1–5 years of service, followed by those with less than one year, indicating a relatively young and less experienced workforce. In addition, most respondents are college graduates, while only a few hold master's degrees. In terms of ICT competencies, the majority have basic ICT training, with limited exposure to advanced or cybersecurity-specific training. This suggests that employees generally have foundational ICT knowledge but lack specialized skills needed for advanced cybersecurity and data privacy functions.

Second, cybersecurity readiness across LGUs is generally at a moderately high to very high level, indicating that many practices are already in place. Strong areas include technical infrastructure such as system backups, secure data storage, endpoint security, and access controls, which are largely fully implemented. However, moderately rated areas include employee training, awareness programs, policy consistency, and simulation exercises. This indicates that while technical safeguards are well established, human and organizational components still require strengthening.

Third, data privacy compliance is also generally moderately high to very high, with stronger performance in technical controls such as data backup, monitoring, access restriction, and system updates. LGUs demonstrate effective implementation of security mechanisms that protect data confidentiality and integrity. However, gaps remain in employee awareness, training, and consistent application of policies, suggesting that compliance is stronger in technical implementation than in behavioral and organizational practices.

Fourth, the results show that demographic factors have limited influence on cybersecurity readiness and data privacy compliance. Most variables such as years of service, educational attainment, and ICT training do not significantly affect compliance levels. However, differences between city and municipal LGUs may influence implementation due to variations in resources, infrastructure, and administrative capacity.

Finally, the findings reveal a significant positive relationship between cybersecurity readiness and

data privacy compliance. This means that as LGUs strengthen their cybersecurity systems, policies, and incident response mechanisms, their level of compliance with data privacy requirements also improves.

4.2. Conclusions

The findings of the study show that LGUs are generally well-equipped but still improving in terms of cybersecurity and data privacy. While essential systems and practices are already in place, implementation is not yet fully uniform across all areas.

A clear pattern in the results is that technical systems are strong, but human and organizational factors remain the weakest areas. LGUs have reliable systems such as backups, access controls, and monitoring tools; however, employee awareness, training, and behavior still need improvement. This indicates that technology alone is not sufficient without proper human understanding and usage.

Another important finding is that training, awareness, and policy enforcement remain inconsistent. Although policies exist, they are not always clearly understood or strictly implemented. This creates gaps that may expose LGUs to cybersecurity risks, particularly since human error remains a major vulnerability.

Finally, the study confirms that improving cybersecurity readiness leads to better data privacy compliance. Strengthening systems, policies, and training programs enhances LGUs' ability to protect sensitive information. This highlights that cybersecurity and data privacy are interdependent and must be improved together.

Based on these findings, the null hypothesis stating that there is no significant relationship between the level of cybersecurity readiness and data privacy compliance with respect to the demographic profile of the respondents is accepted (or failed to be rejected).

4.3. Recommendations

Based on the findings, several recommendations are proposed to improve cybersecurity readiness and data privacy compliance in LGUs.

First, LGUs should strengthen employee training programs by providing regular, structured, and specialized cybersecurity and data privacy training. Since human factors remain a key weakness, improving employee knowledge and skills is essential to reducing risks caused by human error.

Second, LGUs should improve the implementation and communication of cybersecurity policies. Policies must be regularly reviewed, updated, and clearly disseminated to ensure that all employees fully understand and comply with established guidelines.

Third, continuous awareness programs should be conducted. Seminars, workshops, and campaigns on phishing, social engineering, and data protection should be strengthened to improve employee vigilance and awareness.

Fourth, LGUs should enhance organizational capacity by developing internal cybersecurity expertise and strengthening IT governance structures. This is especially important for sustaining long-term cybersecurity resilience.

Fifth, municipal LGUs should be given additional support, including funding, technical assistance, and training opportunities, to reduce gaps between municipalities and cities in terms of cybersecurity implementation.

Lastly, LGUs should institutionalize continuous monitoring and evaluation systems to regularly assess cybersecurity readiness and data privacy compliance. This will help identify weaknesses, track progress, and ensure continuous improvement.

Overall, cybersecurity and data privacy improvement require a balanced approach involving technology, people, and organizational systems working together to ensure effective protection of sensitive information.

4.4. Proposed Action Plan

The proposed action plan is designed to enhance the organization's cybersecurity readiness and data privacy compliance by addressing the areas that require continuous improvement based on the study's findings. Although the results revealed a *moderately high* level of implementation, the plan focuses on strengthening leadership support, improving policy compliance, minimizing risks, upgrading technological capabilities, and increasing awareness among personnel.

First, strengthening leadership support and accountability is a key priority in the action plan. This includes appointing a Data Protection Officer (DPO), allocating sufficient budget for cybersecurity and data privacy programs, and integrating data privacy into the LGU's strategic plans to ensure sustainability. These initiatives demonstrate organizational commitment and align with the Data Privacy Act of 2012, which requires the implementation of appropriate measures to protect personal data.

Table 15. *Proposed Action Plan*

Objectives	**Strategies / Activities**	**Persons Responsible**	**Time Frame**	**Expected Output**
Strengthen leadership support and accountability	Appoint/designate a Data Protection Officer (DPO)	LGU Head / HR	Immediate	Active DPO in LGU
	Allocate budget for cybersecurity and data privacy programs	LGU Management / Budget Office	Annual	Increased funding support
	Integrate data privacy in LGU strategic plans	LGU Officials	Annual	Institutionalized privacy governance
Improve compliance with data privacy laws	Review and update data privacy policies	DPO / Legal Office	Semi-annual	Updated policies
	Develop standard operating procedures (SOPs) for data handling	DPO / IT Office	Semi-annual	Clear procedures implemented
	Conduct policy orientation sessions	HR / DPO	Quarterly	Increased compliance awareness
Identify and mitigate data privacy risks	Conduct Privacy Impact Assessments (PIA)	DPO / IT Office	Annual	Identified risks and mitigation plans
	Perform regular risk assessments and audits	Internal Audit Unit	Quarterly	Reduced vulnerabilities
	Establish an incident reporting system	IT Office / DPO	Continuous	Improved incident tracking
Enhance cybersecurity infrastructure	Upgrade systems and security tools (firewalls, antivirus)	IT Department	Annual	Improved system security
	Implement access control and data	IT Department	Continuous	Secured data access

	encryption			
	Conduct regular system monitoring and maintenance	IT Department	Monthly	Reduced cyber threats
Increase awareness and protect data subject rights	Conduct data privacy awareness campaigns	HR / DPO	Quarterly	Increased employee awareness
	Establish a mechanism for handling data subject requests	DPO	Continuous	Efficient response system
	Integrate privacy training in onboarding programs	HR Office	Continuous	Informed employees

Second, the plan aims to improve compliance with data privacy laws by regularly reviewing and updating policies to ensure alignment with existing regulations. The development of standard operating procedures (SOPs) provides clear guidance on proper data handling, while policy orientation sessions help ensure that all employees understand and consistently follow these guidelines. These initiatives support compliance with Data Privacy Act of 2012, particularly in promoting accountability and lawful processing of personal information.

Third, to identify and mitigate data privacy risks, the action plan includes conducting Privacy Impact Assessments (PIAs) and regular risk assessments. These activities help proactively identify vulnerabilities and implement appropriate mitigation strategies. Establishing an incident reporting system further strengthens the organization's ability to respond effectively to data breaches and security incidents, consistent with the risk management and breach notification principles outlined in the Data Privacy Act of 2012.

Fourth, the plan emphasizes the need to enhance cybersecurity infrastructure. Upgrading systems and security tools, such as firewalls and antivirus software, ensures stronger protection against cyber threats. Implementing access control and data encryption safeguards sensitive information, while regular system monitoring and maintenance reduce the likelihood of security breaches. These measures support the law's requirement for implementing adequate security measures to ensure data protection.

Finally, the plan focuses on increasing awareness and protecting data subject rights. Conducting data privacy awareness campaigns and integrating privacy training into onboarding programs help build a culture of accountability among employees. Establishing mechanisms for handling data subject requests ensures that individuals' rights are respected and addressed efficiently. This is in line with the provisions of the Data Privacy Act of 2012, which upholds the rights of data subjects and requires organizations to ensure transparency and responsiveness.

Overall, this action plan provides a structured and practical approach to improving both cybersecurity readiness and data privacy compliance. It translates the study's findings into actionable steps that promote continuous improvement, strengthen organizational capacity, and ensure adherence to national data privacy regulations.

Acknowledgement

I want to express my sincere gratitude to the Dean of the College of Business Administration and Accountancy (CBAA)**, DR. MARY JANE DIAZ FUENTES**, for granting me the opportunity to undertake and complete this research.

I am deeply thankful to my Thesis Adviser**, ATTY. RUSHID JAY S. SANCON**, for the continuous guidance, valuable insights, and unwavering support throughout this study.

I would also like to extend my appreciation to my Subject Specialist, **ROLANDO CRUZADA JR, DPA,** for sharing his expertise and providing meaningful suggestions that improved the quality of this research.

My sincere thanks are given to my Internal Statistician**, VICTOR A. ESTALILLA JR., MA,** and External Statistician**, ENGR. MANUEL LUIS, R. ALVAREZ**, for the assistance in data analysis and interpretation, which greatly contributed to the accuracy and reliability of the findings.

I am also grateful to my External Panel, **IMEE PRESCILLA P. SANCHEZ, PhD**, for offering professional insights and constructive recommendations that enhanced this study.

Special thanks are extended to my Technical Expert, **ETHELMAY B. ROMERO, DBA**, for providing the necessary technical support and assistance during the research process.

I would also like to acknowledge my Language Expert, **MAIDA OLVIGA SARMIENTO**, for helping refine the clarity, coherence, and overall presentation of this paper.

I am equally thankful to my friends and classmates for their encouragement, support, and cooperation throughout this study.

Finally, I would like to express my deepest gratitude to my family, especially my wife and children, for their constant encouragement, understanding, and unwavering support that made this research possible.

"The Researcher"

References

Anderson, T., & Kim, S. (2019). Cybersecurity workforce challenges in local governments. *Journal of Information Security, 10*(2), 85–97.

Ayuyang, D. M., & Ayuyang, R. (2025). *Strengthening data privacy and cybersecurity awareness for university employees in the Philippines* (Unpublished policy brief).

Brighton, L., & Evans, R. (2021). The role of cybersecurity specialists in government compliance. *Government Information Quarterly, 38*(4), 101–110.

Buenaventura, D. J., et al. (2024). *A comparative study of the Philippines in a global cybersecurity context* (Unpublished research).

De la Cruz, J. (2022). Data privacy compliance in Philippine local government units. *Philippine Journal of Public Administration, 66*(1), 45–60.

Delos Reyes, M. (2020). Barriers to cybersecurity implementation in Philippine LGUs. *Journal of Local Governance, 12*(2), 77–92.

Department of Information and Communications Technology. (2020). *State of ICT development in local government units.*

Department of Information and Communications Technology. (2020). *State of ICT development in local government units.*

Department of Information and Communications Technology. (2022). *National cybersecurity plan 2022 and beyond.*

Department of Information and Communications Technology. (2022). *National cybersecurity plan 2022 and beyond.*

Domingo, R. (2021). Cybersecurity practices in selected local government units in the Philippines. *Asian Journal of Public Administration, 43*(3), 210–225.

Duggan, M., & Doyle, A. (2020). Cybersecurity risks in local governments: A global perspective. *Public Administration Review, 80*(5), 789–799.

Greenleaf, G. (2014). Global data privacy laws 2014: 89 countries, and accelerating. *Privacy Laws & Business International Report*, (128), 1–6.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), Article 5. https://doi.org/10.1186/1869-0238-4-5

Ilagan, J., & Montelibano, A. (2020). Compliance with the Data Privacy Act among Philippine LGUs. *Philippine Governance Review, 8*(1), 33–47.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 information technology—Security techniques—Information security management systems—Requirements.*

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 information technology—Security techniques—Information security management systems—Requirements.*

ISACA. (2020). *Cybersecurity fundamentals: A handbook for the digital age.* ISACA.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Linkov, I., et al. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

Lopez, G., & Chen, Y. (2020). Risk management practices in government cybersecurity. *International Journal of Cybersecurity, 5*(2), 120–134.

Marquez, P., & Bautista, L. (2020). Disparities in cybersecurity readiness among LGUs in Luzon. *Philippine Journal of Development Studies, 15*(2), 98–115.

Massey, A., Smith, J., & Brown, K. (2020). Technological infrastructure and cybersecurity readiness. *Journal of Cyber Policy, 5*(1), 50–65.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1).* https://www.nist.gov

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1).* https://www.nist.gov

National Privacy Commission. (2021). *Data privacy awareness and compliance survey report.*

National Privacy Commission. (2021). *Data privacy awareness and compliance survey report.*

National Privacy Commission. (2024). *Raising the level of cybersecurity awareness and data privacy compliance in government agencies*. https://privacy.gov.ph

National Privacy Commission. (2024). *Raising the level of cybersecurity awareness and data privacy compliance in government agencies*. https://privacy.gov.ph

Ona, M. A. (2024). *Extent of implementation of cybersecurity solutions in the Philippines* (Unpublished research).

Parsons, K., et al. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 59*, 77–90. https://doi.org/10.1016/j.cose.2016.12.003

Pascual, D., & Reganit, M. (2021). Leadership and training as predictors of cybersecurity readiness. *Journal of Public Sector Innovation, 6*(1), 55–70.

Peterson, R., & Lawrence, D. (2020). Cybersecurity strategies in U.S. local governments. *American Review of Public Administration, 50*(6), 567–580.

Philippine Institute for Development Studies. (2021). *Cybersecurity and data privacy awareness in the Philippines*. https://www.pids.gov.ph

Philippine Institute for Development Studies. (2021). *Cybersecurity and data privacy awareness in the Philippines*. https://www.pids.gov.ph

Reeves, J. (2019). Cybersecurity governance in developing countries. *Information Systems Journal, 29*(3), 445–460.

Republic Act No. 10173. (2012). *Data Privacy Act of 2012*. https://www.officialgazette.gov.ph

Republic Act No. 10173. (2012). *Data Privacy Act of 2012*. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph

Santos, K., & Cruz, M. (2021). Data protection officer compliance in Philippine LGUs. *Philippine Journal of Public Policy, 13*(2), 88–102.

Siponen, M., et al. (2014). Employees' adherence to information security policies. *Information & Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Steed, C., & Rhodes, T. (2019). Cybersecurity standards in European municipalities. *European Journal of Information Systems, 28*(4), 389–405.

Velasco, M., & Tan, L. (2021). Employee awareness and cybersecurity practices. *Asia-Pacific Journal of Information Systems, 31*(2), 140–155.

Williams, H. (2022). Resource constraints in local government cybersecurity. *Journal of Cybersecurity Management, 7*(1), 15–29.

Wright, B., & Marshall, D. (2022). Leadership and cybersecurity policy implementation. *Government Information Quarterly, 39*(2), 101–115.