International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@i om

Records Management and Data Security in the Local Government Units

Via U. Tabia

Administrative Aide I
Sangguniang Panlalawigan
Provincial Government of Laguna

Abstract

This research about records management and data security are critical components in the effective functioning of Local Government Units (LGUs). Proper management of records ensures that essential documents are accurately filed, easily accessible, and maintained in compliance with legal, regulatory, and policy requirements. Efficient records management systems support transparency, accountability, and smooth administrative processes, fostering public trust and effective governance. Meanwhile, data security safeguards the confidentiality, integrity, and availability of sensitive information, protecting both citizens and the government from unauthorized access, data breaches, and cyber threats. In an era of rapid technological advancements, LGUs must adopt modern tools and practices to securely store and manage records while ensuring compliance with data protection laws.

The results of integrating efficient records management systems with robust data security measures to improve operational efficiency, prevent data loss, and uphold the public's right to privacy and security in local government operations. The research offers suggestions for enhancing the records management and data security in the local government unit.

Keywords: Records Managament, Data Secuirty, Records Retention, Retention Schedule, Retention Periods, Data Breaching, Access Control

THE PROBLEM AND ITS BACKGROUND

Introduction

In a data-driven world that is currently unfolding, local government units are capacitated to manage huge volumes of information relevant to good governance and service delivery. In fact, as custodians of public records, they handle numerous documents as part of their civic duties—from citizen records and financial data to planning documents and policy archives. The effective management of records in this respect is therefore crucial, not only to the operation of local government but also to transparency, accountability, and trust.

However, the issues of records division management and data protection of LGUs are numerous and complex. In most LGUs, outdated technologies and a lack of resources hinder their capacity to provide clearer and more easily accessible records.

Moreover, a growing body of data privacy and security regulations increases the need for even the least frequently used systems to maintain near-continuous operations in compliance with legal requirements to protect sensitive information.

Local governments are now at the epicenter of cyberattacks. Such breaches can cause severe losses that may overwhelm an otherwise very robust financial base, damage reputations, and, more importantly, compromise citizens' personal information. The urgency of having robust cybersecurity measures and comprehensive disaster recovery plans has never been more pressing.

Thus, even with a national archive agency and the strong support of the Philippine Archives Act, LGUs still face significant challenges such as staff training and retention. Most LGUs experience high turnover, resulting in the loss of valuable institutional knowledge and expertise in records management. This affects the quality of data management and the overall efficiency and effectiveness of local governance.

Background of the Study

In the current administrative era, it is already understood that records management and data protection are fundamental aspects of running Local Government Units (LGUs). The more extensively digital technologies are used in local governments to enable service provision, the greater the need for effective record management and data security strategies.

Local Government Units are the arms of the state that are closest to the citizenry. They provide services, implement policies, and promote participation. The very nature of carrying out these functions generates and preserves extensive records, such as the movement of files from office to office, records of activities, and most importantly, personal details of the citizens.

To arrange, keep, and recover such data speedily and cost-effectively, a records management system should be in place. These systems improve service delivery, help ensure compliance with legal provisions, and promote transparency and accountability in government.

Yet, these significant functions are hindered by numerous challenges in most of the LGUs. More frequently, a lack of financial resources prevents them from adopting modern technologies for information management and enhancing security systems. Also, the theoretical and practical knowledge of records management and information safeguarding techniques may not be adequately imparted to the staff of most of the LGUs, resulting in inefficiency and exposing the systems to a greater risk of being compromised. Their record systems are also disconnected leading to impeded access and a lack of integration across different departmental silos.

Furthermore, there are drawbacks to the development of technology, particularly the elevated dangers of cyberattacks. The significance of putting in place appropriate and efficient security measures for devolved governance units has been brought to light by instances of data breaches and cyberattacks. The need for systems with features that guarantee sensitive information is kept safe and confidential is highlighted by the ineffective security of classified data.

The purpose of this study was to ascertain the Local Government unit complied with national and international regulations pertaining to record retention, data privacy, protection. It also noted the typical difficulties the LGU has in preserving data security and records management. To guarantee better service delivery and adherence to relevant regulations, the study suggested enhancing data security and records management procedures.

Theoretical Framework

The theoretical framework incorporates a number of theories that are pertinent to the foundation of this study on the issues and best practices for data security and records management in LGUs. The acceptance or adoption of information technology (IT) has drawn a lot of attention in the past ten years. The acceptance behavior of end users has been explained by a number of theoretical models. The most widely used and empirically tested of these is Davis's (1989) Technology Acceptance Model (TAM). Since its inception, TAM has been the subject of dozens of empirical studies. TAM is thought to be more robust, predictive, and economical than its rival models (Venkatesh & Davis, 2000).

Pasmore et al. state that the socio-technical approach is a way of looking at organizations that highlights how the social and the socio-technical approach, according to Pasmore et al., is a way of looking at organizations that highlights how the social and technological innovations components of the organization work together and how the organization as a whole relates to its surroundings.

By emphasizing the interplay between the technical (system design, infrastructure) and social (human, organizational, and cultural) aspects of the adoption of technology, socio-technical system theory (STST) provides an important point of view.

In order to explain how organizational factors and external pressures impact technology adoption, this framework integrates a number of theories. External factors like industry standards and regulatory pressures impact the system's design and support, which in turn impacts how users perceive the system's utility and usability. As TAM, users' decisions to adopt the technology are heavily influenced by these perceptions. In order to ensure successful adoption, the Socio-Technical System Theory (STST) also highlights how crucial it is to match the technology with the organization's culture and employee skill set. Additionally, this model's feedback loop suggests that as users make use of the technology, their experiences and input could result in additional system design enhancements as well as modifications to the external environment, like adjustments to industry standards or laws. This cycle of adaptation guarantees that the technology stays effective, relevant, and in line with the social and technical requirements of the company.

Conceptual Framework

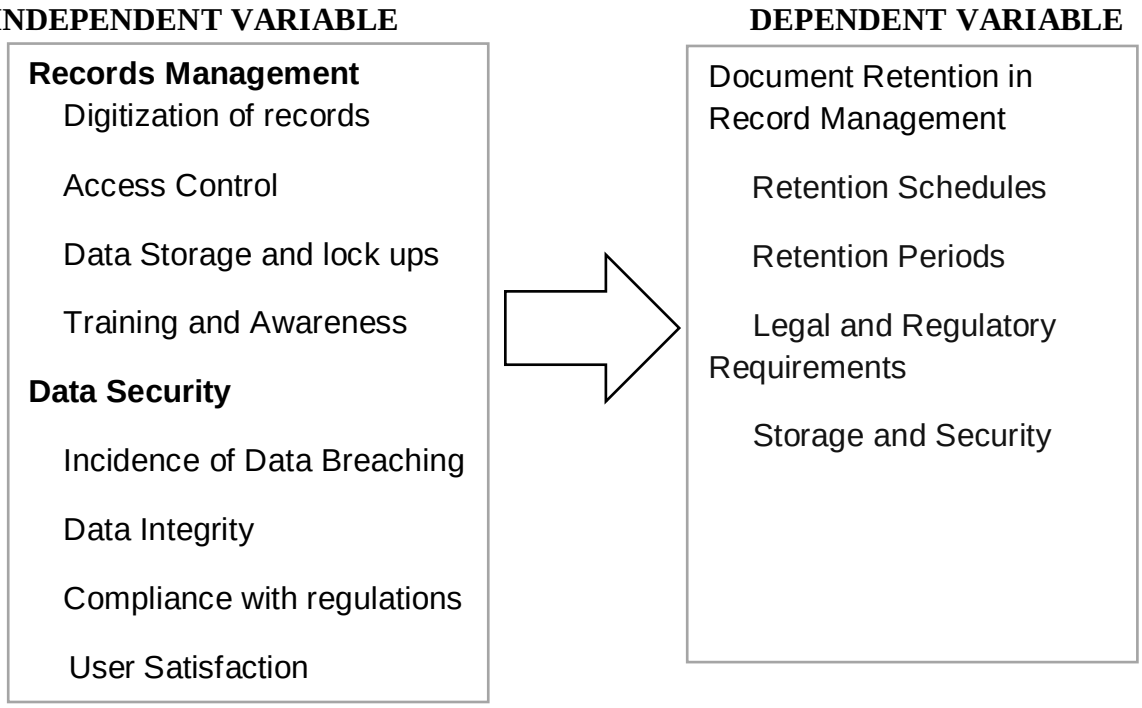

Figure 3. The Research Paradigm of the Study

Statement of the Problem

This study sought to measure the impact of Records Management and Data Security in government on the performance standards of Local Government Units.

Specifically, it answered the following questions:

1. What is the level of records management towards the performance standards with regard to:
   1.1 Digitization of records;
   1.2 Access control;
   1.3 Data storage and lock-ups; and
   1.4 Training and awareness?
2. What is the level of data security in the government in terms of:
   2.1 Incidence of data breaching;
   2.2 Data Integrity;
   2.3 Compliance with regulations; and
   2.4 User Satisfaction?

3. What is the level of document retention in records management?
4. Is there a significant relationship between records management and the level of document retention in Local Government Units?
5. Is there a significant relationship between data security and performance standards in Local Government Units?

Research Hypothesis

There is no significant relationship between the personnel's profile and records management and the performance standards of Local Government Units in Laguna.

Scope and Limitations of the Study

This study focused on the effective management of records and the safeguarding of sensitive data, which were central to the proper functioning of LGUs.

Significance of the Study

This study focused on the impact of personnel profiles and functions on performance standards in the Local Government Unit Offices.

This study is limited only to the records of staff and personnel working in the Local Government Units in the 1st Class, 2nd Class, 3rd Class, 4th Class Municipalities, and in one of the three cities in Laguna:

Definition of Terms

The following terms were defined operationally for a clearer understanding of the study:

Local Government Unit. Refers to as the backbone of local governance in the Philippines, playing a crucial role in the country's administrative and developmental framework.

Access Control refers to setting up permissions and restrictions on users based on their roles, identities, or other factors to protect sensitive data from unauthorized access.

Data Storage. Refers to the methods and technologies used to save and maintain data in a secure and accessible manner.

Digitization. Refers to the process of converting something to digital form.

Data Breach. Refers to the unauthorized access, acquisition, or disclosure of sensitive or confidential data

Data Integrity. Refers to the accuracy, consistency, and reliability of data throughout its lifecycle.

Document Retention. Refers to a system that allows them and their employees to automatically create policies and determine what should be done with particular documents or records

Records Management. This refers to the division that programs the record's life cycle, maintains and adopts effective techniques in controlling forms, reports, correspondence and related paperwork operations, and functional retention and storage areas for documents under custody.

Regulations. Refers to ensure compliance with laws, protect public welfare, and maintain order.

Training and Awareness. Process of educating employees or users about security practices, policies, and tools to help prevent cyberattacks, data breaches, and other security risks.

User Satisfaction. Refers to how products, services, or experiences meet or exceed the expectations of users or customers.

REVIEW OF RELATED STUDIES AND LITERATURE

The review of the literature and related studies are included in this chapter. The following selection of literature and studies comes from authors and research personalities and offers a logical connection to the study's perspectives, theories, and conclusions that could aid in resolving the issues brought up in this investigation.

Review of Related Literature

The 2024 study looked into how records management affected the performance of HRM in the public sector, which found that strong records management procedures greatly improved a number of HRM outcomes. Higher employee motivation, transparent hiring, effective dispute resolution, and well-informed decision-making are all facilitated by established electronic records systems, consistent filing, and efficient monitoring, according to the study. Good records management makes it easier to monitor staff performance and training requirements, promotes retention by maintaining institutional knowledge, and makes it possible to conduct fair hiring procedures by keeping thorough applicant records. Employee utilization and retention issues still exist, nevertheless, underscoring the necessity of more funding for records administration capabilities and connection with HRM procedures.

A systematic review on cybersecurity in local governments highlights that while most cyber incidents tend to be minor, the frequency of breaches remains a significant concern, requiring ongoing prevention and response efforts. The 2025 Data Breach Investigations Report by Verizon underscores that public sector organizations face increasingly sophisticated attacks, emphasizing the critical need for effective incident response planning and employee training to reduce breach frequency and impact.

Likewise, according to a 2024 report on records management risks, the increasing use of cloud computing and digital storage has not only increased accessibility and reduced costs, but also has brought about serious cybersecurity risks like insider threats, data breaches, and vulnerabilities associated with new technologies like AI hacking, IoT attacks, and quantum computing. To reduce these risks and guarantee adherence to laws like the CCPA and GDPR, the report suggests strong cybersecurity solutions like encryption, multi-factor authentication, secure data disposal rules, and frequent audits.

Adu (2020) noted that corruption has been easier for government agencies due to inefficiencies in records management.

Adusei and Mensah Senyah (2022) examined that staff knowledge on records management in Ghanaian local governments found awareness of policies and procedures, including data privacy and security, which was high among staff. Their study emphasized the importance of management support, resource allocation, and staff training to enhance records management effectiveness, including safeguarding sensitive information through proper access controls1. This aligns with the LGU respondents' strong agreement on robust authentication methods and restricted access to sensitive records.

During testing or development, data masking lowers the risk of exposure by substituting real-looking but fake data for sensitive information. Data mining on encrypted data is made possible by methods like secure multiparty computation and homomorphic encryption, which permit analysis without jeopardizing privacy (Alghamdi et al., 2023).

Alharkan et al. (2024) highlighted the cybersecurity challenges faced by local governments, emphasizing the need for secure data infrastructure that includes physical and digital safeguards, encryption, and regular system maintenance to protect sensitive information from evolving threats12. This aligns with respondents' recognition of secure storage locations and encryption use within the LGU.

Artificial intelligence is becoming more significant in the field of archival science. Their comprehensive review explores how AI enhances the automation of records management and facilitates better data retrieval, while also highlighting the necessity of ethical considerations and interdisciplinary collaboration (Ali, M. S., Özdemir, V., & Hutton, J., 2024).

According to Burnes et al. (2020), data breaches occur when personal information is used fraudulently, including to obtain government assistance and other services.Effective records management is pivotal for improving public service delivery. Indicators of a robust records management program include all staff creating and maintaining accurate records, easy accessibility of records, awareness of organizational policies, secure storage, and proper disposal of records Cayrat & Boxall (2023).

Data privacy refers to protecting sensitive information from unauthorized access, use, or disclosure and ensuring that individuals have control over their personal data Chua et al. (2021).

According to Cobalt's 2025 cybersecurity statistics, 70% of breaches resulted in major operational disruptions, and cyberattacks rose by 30% in the second quarter of 2024 over the same period the year before. Because of increased attack surfaces and changing workplace hazards, remote work has increased breach costs by an average of $173,000 per occurrence. Additionally, as businesses look to reduce the growing financial risks associated with cyber disasters, cyber insurance rates are rapidly increasing and are expected to double by 2027.

CM-Alliance (2025) examined how self-storage facilities have changed over time, pointing out that many now incorporate cutting-edge digital security features. To safeguard both digital and physical assets, they include smart access codes, biometric and face recognition access, and round-the-clock surveillance. The research also highlights the increasing popularity of climate-controlled units and cloud-based access, which enables users to safely and remotely manage and recover data. The growing need for hybrid storage options that offer strong physical protection together with the ease of digital access is reflected in this change.

The importance of this topic is demonstrated by the European Council's announcement in April 2021 that a centre of excellence for cybersecurity will be established to pool investments in research, technology, and industrial development. This center aims to increase the security of the Internet and other critical network and information systems European Council (2021).

A study by Fowler & Harris (2022) found that cloud-based records management systems offer scalability, remote access, and built-in security features such as data encryption and multi-factor authentication. However, cloud-based solutions must be carefully selected and managed to meet the specific data security and compliance needs of local governments.

According to the literature, there is no standard integrated definition for Governance, Risk, and Compliance (GRC) Racz et al. (2014). In light of this, there is a need to develop one. They proposed a single-phrase definition for GRC: an integrated, holistic approach to organization-wide governance, risk, and compliance, ensuring that an organization acts ethically, aligns with its risk appetite, internal

policies, and external regulations, and integrates strategy, processes, technology, and people to improve efficiency and effectiveness.

Mandatory Access Control (MAC) enforces access control policies defined by system administrators or security administrators, restricting users' ability to modify access permissions Cho et al. (2021).

According to Dada (2020), a record is the brain box of information packaged in different formats that lives on after the creator's death, passing from generation to generation. In most academic institutions, records come in various formats, from digital to hard copies, and can be stored in physical or cloud-based spaces.

Dootson et al. (2021) noted that records management in the public sector is integral to delivering public goods. However, several institutional challenges inhibit the implementation of innovative and information-centric tools to transform records.

Dunleavy et al. (2006) highlighted both the challenges of digitalization and the opportunities presented by internet technologies to improve public administration. In doing so, they introduce DEG as a new quasi-paradigm for public administration and take a firm position on the positive service benefits of digitalization.

Digitalization, with electronic delivery channels becoming the transformative central approach rather than being supplementary, is causing agencies to become their websites Dunleavy et al. (2022).

Records management is a subject that has become more interesting over the last decade. It has always been an asset for efficient and effective business and may seem strange that this highly significant driver of business efficiency has received so little attention over the years in the developing countries and particularly in (Ghana. Adusei, C. and Mensah Senyah, M., 2022)

Across all industries, data breaches impact numerous users and impose a high cost on organizations IBM (2022).

The transition to digital student registration and record-keeping at three private universities in the Philippines has enhanced administrative efficiency by addressing problems such as incomplete admission documents and non-compliance with scheduling. (Morallos, L. M. R., 2022).

According to the International Association of Privacy Professionals (IAPP), the Philippines' Data Privacy Act mandates that organizations notify the National Privacy Commission and affected data subjects within 72 hours of becoming aware of a data breach. Failure to comply can result in penalties, including fines and imprisonment.

As stated by the National Privacy Commission (NPC), as of August 31, 2024, over 6.8 billion security incidents had been reported in the Philippines since 2018. In 2023 alone, the government reported the highest number of data breaches, followed by the financial services and retail sectors. The top causes included malicious attacks, such as hacking and ransomware, and human errors, like document misdelivery and accidental emails.

According to the National Privacy Commission's Circular 2023-06, organizations must designate a Data Protection Officer, conduct privacy impact assessments, and implement a privacy management program. Additionally, they must ensure that personal data is stored securely and retained only for as long as necessary, and implement a business continuity plan that includes data backups.

Data breaches are security incidents that jeopardize the confidentiality, integrity, and availability of protected, sensitive, or confidential data held by organizations Khan et al. (2021).

Globalization, digitalization and smart technologies have escalated the propensity and severity of cybercrime. While it is an emerging field of research and industry, the importance of robust cybersecurity defence systems has been highlighted at the corporate, national, and supranational levels. The impacts of inadequate cybersecurity are estimated to have cost the global economy USD 945 billion in 2020 Maleks-Smith et al. (2020).

Addressing the challenges of privacy and data protection necessitates the incorporation of privacy-enhancing technologies into blockchain systems. These technologies are engineered to anonymize transactions, shield user identities, and prevent sensitive information from being divulged on the blockchain. Techniques such as zero-knowledge proofs and ring signatures enhance anonymity and confidentiality, allowing users to engage in transactions without revealing their identities Mahmood & Vacius (2020).

Mohammed et al. (2022) argued that records management in the institution is challenged by improper records management; inadequate proper security for records; inadequate professionally trained records managers; there are inadequate resources to facilitate proper records management practices in the institution; insufficient space for records management; misplacement of vital records in the institution; loss of vital records in the institution; inadequate computer terminals; lack of record keeping policy; lack of record retention; lack of disposition schedule in the institution; ineffective means of retrieving record; improper records management in the institution. The institution's management should consider the study's findings and address these challenges for proper records management and its associated benefits.

Digitization and digital preservation are no longer emerging tools; they are now the preferred and accepted practice for saving many analog records. Libraries and archives are in a transitional period and many are moving away from print into a primarily, or, in some cases, entirely, digital format Moghaddam, (2010).

Mojapelo and Ngoepe (2021) affirmed that records, if properly managed, organized, and monitored, ensure effective and efficient updates to organizations. They believed that proper records management is necessary to promote good governance.

Organizations must take steps to guarantee the integrity of personal data, as outlined in the National Privacy Commission's Circular 2023-06. This entails carrying out privacy impact analyses, putting privacy management plans into place, and making sure that personal information is kept safe and only for as long as is required.

The government is actively addressing privacy issues and violations, according to the Digital Security and Privacy Quick Response (DSPQR) project of the National Privacy Commission. The project intends to improve user satisfaction and trust by promptly addressing privacy concerns, increasing awareness, and educating people and organizations about data protection.

Through digital transformation, the Texas Department of Insurance was able to save costs and im prove disaster recovery by digitizing over 800,000 healthcare case files (Image API, 2023).

According to **Islam, Rahman, and Kabir (2022)**, systems for deep learning-based access control, such as DLBAC_alpha, have the potential to improve the automation and flexibility of access choices. Their tests showed that, with sufficient training, deep learning may perform better in dynamic situations than conventional rule-based systems.

Jalsovszky and Feldesman (2023) found that recent advances in Handwritten Text Recognition (HTR) technologies from projects like tranScriptorium and READ have significantly improved the

accessibility of digitized historical documents, even those with poor legibility.

Furthermore, local governments need to put in place thorough data security measures, according to Nguyen et al. (2020). These consist of disaster recovery plans, frequent audits, encryption, and access control systems. Local governments must safeguard data and have explicit policies and procedures for managing and getting rid of sensitive records, according to a significant study on data security in public administration by Schenk & Day (2017).

The National Archives and Records Administration (NARA) outlined in its 2022–2026 Strategic Plan a target of digitizing 500 million pages of records to improve public accessibility and promote digital equity initiatives (National Archives and Records Administration, 2022).

According to a study by Njue, Kyalo, and Muchina (2021), the tendering process was impacted by records management. According to the study, the public sector's tendering process is statistically significantly impacted by records management. When records are mismanaged, more time is spent looking for information, which reduces time spent on productive tasks. Some cases also have financial repercussions because lawsuits cause records to be lost.

According to Nobi, Sakib, and Islam (2022), in order to automate policy creation, identify irregularities, and improve decision-making, machine learning (ML) techniques are being included into access control systems more often. But according to their research, in order for ML-powered access control models to be reliable in delicate settings, they need better interpretability and high-quality datasets.

Research consistently identifies the importance of staff training in maintaining data security. Local government employees must know how to handle records securely, recognize phishing attempts, and follow protocols for dealing with breaches. Studies by Alvarado & Gomez (2021) found that training programs on data security practices are often lacking, resulting in increased vulnerability to security breaches.

The causes are complex and multifaceted, ranging from external attacks to internal leaks, technological loopholes to management flaws, new risks arising from new technologies to new models and repeated occurrences of traditional security problems Lee et al. (2020).

Panpan (2022) examined the security situation of preserving electronic records in central China and found important problems like a lack of knowledge about the characteristics of electronic records, inadequate disaster recovery capabilities, and a lack of awareness of security threats. Regular security risk assessments, the implementation of new technologies, application-level backups, and improved training and hiring of IT personnel are some of the remedies suggested by the study to improve the protection of electronic documents.

Restore (2024) offered a thorough analysis of statutory retention periods under UK law, some HR and personnel records must be kept for predetermined amounts of time as required by laws like the Companies Act, the Limitation Act of 1980, and the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR). The legal requirement to preserve information for prospective civil claims and regulatory compliance is reflected in the wide range of retention periods, which range from as short as two years for working time records to as long as 40 years for medical records pertaining to exposure to dangerous substances.

Saffady (2021) stated that records management is concerned with the systematic analysis and control of recorded information, which includes any information created, received, maintained, or used by an organization in support of its mission, operations, and activities. The proliferation of digital

technologies and the exponential growth of data have amplified the importance of safeguarding data in digital environments Saraswat & Meel (2022).

According to Shen (2023), Misconfigured access controls continue to be a serious weakness in digital systems. In order to avoid unwanted access, his review examines a number of methods for detecting and resolving these problems, including as data mining, formal verification, and test-based approaches.

Shredall (2025) emphasized the essential importance of legal obligations in influencing document retention strategies. Although most company records generally need to be kept for around six years, specific documents—like payroll information and tax records—might have to be stored for as long as ten years to adhere to tax and employment regulations. This guidance highlights the importance of organizations creating retention schedules that meet legal requirements while also effectively managing organizational risks. Diligent coordination of retention policies with legal requirements aids in guaranteeing compliance and reducing possible legal and financial risks.

According to Surfshark's Global Data Breach Statistics, the Philippines ranks fifth in Asia for the number of data breaches since 2004, with 124 million accounts compromised. This equates to an average of 106 breaches per 100 people, indicating that nearly every Filipino has been affected by a data breach at least once.

The city government of San Fernando Pampaga, has implemented a comprehensive data protection measure which in line with the requirements of the Data Privacy Act of 2012. It stated that a Data Protection Officer (DPO) should be appointed to ensure the compliance with data privacy laws and internal policies. Personal information is safely preserved through a combination of digital and physical security measures, such as secured servers and locked filing cabinets, with access granted solely to authorized individuals. Furthermore, the management of data retention is handled with care, ensuring that records are maintained only as long as required and disposed of securely in line with the General Records Disposition Schedule established by the National Archives of the Philippines (NAP). These practices demonstrate the city's dedication to safeguarding the privacy and security of its residents' data.

The Chandigarh administration has initiated a project to digitize property documents in collaboration with the National Informatics Centre, with the goal of enhancing transparency and enabling real-time file monitoring (Times of India, 2025).

Records management entails more than just preventing legal costs and protecting intellectual property, claim Ongwenyi et al. (2020). It also entails preserving business continuity.

Regarding data safety in blockchain systems, immutability is one of the main obstacles. Data stored on the blockchain becomes immutable, and any attempt to alter or delete it invalidates the entire blockchain. This poses challenges when complying with data protection laws, such as the GDPR, which mandates deleting personal data upon request Schellinger et al. (2022).

Torgerson (2024) carried out a systematic mapping review of retention methods utilized in National Institute for Health and Care Research (NIHR) Health Technology Assessment studies. Their research revealed that the frequently mentioned retention strategies encompassed adaptability in data collection methods and sites, participant diaries, utilization of routine data, input from patient and public involvement (PPI), reminders through phone and mail, monitoring techniques, and newsletters for participants. Nonetheless, they observed that most of these strategies had weak evidence for their effectiveness, with the majority backed solely by low or very low-quality evidence. The writers

highlighted the necessity for more thorough Study Within a Trial (SWAT) investigation to enhance the assessment and prioritization of successful retention strategies.

Ukaogba and Nwankwo (2020) argued that effective record management in academic institutions provides well-organized, properly stored, and easily retrieved information. If the academic records are in place, administrative tasks are easier, and records release services are faster and more accurate.

Data masking replaces sensitive information with fictitious or anonymized data, preserving data utility while protecting privacy Uchechukwu et al. (2023). Generalization involves replacing specific values with broader categories or ranges, reducing the granularity of data while maintaining its usefulness for analysis Ukoba and Jen (2023). Suppression removes or suppresses certain attributes or records containing sensitive information from datasets.

Way, R., Gamble, C., Cook, J., and Davidson, P. (2024) examined retention techniques employed in NIHR Health Technology Assessment trials published from 2020 to 2022. They discovered shared methods such as adaptable data gathering, participant journals, reminders, and involvement of patients/public commonly employed, yet the majority lacked strong proof of efficacy. The median dropout rate was 12%, presenting threats to trial validity and expenses. The authors emphasized the necessity for more thorough embedded Studies Within A Trial (SWATs) to enhance the evaluation and prioritization of effective retention techniques. This study is the first to systematically outline retention strategies in NIHR HTA trials and identify evidence gaps.

Digital preservation of government archives enhances accessibility and data security, which facilitates the use of electronic-based solutions. But issues like a lack of administrative support and a lack of technical expertise continue to exist. (Wijaya, B. H., 2023).

By increasing operational effectiveness, transparency, and public participation, digitalization is revolutionizing local governments, according to the ICLEI Digitalization Policy Brief (2023). Similarly, SymQuest (2025) described how municipal governments' document management systems (DMS) provide compliance with legal frameworks like HIPAA and FOIA while streamlining the whole document lifecycle, from collection and storage to retrieval and disposal. These solutions increase productivity and enhance service delivery by automating processes, enhancing interdepartmental communication, and providing secure mobile access

According to the World Economic Forum, more than half (52 percent) of public organizations cite a lack of resources and skills as the greatest challenge in creating effective cyber resilience programs. Much has been reported about the dearth of experienced cyber talent and the skills gap, which creates an attrition rate nearly eight percentage points higher than other roles, making team consistency difficult to maintain.

According to Yang and Zhao (2021), zero-knowledge proofs in conjunction with blockchain-based access control can provide decentralized, privacy-preserving identity and access management solutions for Internet of Things applications. Because their strategy eliminates the need for centralized authority, trust is increased and vulnerabilities are decreased.

Review of Related Studies

As stated in Republic Act No. 94, otherwise known as the National Archives of the Philippines Act of 2007, this act mandates all government offices, include the LGUS to establish records management system, which key provisions to include is to Establishment of Archives and Records

Offices for all government must create a dedicated units for records managements. Inventory disposition which states regular inventory and proper disposal of records are required, adhering to guidelines set by the National Archives of the Philippines (NAP) and lastly the Protection of the Vital and Protected Records needs a special to preserved records that are essential for the continuity of government operations and those that are legally

Republic Act No. 9470, otherwise known as the National Archives of the Philippines Act of 2007, underscores the mandate for various government offices to provide efficient and prompt services related to public records, which are essential to the administration and operation of all government offices, whether national or local, including GOCCs and government financial institutions (GFIs). This includes compliance with the time frame mandated by civil service laws for releasing documents needed by clients.

RA 8973 or the Agricultural and Fisheries Modernization Act of 1997 states that primarily, it focuses on agriculture and fisheries, emphasizing the importance of information dissemination and transparency, which are closely linked to the effective records management and data security.

ISO 15489-1:2001 defines records as information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or the transaction of business. ISO 15489 is divided into concepts, principles, and guidelines. Together, these two parts outline a comprehensive records management program.

The National Cybersecurity Plan (NCSP) 2023-2028, created by the Department of Information and Communications Technology (DICT) under Section 15 of Republic Act No. 10844, demonstrates the Philippines' continued commitment to improving its national cybersecurity posture. The NCSP's second iteration was developed through broad consultations with public and private sector partners, building on the framework of the first plan. To maintain consistency and synergy in the nation's cybersecurity approach, the plan is closely integrated with the Philippine Development Plan 2023–2028, the National Security Strategy, the National Cybercrime Strategy, and other pertinent government plans. A safe and resilient digital environment for all Filipinos is the goal of the NCSP, which will be achieved by strengthening national capabilities and encouraging cooperation.

The Department of the Interior and Local Government (DILG) issued Memorandum Circular No. 2024-135, which is a recent development in the Philippines' local data privacy regulatory environment. DILG Memorandum Circular No. 2018-036 has undergone a substantial change with this publication. It seeks to increase Local Government Units' (LGUs') adherence to the Data Privacy Act of 2012 (Republic Act No. 10173).

The National Privacy Commission (NPC) Circular No. 2022-04, which provides updated rules and procedures for data protection practices, was followed by the issuance of DILG M.C. No. 2024-135. It requires all local government units (LGUs) to select Data Protection Officers (DPOs) at the provincial, city, and municipal levels and to register their data processing systems (DPS) through the NPC Registration System if they process sensitive or personal data, especially when automated decision-making or profiling is involved.

Training on Data Privacy and Security Awareness has been provided by the Philippine Statistics Authority (PSA) to Data Protection Officers (DPOs) in local government units. In order to improve LGU DPOs' ability to protect personal information and guarantee data privacy within their domains, the training placed a strong emphasis on adherence to the Data Privacy Act of 2012.

According to Abdulkadhim et al. (2015), information technology (IT) infrastructure is essential to digitizing records and archives since it facilitates efficient task, job, and responsibility performance.

Anderson and Kim (2021) highlight businesses who have successfully integrated compliance and data governance frameworks into their big data projects. In order to promote a culture of data security and regulatory compliance, the article emphasizes the importance of rules, procedures, and auditing methods.

According to Aquino and Reyes (2023), the majority of LGUs in the Philippines continue to store their records physically, which presents serious security problems. To improve data security and guarantee adherence to retention guidelines, they suggested switching to digital records management systems with encryption and multi-factor authentication.

According to Cruz and Reyes (2022), the impact of cyber incidents on public trust in government digital services is explored, emphasizing the urgency of implementing robust security measures, an issue directly addressed in the NCSP through its focus on securing critical information infrastructure.

Brown and Johnson (2021) highlight organizations' challenges in implementing granular access controls within big data frameworks. Their study argues the need to develop sophisticated access management strategies that align with the unique demands of large-scale data processing.

Big Data is the key property of massive data, reflected in its volume. The huge number of large data leads to data heterogeneity and a broad variety of dimensionalities in datasets. Efforts are, therefore, needed to decrease the amount to analyze large figures effectively Che et al. (2020).

According to Brunskill, Mellon, and Demb (2012), their study is doubtless to prove to be a useful guide for those responsible for records management in the museum and gallery sector. Systematic records management is an important activity for ‘information businesses’ such as museums and galleries, but is not always recognized as a core function. Record-keeping activities are often concentrated on small groups of records, and staff charged with managing them may have limited experience in the field.

According to Codilla et al. (2024), digitization at the barangay level in Quezon City enhanced retrieval time and improved the reliability of local governance documents, making operations more efficient and transparent.

De Guzman (2020) found that many government agencies continue to struggle with out-of-date retention schedules in public sector organizations. The report also emphasized the dangers of storing records physically, including the possibility of theft and natural calamities. In order to guarantee adherence to retention requirements, the study suggested updating storage procedures.

Garcia and Ramos's (2022) study, which looked at retention schedules in the context of Philippine LGUs, discovered that retention periods were not always followed. Because of this discrepancy, records frequently outlived their retention spans as a result of poor storage options. The authors also underlined how crucial it is to match national regulatory frameworks like the Data Privacy Act with local government records management procedures.

According to Garcia and Tan (2023), their study on document retention policies emphasized their crucial role in ensuring data security and privacy. They reviewed instances where poor retention practices resulted in security breaches, particularly in digital environments. They recommended that document retention schedules align with legal frameworks such as the Data Privacy Act of 2012 to protect sensitive data better.

Research investigating the 23andMe data leak claimed that credential stuffing assaults exposed the private and genetic information of roughly 5.5 million people by taking advantage of re-used usernames and passwords. The study highlights the significance of more robust user authentication procedures and corporate accountability for protecting sensitive information (Gracy, 2025).

A study examining the 23 and ME data leak claimed that credential stuffing attacks exposed the private and genetic information of roughly 5.5 million people by taking advantage of reused user names and passwords. The report emphasizes how important it is to have more robust user authentication procedures and corporate accountability for protecting sensitive data. (Holthouse et.al., 2025)

Horizon 2020 mandated research data publication, describing such data as information, in particular facts or numbers, collected to be examined and considered and as a basis for reasoning, discussion, or calculation. Practical manuals for researchers also provide definitions, for example Managing and Sharing Research Data: Best Practice for Researchers states: We define research data as any research materials resulting from primary data collection or generation, qualitative or quantitative, or derived from existing sources intended to be analyzed in the course of a research project. Research data can therefore be considered as including information or data that may be the input or the product of research.

According to Jain (2025), integrating provenance tracking within Semantic Web frameworks can significantly enhance data integrity. By employing the PROV Data Model and its Semantic Web variant, PROV-O, the study demonstrates how systematic recording and management of provenance information across multiple data processing domains can improve data reliability, traceability, and facilitate seamless integration across heterogeneous systems.

A Michigan State University study found that over the past 15 years, ransomware attacks have compromised 285 million patient records, making them the main cause of healthcare data breaches in t he United States.The study emphasizes how ransomware significantly affects patient data security and healthcare operations. (Jiang et al., 2025)

Khin et al. (2021) also found that data integrity remains a pivotal concern in clinical research. Their paper discusses the perspectives of the US FDA and the UK's MHRA on good clinical practice, emphasizing the importance of accurate data collection, management, and reporting. The study underscores the need for robust regulatory frameworks to ensure the credibility and reliability of clinical trial data.

According to Pangcatan and Prado (2020), digitization is increasingly seen as a solution for improving the preservation and retrieval of documents in higher education and government settings. Their study at Mindanao State University revealed that digitizing records reduced physical storage constraints and improved efficiency, although implementation was limited by budget and staff training.

Patel et al. (2020) examined the particular dangers that big data ecosystems confront, such as malicious assaults, identity theft, and data breaches. The difficulties described in this research highlight the necessity of a proactive strategy for big data-based threat identification and mitigation.

According to Reyes and Ramos (2024), they examined the difficulties in keeping and conserving digital government documents. They emphasized the particular difficulties government organizations have in making sure digital documents are kept for the legally mandated durations when they transition to digital technologies for service delivery. They suggested integrating digital archiving solutions into government processes and establishing explicit digital retention timelines.

Rodriguez et al. (2024) stated that the eDALAYON system was developed and put into use with

the intention of resolving ongoing issues with document management in the Philippine government sector. The system's four main modules—user access roles, document management, document tracking, and reporting—were created using the Agile Scrum approach. Using a standardized evaluation tool, staff members from the Department of the Interior and Local Government (DILG) in Negros Occidental first implemented and evaluated the system. The outcomes demonstrated the system's efficacy in improving operational efficiency by showing a notable decrease in the organization's workload and document retrieval time. While the integrated access control module guarantees strong document security and compliance, the system's cloud-based storage and version control features have significantly enhanced collaboration. In addition to addressing the drawbacks of conventional document management, this digital solution supports the larger government objective of digital transformation.

Research on the digital transformation of the Science City of Muñoz brought to light concerns with user acceptance, cybersecurity, skill gaps, and budgetary limits. Among the best practices found include infrastructure investment, stakeholder engagement, partnerships, skill development, and change management. Enhancement of the internet infrastructure, thorough training in digital skills, cybersecurity reinforcement, teamwork, cloud storage solutions, e-government portal improvement, and age-appropriate staff training are among the recommendations (Romeiro, 2023).

According to a 2020 study by Macapinlac and Buenaventura on the retention and disposal of public records in local government agencies, many LGUs did not fully comply with the required retention periods specified in the Freedom of Information Act and other local regulations. To improve comprehension and compliance with records preservation regulations, they recommended bolstering training initiatives for public sector workers.

Santos and Medina (2021) found that although some local government units were moving to digital systems, many still used manual methods in their study on digital records management in LGUs in the Philippines. It was difficult to maintain legal compliance and appropriate record preservation because of this lack of modernization. In order to enhance record retention procedures, they emphasized the necessity of precise retention schedules and the incorporation of electronic technologies.

Thompson and Mitchell (2024) stated that the shift to digital record-keeping has made data retention and destruction policies more complex. Their study discussed how digital records can be stored indefinitely unless retention and deletion policies are established. They recommended adopting advanced document management systems that automatically enforce retention and destruction protocols to meet legal and regulatory requirements.

Ukaogba & Nwankwo (2020) asserted that effective record management makes administrative tasks easy. The benefit of school records is derived when information is properly managed through record management practices.

Ralph Merkle patented the idea of the Merkle tree in 1979 and changed its name from Binary hash tree to Merkle tree in 1987. The paper discusses how to create a new digital signature that is as safe as the underlying encryption mechanism while avoiding the high computing expenses of modular arithmetic and using a regular encryption method like DES (Data Encryption Standard).

Velasco (2022) showed that ineffective document retention procedures had a direct effect on public administration firms' productivity. Delays and a lack of transparency resulted from ineffective record-keeping and disregard for retention guidelines. To improve the general effectiveness of government agencies, they suggested implementing simplified procedures for document storage and retention.

According to VillegasCh and García-Ortiz (2023), in order to reduce risks and guarantee regulatory compliance, it is becoming increasingly necessary for organizations to implement strong data privacy and security measures, such as encryption, access controls, data anonymization, and threat intelligence.

Verizon's 2025 Data Breach Investigations Report (DBIR) found that 86% of data breaches include stolen or compromised credentials, making credential theft one of the top causes of data breaches. In order to reduce these risks, the study stresses the significance of putting strong access controls and personnel training into place.

According to Zamora (2021), looked at the legal frameworks for record keeping in Philippine government entities as well as those across the globe. The study covered the methods used by regional organizations, including the Philippine National Archives, to set rules for the preservation of public records. The report underlined that in order to preserve accountability and openness, compliance with legislation like the Freedom of Information Act and the Government Procurement Reform Act is crucial.

RESEARCH METHODOLOGY

This chapter contains the research design, subject of the study, population, sampling techniques, data gathering procedure, research instrument and statistical treatment.

Research Design

The research design used in this study was descriptive research. According to Calderon and Gonzales (2007), descriptive research is concerned with conditions of relationships that exist, practices that prevail, beliefs, processes that are going on, effects that are being felt, or trends that are developing. The process of descriptive research goes beyond mere gathering and tabulation of data.

Respondents of the Study

The study's respondents were two hundred (200) staff members from two (2) Municipalities within the Local Government Units of the Province of Laguna.

Sampling Technique

The sampling technique used in this study was purposive sampling, which involved selected municipalities from two (2) within Local Government Units of the Province of Laguna. The researcher aimed to identify participants directly involved in the management of records or data security, such as records manager, staff and department heads.

Purposive sampling refers to a group of non-probability sampling techniques in which units are selected because they have characteristics you need in your sample. In other words, units are selected “on purpose” in purposive sampling.

Research Procedure

Identifying the issue was the first step in conducting the study, followed by the formulation of the primary questions that addressed the effectiveness of records management systems in the LGU, the implementation of data security measures to protect sensitive records, and the challenges faced by different departments in maintaining these systems. The objective was to describe the current practices in records management, assess data security protocols, identify existing challenges, and propose

actionable recommendations for improvement.

Research Instruments

The questionnaire was used as the main data-gathering instrument. The instrument was designed to answer the statement of the problem. The questionnaire consisted of sixty (60) questions, which were distributed to the respondents.

The data-gathering instrument was structured on a scale of 1-5, where (5) represents strongly agree, 4 represents agree, 3 represents neutral, 2, represents disagree and 1 represents strongly disagree. This scale helped the researcher analyze the results of data gathering.

Statistical Treatment of Data

The researcher incorporated inferential statistics. Using this method, the researcher analyzed data from the sample population and drew conclusions or made inferences about the larger population. Statistical measures such as regression analysis, ANOVA, correlation, t-tests, and confidence intervals were applied, based on the queries and data properties.

PRESENTATION, INTERPRETATION AND ANALYSIS OF DATA

This chapter presents and analyzes the results obtained from the data gathered in this study. The following tables and discussions illustrate and interpret the findings of the research problem. Each result is examined in detail to identify patterns, relationships, and significant insights that contributed to addressing the study's objectives. Furthermore, the interpretation provided offered a deeper understanding of the implications of the data, ensuring a comprehensive discussion of the study's key findings and discussions that characterized the problem presented in the study.

Records Management

In this study, the level of records management and data security in the local government units refers to the Digitization of records, Access Control, Data Storage and lock ups and data security.

The information in Table 1 illustrates the degree of records management about digitalization in the Local Government Unit (LGU).

The comments generally show that the digitalization activities are viewed favorably. With a mean score of 4.55 and a standard deviation of 0.53 for the highest-rated statement, respondents firmly believe that the LGU has successfully digitized the majority of its significant records. This is a noteworthy finding, indicating that digitalization is widely and successfully covered, and respondents strongly agree about this accomplishment.

Table 1. Level of Records Management with regard to the digitization of records

Statement	Mean	Std. deviation	Verbal Interpretation
1. The LGU has successfully digitized	4.5500	.52810	

the majority of its important records.			Strongly Agree
2. Digitization records are easily accessible when needed.	4.4500	.57371	Strongly Agree
3. The Digitization process is well-organized and efficient	4.3200	.73505	Agree
4. The quality of digitized records is sufficient for long-term storage and retrieval	4.1400 4.1650	.65770	Agree
5. The transition from paper-based records to digital has improved overall efficiency.		.52837	Agree
Digitization of Records	4.3250	.31603	Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Furthermore, with a mean score of 4.45, the statement "The transition from paper-based records to digital has improved overall efficiency" was rated well, suggesting that respondents see real advantages in the move to digital formats. The quality of digital files for long-term storage, the management of the digitization process, and the accessibility of digitized documents were among the other factors that got mean scores ranging from 4.14 to 4.32. All of these are evaluated as "Agree," suggesting a generally positive viewpoint with a little more variance than the top-rated items.

With an overall mean score of 4.325 and a comparatively low standard deviation of 0.316 for record digitization, respondents' generally optimistic view is further supported. Although the results demonstrate a high level of support for the digitization effort, they also point to areas that may need further development, especially in terms of improving the organization's long-term digital record quality.

As cited in the study of Romeiro (2023), research on the digital transformation of the Science City of Muñoz brought to light concerns with user acceptance, cybersecurity, skill gaps, and budgetary limits. Among the best practices found include infrastructure investment, stakeholder engagement, partnerships, skill development, and change management. Enhancement of the internet infrastructure, thorough training in digital skills, cybersecurity reinforcement, teamwork, cloud storage solutions, e-government portal improvement, and age-appropriate staff training are among the recommendations.

By increasing operational effectiveness, transparency, and public participation, digitalization is revolutionizing local governments (ICLEI Digitalization Policy Brief, 2023). Similarly, SymQuest (2025) described how municipal governments' document management systems (DMS) provide compliance with legal frameworks like HIPAA and FOIA while streamlining the whole document lifecycle, from collection and storage to retrieval and disposal. These solutions increase productivity and enhance service delivery by automating processes, enhancing interdepartmental communication, and providing secure mobile access.

Table 2. Level of Records Management with regard to access control.

Statement	Mean	Std. deviation	Verbal Interpretation
1. *Only authorized personnel have access to sensitive records in the office.*	4.5200	.60947	Strongly Agree
2. The office uses robust authentication methods (e.g., passwords, biometrics) for access control	4.5200	.54873	StronglyAgree
3. Access control policies are regularly updated and communicated to employees.	4.2450	.65354	Agree
4. Records access is logged, and audit trails are maintained for accountability.	4.3350	.70374	Agree
5. The LGU enforces strict user permissions to ensure proper access control.	4.2550	.64968	Agree
ACCESS CONTROL	4.3750	.38512	Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagre; 1.00 – 1.79 - Strongly Disagree*

The data in Table 2 reflect respondents' perceptions of the level of records management regarding access control within the Local Government Unit (LGU). The results indicate an overall positive assessment, with particular strengths in restricting access to sensitive information. The highest-rated statements are: "Only authorized personnel have access to sensitive records in the office" and "The office uses robust authentication methods (e.g., passwords, biometrics) for access control", both receiving a mean score of 4.52 and verbal interpretation of "Strongly Agree." These findings show that respondents strongly agreed that the LGU has put in place efficient authentication procedures and access controls to safeguard private information.

Additional facets of access control, include audit trails, policy modifications, and he mean ratings for user permissions were somewhat lower, ranging from 4.245 to All of them fall under the "Agree" category (4.335). This implies that even though these. Although there are procedures in place and they are usually successful, there is less regularity or greater assurance in their execution than the best-rated items. Access control has an overall mean score of 4.375, with a standard variation of 0.38512, suggesting a strong and reliable correlation between responders. In conclusion, the LGU has a solid basis in access control, particularly when it comes to implementing secure authentication and protecting private information. Nonetheless, there is potential to improve communication, policy updates, and monitoring systems to improve responsibility and guarantee ongoing conformity.

To support the findings of strong access control practices, Adusei and Mensah Senyah (2022) examined staff knowledge on records management in Ghanaian local governments and found that awareness of policies and procedures, including data privacy and security, was high among staff. Their study emphasized the importance of management support, resource allocation, and staff training to

enhance records management effectiveness, including safeguarding sensitive information through proper access controls1. This aligns with the LGU respondents' strong agreement on robust authentication methods and restricted access to sensitive records.

Table 3. Level of Records Management with regard to data storage and lock-ups

Statement	Mean	Std. deviation	Verbal Interpretation
1. The LGU data storage system is secure and well-maintained.	4.4450	.63955	Agree
2. Records are stored in secure locations, both physically and digitally.	4.4650	.57483	Agree
3. The LGU employs encryption methods to secure the storage of sensitive records.	4.2700	.65517	Agree
4. Backup systems are regularly tested to ensure data recovery in case of failure.	4.3950	.67174	Agree
5. Data storage systems are regularly updated to address emerging security vulnerabilities.	4.1450	.59645	Agree
Data storage and Lock ups	4.3440	.39553	Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Table 3 shows the evaluation of the Local Government Unit's (LGU) level of records management with regard to data storage and lockups.

With a verbal interpretation of "Agree" for every phrase, the replies show a largely positive perception. With a mean score of 4.4650 and a comparatively low standard deviation of 0.57483, the item with the highest rating—"Records are stored in secure locations, both physically and digitally"—indicates that respondents regularly acknowledge the existence of secure storage techniques.

The statement "The LGU data storage system is secure and well-maintained" comes next, with a mean score of 4.4450, indicating a high level of agreement that the systems in place are trustworthy and protected. Additionally, respondents agreed that encryption techniques are used (mean: 4.2700) and backup systems are routinely tested (mean: 4.3950), two crucial procedures in guaranteeing data confidentiality and integrity.

The statement that received the lowest rating in this area, "Data storage systems are regularly updated to address emerging security vulnerabilities," although it is still read as "Agree," with a mean score of 4.1450. This implies that even while upgrades are being made, the LGU's proactive approach to addressing changing security threats may not be as consistent or confident.

With an overall mean score of 4.3440 and a standard deviation of 0.39553 for data storage and lockups, respondents showed a strong and generally stable degree of agreement. The results demonstrate

that the LGU has put in place reliable systems for data storage and security. To stay on top of new security threats, there is space for improvement, especially in terms of increasing the frequency and visibility of system upgrades.

As cited by the DILG's deployment of the eDALAYON system, which emphasized cloud-based storage, secure access management, and document protection features that improve security and cooperation, lends support to this (as quoted in Philippine Journal of Science, Engineering and Technology, 2022).

A systematic review by Alharkan et al. (2024) highlighted the cybersecurity challenges faced by local governments, emphasizing the need for secure data infrastructure that includes physical and digital safeguards, encryption, and regular system maintenance to protect sensitive information from evolving threats12. This aligns with respondents' recognition of secure storage locations and encryption use within the LGU.

Table 4. Level of Records Management with regard to training and awareness

Statement	Mean	Std. deviation	Verbal Interpretation
1.Employees receive regular training on records management practices.	4.4450	.63955	Strongly Agree
2.Training programs on records management are comprehensive and up-to-date.	4.4650	.57483	Strongly Agree
3. The LGU ensures employees understand the importance of proper records management.	4.2700	.65517	Strongly Agree
4. Awareness campaigns are regularly held to highlight the importance of data privacy and security.	4.1600	.74645	Agree
5. Employees feel confident in managing and handling office records properly.tr	4.2400	.63594	Strongly Agree
Training and Awareness	4.3480	.42355	Strongly Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

The evaluation of the level of records management awareness and training within the Local Government Unit (LGU) is shown in Table 4. A high degree of satisfaction and agreement among respondents on the LGU's efforts to train staff and create awareness on records management is shown by the overall mean score of 4.3480, which falls within the "Strongly Agree" category.

With a mean rating of 4.4650, the item with the highest rating is "Training programs on records management are comprehensive and up-to-date." "Employees receive regular training on records management practices" (mean: 4.4450) is also highly valued. These results demonstrate a strong organizational commitment to provide employees with up-to-date, pertinent records handling expertise. Similarly, the statements "Employees feel confident in managing and handling office records properly" (mean: 4.2400) and "The LGU ensures employees understand the importance of proper records management" (mean: 4.2700) both received "Strongly Agree" ratings, indicating that training programs are not only frequent but also successful in fostering competence and confidence among staff members.

Only the statement "Awareness campaigns are regularly held to highlight the importance of data privacy and security" had a little lower but still favorable rating; it fell into the "Agree" category with a mean score of 4.1600. This suggests that, in contrast to other training initiatives, there can be less uniformity or exposure during campaigns. In conclusion, the LGU has done a great job of raising awareness and offering training about records management. Even if the fundamental training elements are strong and well-liked, there is room to improve the frequency and effect of data privacy and security awareness campaigns in order to create a framework for training and awareness that is even more thorough.

To support this viewpoint, CM-Alliance (2025) examined how self-storage facilities have changed over time, pointing out that many now incorporate cutting-edge digital security features. To safeguard both digital and physical assets, they include smart access codes, biometric and face recognition access, and round-the-clock surveillance. The research also highlights the increasing popularity of climate-controlled units and cloud-based access, which enables users to safely and remotely manage and recover data. The growing need for hybrid storage options that offer strong physical protection together with the ease of digital access is reflected in this change.

The 2024 study looked into how records management affected the performance of HRM in the public sector found that strong records management procedures, which greatly improved a number of HRM outcomes. Higher employee motivation, transparent hiring, effective dispute resolution, and well-informed decision-making are all facilitated by established electronic records systems, consistent filing, and efficient monitoring, according to the study. Good records management makes it easier to monitor staff performance and training requirements, promotes retention by maintaining institutional knowledge, and makes it possible to conduct fair hiring procedures by keeping thorough applicant records. Employee utilization and retention issues still exist, nevertheless, underscoring the necessity of more funding for records administration capabilities and connection with HRM procedures.

Table 5 compares the frequency of data breaches inside the Local Government Unit (LGU) to assess the degree of data security. The "Agree" category is represented by the overall mean score of 3.8560 with a standard deviation of 0.45596, indicating that respondents generally think the LGU is managing and responding to data breaches appropriately, even though there is still room for improvement.

Significantly, the statement "The frequency of data breaches within the office has decreased over time" scored 4.0300 on average, suggesting that respondents are aware of the effort made in reducing these occurrences. Similarly, claims like "Employees are trained to recognize and report potential data security incidents" (mean: 3.9400) and "The LGU has effective measures in place to prevent data

breaches" (mean: 3.9200) imply that awareness campaigns and preventative measures are being actively carried out.

Table 5. Level of Data Security in terms of the incidence of data breaching

Statement	Mean	Std. deviation	Verbal Interpretation
1. The LGU has experienced a data breach in the past year.	3.7750	.63955	Agree
2. The frequency of data breaches within the office has decreased over time.	4.0300	.57483	Agree
3.The LGU has effective measures in place to prevent data breaches.	3.9200	.65517	Agree
4. Employees are trained to recognize and report potential data security incidents.	3.9400	.66226	Agree
5. The LGU responds promptly and effectively when a data breach occurs.	3.6150	.65492	Agree
Incidence of Data Breaching	3.8560	.45596	Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 – Neutral; 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

But with a lower mean score of 3.6150, the item "The LGU responds promptly and effectively when a data breach occurs" indicated a possible gap in response effectiveness. Furthermore, the assertion that “The LGU has experienced a data breach in the past year” (mean: 3.7750) suggests that although breaches have happened, people believe they are being handled rather effectively. In conclusion, efforts at preventive and staff training are recognized, and the LGU is seen as proactive in minimizing and managing data breaches. Stakeholder confidence could be raised and overall data security strengthened by improving the promptness and efficacy of breach responses.

A systematic review on cybersecurity in local governments highlights that while most cyber incidents tend to be minor, the frequency of breaches remains a significant concern, requiring ongoing prevention and response efforts1. The 2025 Data Breach Investigations Report by Verizon underscores that public sector organizations face increasingly sophisticated attacks, emphasizing the critical need for effective incident response planning and employee training to reduce breach frequency and impact.

According to Cobalt's 2025 cybersecurity statistics, 70% of breaches resulted in major operational disruptions, and cyberattacks rose by 30% in the second quarter of 2024 over the same period the year before. Due to increased attack surfaces and changing workplace hazards, remote work

has increased breach costs by an average of $173,000 per occurrence. Additionally, as businesses look to reduce the growing financial risks associated with cyber disasters, cyber insurance rates are rapidly increasing and are expected to double by 2027.

Table 6 shows the Local Government Unit's (LGU) evaluation of the degree of data security with regard to data integrity. With a mean score of 4.3130 overall and a standard deviation of 0.39217, the respondents' agreement that the LGU successfully preserves the integrity of its data is strong, falling inside the "Strongly Agree" range.

Table 6. Level of Data Security in terms of data integrity

Statement	**Mean**	**Std. deviation**	**Verbal Interpretation**
1. The LGU regularly checks data for consistency and accuracy.	4.3650	.65874	Strongly Agree
2. There are measures to prevent unauthorized alterations to office data.	4.0100	.60309	Agree
3.Data integrity is maintained throughout the entire data lifecycle.	4.3750	.63750	Strongly Agree
4. The LGU uses automated tools to ensure the integrity of its data.	4.2350	.64174	Strongly Agree
5. The quality of office data is continuously monitored and improved.	4.1800	.63214	Agree
Data Integrity	4.3130	.39217	Strongly Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Table 6 shows the Local Government Unit's (LGU) evaluation of the degree of data security with regard to data integrity. With a mean score of 4.3130 overall and a standard deviation of 0.39217, the respondents' agreement that the LGU successfully preserves the integrity of its data is strong, falling inside the "Strongly Agree" range.

With a mean score of 4.3750, the item with the highest rating is "Data integrity is maintained throughout the entire data lifecycle." It is closely followed by "The LGU uses automated tools to ensure the integrity of its data" (mean: 4.2350) and "The LGU regularly checks data for consistency and accuracy" (mean: 4.3650). According to these answers, the LGU not only places a high priority on making sure data is correct and consistent, but it also leverages technology to help with these initiatives, boosting confidence in the dependability of the system.

However, the statements "The quality of office data is continuously monitored and improved" (mean: 4.1800) and "There are measures to prevent unauthorized alterations to office data" (mean:

4.0100) scored marginally lower. They still fit into the "Agree" category, though. This suggests that although most of the procedures for protecting and improving data are in place, there might be space to increase continuous improvement initiatives and fortify safeguards against unwanted modifications.

The LGU maintains data integrity with vigor and initiative. In order to maintain these standards, respondents acknowledge that the company uses technology and adheres to best practices for data protection and accuracy. Reinforcing preventive controls and ongoing data quality improvement across all departments could be the focus of future improvements.

Table 7 presents the assessment of the Local Government Unit's (LGU) compliance with data security regulations. "Strongly Agree" is the category that the overall mean score of 4.2900 with a standard deviation of 0.37764 falls within. This suggests that respondents have a high degree of confidence in the LGU's ability to vigorously enforce legal and regulatory privacy and data protection norms.

With an average score of 4.4400, the item with the highest rating is "Regular internal audits assess compliance with data security regulations." It is closely followed by "The LGU is fully compliant with data protection and privacy regulations" (mean: 4.2850) and "Employees are regularly trained on relevant data security and privacy regulations" (mean: 4.3450). These ratings demonstrate the LGU's dedication to upholding compliance as well as its provision of ongoing internal monitoring and personnel training to help achieve that objective.

Table 7. Level of Data Security in terms of compliance with regulations

Statement	**Mean**	**Std. deviation**	**Verbal Interpretation**
1.The LGU is fully compliant with data protection and privacy regulations.	**4.2850**	.58779	Strongly Agree
2. Regular internal audits assess compliance with data security regulations.	4.4400	.55492	Strongly Agree
3. Employees are regularly trained on relevant data security and privacy regulations.	4.3450	.70602	Strongly Agree
4. The LGU promptly addresses any issues related to non-compliance with regulations.	4.2150	.66406	Strongly Agree
5. The office keeps up-to-date with changes in data protection and privacy laws.	4.1650	.64018	Agree
Compliance with Regulations	4.2900	.37764	Strongly Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Furthermore, with a mean score of 4.2150, the statement "The LGU promptly addresses any issues related to non-compliance with regulations" confirmed that the business takes corrective action seriously. Though it was still in the "Agree" range, the statement "The office keeps up to date with changes in data protection and privacy laws" scored the lowest score of all the items, at 4.1650. This implies that even if compliance is high, there can be space for improvement in terms of monitoring and adjusting to changing regulatory requirements.

In conclusion, the LGU has a solid dedication to adhering to data security legislative frameworks. The company is acknowledged for its efforts in personnel training, internal audits, and taking prompt action when non-compliance occurs. Its compliance stance may be further improved by fortifying systems for staying up to date with modifications to data regulations.

Table 8. Level of Data Security in terms of user satisfaction

Statement	**Mean**	**Std. deviation**	**Verbal Interpretation**
1. Users are satisfied with the office's data security measures.	4.2000	.72984	Strongly Agree
2.Users feel confident that their personal and organizational data is secure.	4.3850	.61536	Strongly Agree
3. The LGU provides clear communication regarding data security policies	4.1150	.715140	Agree
4. Users believe the offices' data security measures are effective in preventing breaching	3.9650	.76597	Agree
5. Users feel supported and have access to resources if they have concerns regarding data security.	3.9200	.68991	Agree
USER SATISFACTION	4.1170	.48215	Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Table 8 shows how satisfied users are with the data security procedures implemented by the Local Government Unit (LGU). The "Agree" category is represented by the overall mean score of 4.1170 with a standard deviation of 0.48215. This suggests that, despite some variation in satisfaction across certain regions, consumers have a good opinion of the LGU's data security procedures. "Users are satisfied with the office's data security measures" and "Users feel confident that their personal and organizational data is secure" were the two statements with the highest mean scores, both of which fell into the "Strongly Agree" category (4.3850 and 4.2000, respectively). These answers imply a high level of confidence in the general safety of the LGU's data processing procedures.

Within the "Agree" range, the scores for the other statements were marginally lower. These include "Users feel supported and have access to resources if they have concerns regarding data security" (mean: 3.9200), "The LGU provides clear communication regarding data security policies" (mean: 4.1150), and "Users believe the office's data security measures are effective in preventing breaches" (mean: 3.9650). These findings suggest that although users are usually happy, user assistance, communication, and breach prevention could all need some work.

In summary, the LGU has effectively generated user confidence in its data security policies, notably on overall satisfaction and data protection. To further boost user satisfaction, the LGU may consider enhancing communication tactics and ensuring that customers feel constantly supported in areas relating to data security.

Table 9 assesses the Local Government Unit's (LGU) document retention policies using predetermined retention schedules. The respondents' high level of trust in the LGU's retention schedule management strategy is indicated by the overall mean score of 4.3360, which falls inside the "Strongly Agree" category with a standard deviation of 0.34714.

Table 9. Level of document retention in terms of retention schedules

Statement	Mean	Std. deviation	Verbal Interpretation
1. The office has a clear and defined retention schedule for all types of records.	4.5350	.54797	Strongly Agree
2. Retention schedules are regularly reviewed and updated to reflect business or legal requirements changes.	4.3000	.61536	Strongly Agree
3. Employees are trained to understand and implement the retention schedules for different types of records.	4.3400	.59681	Strongly Agree
4. The LGU has a system to track and manage records according to their retention schedule.	4.2550	.61797	Strongly Agree
5. Retention schedules are easily accessible to relevant staff members in the office.	4.2500	.68991	Strongly Agree
Retention Schedules	4.3360	.34714	Strongly Agree

Legend: *4.20 – 5.00 - Strongly Agree; 3.40 – 4.19 - Agree; 2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

With a mean score of 4.5350, the highest-rated item, "The office has a clear and defined retention schedule for all types of records," indicates great agreement that the LGU has a thorough and organized method for determining how long information should be maintained. Other highly rated items include "Retention schedules are regularly reviewed and updated" (mean: 4.3000) and "Employees are trained to understand and implement the retention schedules" (mean: 4.3400), which imply that staff members are knowledgeable and that the system is kept up to date with evolving organizational or legal requirements.

Similarly, the items "Retention schedules are easily accessible to relevant staff members" (mean: 4.2500) and "The LGU has a system to track and manage records according to their retention schedule" (mean: 4.2550) both obtained somewhat lower but still high ratings. These answers attest to the existence of appropriate procedures and accessibility to facilitate uniform implementation throughout the office.

In conclusion, the results show that the LGU has a strong and successful policy for document retention. The respondents overwhelmingly concur that retention schedules are clearly laid out, updated often, and successfully conveyed and carried out inside the company.

As cited in the study of Torgerson (2024), a systematic mapping review of retention methods utilized in National Institute for Health and Care Research (NIHR) Health Technology Assessment studies. Their research revealed that the frequently mentioned retention strategies encompassed adaptability in data collection methods and sites, participant diaries, utilization of routine data, input from patient and public involvement (PPI), reminders through phone and mail, monitoring techniques, and newsletters for participants. Nonetheless, they observed that most of these strategies had weak evidence for their effectiveness, with the majority backed solely by low or very low-quality evidence. The writers highlighted the necessity for more thorough Study Within a Trial (SWAT) investigation to enhance the assessment and prioritization of successful retention strategies.

Way, R., Gamble, C., Cook, J., and Davidson, P. (2024) examined retention techniques employed in NIHR Health Technology Assessment trials published from 2020 to 2022. They discovered shared methods such as adaptable data gathering, participant journals, reminders, and involvement of patients/public commonly employed, yet the majority lacked strong proof of efficacy. The median dropout rate was 12%, presenting threats to trial validity and expenses. The authors emphasized the necessity for more thorough embedded Studies Within a Trial (SWATs) to enhance the evaluation and prioritization of effective retention techniques. This study is the first to systematically outline retention strategies in NIHR HTA trials and identify evidence gaps.

Table 10. Level of document retention in terms of retention periods

Statement	Mean	Std. deviation	Verbal Interpretation
1. The LGU clearly defines and communicates retention periods for all records.	4.2650	.63782	Strongly Agree
2. Records retention periods align with the industry's best practices and organizational needs.	4.4700	.56631	Strongly Agree

3. Retention periods are consistently adhered to across all departments in the LGU.	4.2800	.72403	Strongly Agree
4. The LGU adjusts retention periods to comply with legal and regulatory requirements.	4.0850	.65969	Strongly Agree
5. The LGU has a process to dispose of records once their retention period has expired.	4.0850	.67084	Strongly Agree
RETENTION PERIODS	4.2370	.40997	Strongly Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Table 10 assesses the document retention periods used by the Local Government Unit (LGU). The "Strongly Agree" category is occupied by the total mean score of 4.2370 with a standard deviation of 0.40997, which shows that respondents had a favorable opinion of the LGU's strategy for establishing and enforcing retention periods.

The statement with the highest mean grade (4.4700) was "The LGU has a process to dispose of records once their retention period has expired," indicating that the LGU successfully completes the end-of-life stage of document management.

Retention policies are clear, relevant, and aligned, as evidenced by statements like "The LGU clearly defines and communicates retention periods for all records" (mean: 4.2650) and "Retention periods align with the industry's best practices and organizational needs" (mean: 4.2800).

The statements "Retention periods are consistently adhered to across all departments" and "The LGU adjusts retention periods to comply with legal and regulatory requirements" both received 4.0850, which is still within the "Strongly Agree" category, albeit being somewhat lower. These show that although there may be some variations in actual execution, the organization-wide standard is nonetheless high and compatible.

The LGU's mechanism for controlling document retention periods is strong and efficient. The high results for every item indicate that policies are clear, compliant with the law, regularly implemented, and backed by organized disposal procedures, all of which promote good records management and organizational responsibility.

Atkinson and Cousineau (2021) showcased two case studies illustrating exceptionally long-term retention over decades. In the first instance, Atkinson reconsolidated word sequences 67 years after first acquiring them, demonstrating improved relearning for words in their original arrangement despite a lack of conscious recollection. In the second instance, Cousineau preserved a significant portion of his enhanced visual search ability after 22 years, reacquiring it more swiftly than with unfamiliar stimuli. These examples underscore that period of retention can differ significantly and that knowledge and skills acquired in the past may still be retained and relearned more effectively than new information, stressing the intricacy of long-term cognitive and behavioral retention.

The Local Government Unit's (LGU) compliance with legal and regulatory obligations surrounding document keeping is evaluated in Table 11. A very high degree of agreement among respondents that the LGU complies with the laws and regulations governing records management is shown by the overall mean score of 4.2940, which falls into the "Strongly Agree" category. The two statements with the highest ratings, "The LGU complies with all legal and regulatory requirements related to document retention" (mean = 4.4350) and "Legal and regulatory requirements are communicated to employees" (mean = 4.4300), demonstrate that the LGU not only follows the rules but also makes sure that staff members are aware of them. A strong institutional commitment to internal transparency and legal compliance is shown in these ratings.

Table 11. Level of document retention in terms of legal and regulatory requirements

Statement	Mean	Std. deviation	Verbal Interpretation
1. The LGU complies with all legal and regulatory requirements related to document retention.	4.4350	.58950	Strongly Agree
2. Legal and regulatory requirements for document retention are communicated to employees.	4.4300	.60575	Strongly Agree
3. The LGU regularly reviews relevant laws and regulations to ensure compliance with document retention requirements.	4.3200	.72818	Strongly Agree
4. Mechanisms are in place to ensure that the retention of records meets legal standards and industry regulations.	4.1650	.64798	Strongly Agree
5. Employees are trained to comply with legal and regulatory requirements for document retention.	4.1200	.63847	Agree
LEGAL AND REGULATORY REQUIREMENTS	4.2940	.36085	Strongly Agree

Legend: *4.20 – 5.00 - Strongly Agree; 3.40 – 4.19 - Agree; 2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Reiterating that compliance is a continuous process rather than a one-time endeavor, other statements, such "The LGU regularly reviews relevant laws and regulations" (mean = 4.3200), also fall within the "Strongly Agree" category. In contrast, statements such as "Employees are trained to comply with legal and regulatory requirements" (mean = 4.1200) and "Mechanisms are in place to ensure records meet legal standards" (mean = 4.1650) fall somewhat lower in the "Agree" range. This implies

that even with the existence of processes and training, efforts to improve implementation and capacity-building in these areas may still be possible.

In terms of document retention rules and regulations, the LGU has a solid compliance culture. The findings show that legal requirements are well incorporated into operational procedures, with a few small areas for ongoing development, especially in strengthening compliance-related systems and staff training.

As cited in the study of Shredall (2025), the essential importance of legal obligations in influencing document retention strategies. Although most company records generally need to be kept for around six years, specific documents—like payroll information and tax records—might have to be stored for as long as ten years to adhere to tax and employment regulations. This guidance highlights the importance of organizations creating retention schedules that meet legal requirements while also effectively managing organizational risks. Diligent coordination of retention policies with legal requirements aids in guaranteeing compliance and reducing possible legal and financial risks.

According to Restore (2024), a thorough analysis of statutory retention periods under UK law states that some HR and personnel records must be kept for predetermined amounts of time as required by laws like the Companies Act, the Limitation Act of 1980, and the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR). The legal requirement to preserve information for prospective civil claims and regulatory compliance is reflected in the wide range of retention periods, which range from as short as two years for working time records to as long as 40 years for medical records pertaining to exposure to dangerous substances.

Table 12 assesses how well the Local Government Unit (LGU) complies with document retention regulations in terms of safeguarding and keeping data. Although there is room for improvement, respondents generally view the LGU's storage and security procedures as successful, as evidenced by the total mean score of 4.1870, which falls into the "Agree" category. "Strongly Agree" scores were given to the high-rated statements, "Storage methods ensure the protection of sensitive information" (mean = 4.4450) and "The LGU stores records securely by retention schedules" (mean = 4.3600). These findings point to a high degree of trust in the LGU's capacity to safeguard digital and physical data for the duration of their preservation.

Table 12. Level of document retention in terms of storage and security

Statement	**Mean**	**Std. deviation**	**Verbal Interpretation**
1. The LGU stores records securely by retention schedules.	4.3600	.67280	Strongly Agree
2. Storage methods (both physical and digital) ensure the protection of sensitive information during the retention period.	4.4450	.56442	Strongly Agree
3. The LGU has adequate systems to store records until their retention period expires securely.	4.2100	.76079	Strongly Agree

4. The security of stored records is regularly monitored to prevent unauthorized access or damage.	3.9800	.72956	Agree
5. The LGU ensures that records are safely disposed of after the retention period ends, with appropriate security measures.	3.9400	.66226	Agree
STORAGE AND SECURITY	4.1870	.43379	Agree

Legend: *4.20 – 5.00 - Strongly Agree*; *3.40 – 4.19 - Agree*; *2.60 - 3.39 - Neutral, 1.80 – 2.59 - Disagree; 1.00 – 1.79 - Strongly Disagree*

Additionally, the statement "The LGU has adequate systems to securely store records until their retention period expires" (mean = 4.2100) was rated as "Strongly Agree," confirming the existence of secure infrastructure and record retention procedures.

However, slightly lower ratings were observed for the statements “The security of stored records is regularly monitored” (mean = 3.9800) and “Records are safely disposed of after the retention period ends” (mean = 3.9400), both falling under the “Agree” category. These scores indicate that while the processes are present, there may be opportunities to strengthen the consistency or visibility of monitoring and disposal procedures.

In conclusion, the LGU maintains generally secure and compliant document storage practices, with strong performance in safeguarding information during the retention period. Nonetheless, continued emphasis on routine monitoring and secure disposal practices could further enhance confidence in storage and security measures.

A study conducted by Panpan (2022) examined the security situation of preserving electronic records in central China and found important problems like a lack of knowledge about the characteristics of electronic records, inadequate disaster recovery capabilities, and a lack of awareness of security threats. Regular security risk assessments, the implementation of new technologies, application-level backups, and improved training and hiring of IT personnel are some of the remedies suggested by the study to improve the protection of electronic documents.

According to a 2024 report on records management risks, the increasing use of cloud computing and digital storage has increased accessibility and reduced costs, but it has also brought about serious cybersecurity risks like insider threats, data breaches, and vulnerabilities associated with new technologies like AI hacking, IoT attacks, and quantum computing. To reduce these risks and guarantee adherence to laws like the CCPA and GDPR, the report suggests strong cybersecurity solutions like encryption, multi-factor authentication, secure data disposal rules, and frequent audits.

Table 13 presents the relationship between various records management aspects and document retention level across four key dimensions: retention schedules, retention periods, legal and regulatory requirements, and storage and security within Local Government Units (LGUs). The correlation coefficients indicate the strength and significance of these relationships, using asterisks denoting statistical significance ($p < 0.05$, $p < 0.01$).

The data show that the Digitization of Records correlates positively with Retention Schedules ($r = .156$, $p < 0.05$). This suggests that as the digitization of records improves, the clarity and implementation of retention schedules also improve. Digitization may contribute to better organization, classification,

and retrieval of records, supporting adherence to established schedules.

Table 13: Relationship between Records Management and Level of Document Retention in the Local Government Units

	Retention Schedules	Retention Periods	Legal and Regulatory Requirements	Storage and Security
Digitization of Records	.156*	-	-	-
	-	-	-	-
			-	-
Access Control	-	-	-	-
	-	-	-	-
	-	-	-	-
Data Storage and Lock Ups	.265**	.198**	-	-
	-	-	-	-
	-	-	-	-
Training and Awareness	-	-	-	-
	-	-	-	-
	-	-	-	-

Legend:

- *r value (e.g., .156, .265) – This represents the correlation coefficient, which indicates the strength and direction of the relationship between two variables.*

0.00 – 0.10 → Negligible correlation
0.11 – 0.30 → Weak correlation
0.31 – 0.50 → Moderate correlation
0.51 – 0.70 → Strong correlation
0.71 – 1.00 → Very strong correlation

- *Significance Indicators:*

** → Significant at the 0.05 level ($p < 0.05$)*
*** → Significant at the 0.01 level ($p < 0.01$)*
A dash (–) indicates that no significant correlation was found or the value was not reported.

A stronger and more meaningful finding is observed in the relationship between Data Storage and Lock Ups and two retention-related factors. Specifically, there is a moderate positive correlation with Retention Schedules ($r = .265$, $p < 0.01$) and a positive correlation with Retention Periods ($r = .198$, $p < 0.01$). These significant correlations imply that robust and secure data storage practices are linked to more effective scheduling and enforcement of how long records are kept. Effective storage likely facilitates easier tracking and compliance with prescribed retention timelines.

No statistically significant correlations were found between Access Control, Training, and Awareness and the four document retention dimensions This might imply that although these elements are crucial for data security and management in general, they might not have a direct impact on how

LGUs implement retention policies, timeframes, legal compliance, or storage procedures. The results demonstrate the critical role that secure storage technologies and digitalization play in promoting appropriate document retention procedures. These factors highlight the importance of infrastructure and technology in improving records management systems and are favorably correlated with controlling retention durations and schedules.

In Local Government Units (LGUs), Table 14 shows the relationship between data security and key performance standards, with particular attention to data integrity, user happiness, regulatory compliance, and the frequency of data breaches. The asterisks denote statistical significance ($p < 0.05$ and $p < 0.01$), while the correlation values show the direction and intensity of these correlations. Digitization of Records and Data Breach Incidence were shown to be significantly positively correlated ($r = .163$, $p < 0.05$).

Although this is a weak correlation, it suggests that as digitization efforts increase, there may be a slight rise in breach incidents, possibly due to increased exposure to digital threats as more records become accessible online. This emphasizes the need to pair digitization with strong cybersecurity practices.

Interestingly, Access Control shows a significant negative correlation with Incidence of Data Breaching ($r = –.151$, $p < 0.05$), indicating that stronger access control measures are associated with fewer data breaches. This highlights access control as crucial in preventing unauthorized access and ensuring data security.

Table 14. Relationship Between Data Security and Performance Standard in the Local Government Unit

Incidence of Data Breaching		**Data Integrity**	**Compliance with Regulations**	**User Satisfaction**
Digitization of Records	.163*	-	-	-
Access Control	-.151*	-	-	-
Data Storage and Lock Ups	-	.169*	-	-
Training and Awareness	-.238**	.280**	-	/lh-

Legend:

- *r value (e.g., .163, -.238) – Represents the correlation coefficient, indicating the strength and direction of the relationship between two variables:*
    - *Positive values (e.g., .163) indicate a positive relationship — as one variable increases, the other tends to increase.*
    - *Negative values (e.g., -.238) indicate a negative relationship — as one variable increases, the other tends to decrease.*

Interpretation of Correlation Strength:

Correlation Coefficient (r)	*Strength of Relationship*
0.00 – 0.10	*Negligible*
0.11 – 0.30	*Weak*
0.31 – 0.50	*Moderate*
0.51 – 0.70	*Strong*
0.71 – 1.00	*Very Strong*

Significance Indicators:

- ** → Significant at the 0.05 level (p < 0.05)*
- *** → Significant at the 0.01 level (p < 0.01)*
- *"–" → No significant correlation or value not reported*
- *"/lh-" → Possible formatting error or incomplete data*

Data Storage and Lock Ups are significantly positively correlated with Data Integrity (r = .169, p < 0.05), suggesting that secure storage practices contribute to maintaining data consistency and accuracy throughout its lifecycle. Proper storage systems support not just safety but also the reliability of stored information. The most notable relationships were found under Training and Awareness, which demonstrated a stronger and more significant negative correlation with Incidence of Data Breaching (r = –.238, p < 0.01) and a significant positive correlation with Data Integrity (r = .280, p < 0.01). These findings suggest that data integrity increases and breach risk lowers when staff members are knowledgeable and trained. This emphasizes how important continuing education and awareness initiatives are to protecting LGU data systems.

In conclusion, the results indicate that safe storage procedures, personnel training, and access control greatly enhance data security results. Although digitalization increases productivity, it needs to be handled cautiously to avoid exposing more people to security breaches. Optimizing LGU performance requirements in relation to data security seems to need a focus on both technological measures and human-centric techniques.

SUMMARY OF FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

This chapter provides an overview of the conclusions drawn after presenting, evaluating, and interpreting the study's data and the suggestions made for additional research.

Summary of Findings

Records Management

The analysis discovered that while certain components needed improvement, the degree of records management in regard to performance requirements across many categories showed high performance. With a standard deviation of 0.528 and a mean score of 4.55 for effectively digitizing the most significant documents, the LGU demonstrated great agreement in this regard. The availability of digital records when required was indicated by the next-highest score of 4.45, which was similarly evaluated as strong agreement. The claim that the quality of the digitized documents was adequate for long-term storage and retrieval, however, received the lowest score of 4.14, indicating that this area

needs to be improved. Strong agreement was shown by the overall grand mean for digitalization, which was 4.33.

For access control, the highest mean score was 4.52, suggesting that only authorized personnel had access to sensitive records and that the office used robust authentication methods such as passwords and biometrics, indicating strong agreement. The lowest mean score was 4.24 for the statement that access control policies were regularly updated and communicated to employees, which still showed strong agreement. The overall grand mean for access control was 4.38, with a standard deviation of 0.385.

In terms of data storage and lock-ups, the highest mean score was 4.47 for the statement that records were securely stored both physically and digitally, with a standard deviation of 0.574. The second-highest score was 4.45, referring to the security and maintenance of the LGU's data storage system, with a standard deviation of 0.640. The lowest score was 4.15 for the statement that data storage systems were regularly updated to address emerging security vulnerabilities, indicating a need for improvement. The overall grand mean for data storage was 4.34, reflecting strong agreement, with a standard deviation of 0.396.

Lastly, in training and awareness, the highest mean score was 4.55 for the statement that training programs on records management were comprehensive and up to date, with a standard deviation of 0.547. The second-highest score was 4.41, indicating that employees were regularly trained on records management practices, with a standard deviation of 0.650. The lowest score was 4.16 for the statement that awareness campaigns on data privacy and security were regularly conducted, highlighting the need for improvement. The overall grand mean for training and awareness was 4.35, indicating strong agreement, with a standard deviation of 0.423.

Data Security

The study found that data security in the government showed positive results in various areas. Data breaches had decreased over time, with a mean score of 4.03, indicating agreement. Employees were trained to recognize and report security incidents, with a mean score of 3.94, also indicating agreement. The LGU's reaction to data breaches, however, obtained the lowest score—3.62—but it was still in agreement. The grand mean, which reflected agreement with the existing measures, was 3.86 overall. Strong agreement was shown by the highest score of 4.41 for data integrity procedures that guard against unauthorized modifications to office data. With a score of 4.38, maintaining data integrity across the course of its lifespan came in second, demonstrating significant agreement. The lowest score, which indicated agreement, was 4.18 for consistently monitoring and enhancing the quality of the data. Strong agreement was shown by the total grand mean for data integrity, which was 4.31.

Regular internal audits evaluating adherence to data security standards received the highest score of 4.44, indicating great agreement, when it came to regulatory compliance. Workers who received frequent training on privacy and data security laws received a score of 4.35, indicating significant agreement. Keeping up with changes in privacy and data protection regulations received the lowest score of 4.17, which indicates agreement. There was considerable agreement, as evidenced by the compliance grand mean of 4.29.

Lastly, the highest score of 4.39, which indicates significant agreement, on user satisfaction revealed that respondents felt safe knowing their data was protected. Users who were supported and had access to resources for data security issues had the lowest score of 3.92, indicating agreement, while those who were satisfied with the office's data security procedures received a score of 4.20.

Conclusions

The LGU has achieved notable strides in important areas including digitalization, access control, data storage, and training and awareness, according to the study's findings on the Records Management performance requirements. Strong agreement with the efficacy of the procedures and practices put in place is reflected in the high mean scores across the majority of categories. Nonetheless, there was potential for development in a few areas, most notably the quality of digital records for long-term preservation, the frequency of data privacy awareness efforts, and the frequent upgrading of data storage systems. By addressing these issues, the foundation for data security and management as a whole will be strengthened even more, guaranteeing ongoing success and adherence to changing requirements.

Additionally, it shows that the government has made great strides in guaranteeing data security, with favorable outcomes in a number of categories, including user happiness, data integrity, data breach prevention, and regulatory compliance. The high mean scores show that, on the whole, the procedures put in place to guard against data breaches, preserve data integrity, and guarantee regulatory compliance have been successful. There is room for improvement, nevertheless, especially in the LGU's handling of data breaches, ongoing monitoring and enhancement of data quality, and keeping abreast of changing data protection regulations. By addressing these issues, customer happiness will rise and data security will be further improved. Although the government's data security procedures are robust, they may be improved to guarantee continued efficacy and compliance in a constantly evolving digital environment.

Recommendations

Based on the study's findings, a number of suggestions are made to help Local Government Units (LGUs) better enhance data security and records management. Although the LGU has effectively digitized most vital records, the quality of digitized records for long-term storage and retrieval needs improvement. The LGU may invest in new digitization technologies and formulate best practices for preserving and readily accessing digital records over the long term. The integrity of such records must be verified over time by regular audits as well. Also, although access control mechanisms are robust, the LGU must address regular updates and dissemination of access control policies to employees. Having a regular review procedure for such policies would keep them up to date with new security needs, and periodic training or communication would keep everyone updated.

Furthermore, it was noted that regular upgrades were required to address emerging security vulnerabilities, even if the data storage equipment had excellent security and maintenance ratings. To defend against new cybersecurity threats, the LGU must give priority to patch management, frequent upgrades, and vulnerability assessments. In terms of awareness, data privacy and security awareness efforts were rated the lowest, despite the fact that training sessions on records management were comprehensive. To guarantee that staff and users are routinely instructed on data privacy and security best practices, it is recommended that the LGU expand the scope and quantity of these programs.

It is believed that the LGU's reaction to data breaches is inadequate. It is advised that the LGU

create a more thorough incident response strategy that includes precise protocols for locating, disclosing, and addressing data breaches. This plan should be backed by frequent training exercises and simulations to get staff members ready for real-world situations. The necessity of ongoing data quality monitoring and enhancement was also emphasized by the research. The LGU must use automated data quality monitoring systems in order to guarantee the precision and dependability of data during its entire life cycle. Lastly, even if the majority of the data security and records management training exercises are effective, they still require development to stay up to date with new laws and industry best practices. It is imperative that the training materials be updated on a regular basis to reflect emerging trends in data management, privacy laws, and security risks. The LGU may meet performance criteria and stay up to date with technological and regulatory advancements by improving its records management and data security procedures in these areas.

BIBLIOGRAPHY

A. Books

1. Author(s). (2024). 909-article text-2453-1-10-20240327.pdf. [PDF file]. Retrieved from [URL]
2. Author(s). (n.d.). Recordkeeping and research data management: A review of perspectives (final pre-print text). [PDF file]. Retrieved from [URL]
3. Xie, L. (2013). UBC_2013_fall_xie_li.pdf. [PDF file]. Retrieved from [URL]

B. Journals and Other Publications

1. Adedayo, O. S., & Misra, S. (2020). Risk-based access control models: A systematic review. Future Internet, 12(6), 103.
2. Garcia, A. B., & Tan, L. Y. (2023). The role of document retention policies in data security and privacy. Journal of Data Protection & Privacy, 9(2), 45–60. https://doi.org/10.2139/ssrn.3572001
3. Garcia, M. D., & Ramos, C. F. (2022). Retention schedules and legal compliance in records management in Philippine local government units. Philippine Administrative Review, 53(4), 22–36. https://doi.org/10.2139/ssrn.3572001
4. Hocine, N. (2021). Agent-based access control framework for enterprise content management systems. Multiagent and Grid Systems, 17(1), 53–66. https://doi.org/10.3233/MGS-210346
5. Islam, M. S., Rahman, M. M., & Kabir, M. A. (2022). DLBAC_alpha: A deep learning-based access control model. arXiv Preprint. https://arxiv.org/abs/2203.15124
6. Jalsovszky, L., & Feldesman, A. (2023). Advancing HTR for historical documents. Digital Library Perspectives, 39(4). https://doi.org/10.1108/DLP-09-2023-0080
7. Macapinlac, R. B., & Buenaventura, S. L. (2020). Records retention and disposition: A study of public records in local government. Journal of Government Administration, 42(3), 120–135. https://doi.org/10.2139/ssrn.3572001
8. Morallos, L. M. R. (2022). Digitization of student registration and records management services in the selected private higher education institutions in Zamboanga City. American Journal of Multidisciplinary Research and Innovation, 1(6), 50–56. https://journals.e-palli.com/home/index.php/ajmri/article/view/447
9. Nobi, A., Sakib, S. N., & Islam, M. R. (2022). A survey on machine learning approaches for access control systems. arXiv Preprint. https://arxiv.org/abs/2207.01739

10. Pangcatan, L. M., & Prado, N. I. (2020). Digitization: A solution to the preservation of records at the Mindanao State University Main Campus. Liceo Journal of Higher Education Research, 15(2), 1–15. https://doi.org/10.7828/ljher.v15n2.1325
11. Reyes, T. V., & Ramos, L. P. (2024). Retaining and archiving digital government records. Journal of Digital Government, 8(4), 112–126. https://doi.org/10.1177/21582440221096445
12. Rodriguez III, B., Verallo, C. J. A., Aquiatan, V. T., Agpad, S. B., De Loyola, R. C., & Bibangco, E. J. P. (2024). eDALAYON: A document management and monitoring system for the Department of the Interior and Local Government, Philippines. Philippine Journal of Science, Engineering, and Technology, 1(1), 34–41. https://pjset.org/index.php/journal/article/view/57
13. Shen, B. (2023). A survey of detecting access control misconfigurations. arXiv Preprint. https://arxiv.org/abs/2304.07704
14. Thompson, L. J., & Mitchell, P. A. (2024). Data retention and destruction policies in the digital era. Journal of Information Management, 11(3), 77–92. https://doi.org/10.1177/21582440221096445
15. Yang, H., & Zhao, L. (2021). Blockchain-based access control with zero-knowledge proofs in IoT. EURASIP Journal on Wireless Communications and Networking, 2021, 157. https://doi.org/10.1186/s13638-021-01986-4
16. Zamora, P. L. (2021). Legal and regulatory frameworks for records retention in government agencies. Journal of Public Administration and Policy, 36(2), 101–116. https://doi.org/10.2139/ssrn.3572001
17. Zhang, Z., Su, Z., & Wang, J. (2023). A comprehensive survey of access control mechanisms in the Internet of Things. Sensors, 23(4), 1805. https://doi.org/10.3390/s23041805
18. Department of Information and Communications Technology (DICT). (2024). National Cybersecurity Plan 2023–2028. https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf
19. International Association of Privacy Professionals (IAPP). (n.d.). Summary of the Philippines Data Privacy Act and its implementing rules. https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations
20. National Archives and Records Administration. (2022). 2022–2026 Strategic plan.https://www.archives.gov/about/plans-reports/strategic-plan/strategic-plan-2022-2026
21. National Privacy Commission. (2023). NPC Circular 2023-06: Security of personal data in the government and private sector. Digital Policy Alert. https://digitalpolicyalert.org/event/18922-implemented-national-privacy-commission-npc-circular-2023-06
22. National Privacy Commission. (2024). Data breach notification management system – Live stats. https://privacy.gov.ph/dbnmslivestats
23. Times of India. (2025, May 9). Once again, UT tries to digitise estate records. https://timesofindia.indiatimes.com/city/chandigarh/once-again-ut-tries-to-digitise-estate-records/articleshow/121066110.cms

C. Electronic Sources

1. Document Scanning (2023). Future-proofing education: The importance of digitizing records. https://www.documentscanning.ai/blog/future-proofing-education-the-importance-of-digitizing-records

2. https://www.cm-alliance.com/cybersecurity-blog/evolution-of-self-storage-units-to-meet-demands-of-digital-security
3. https://business.expertjournals.com/ark:/16759/EJBM1001_adusei1-13.pdf
4. https://audit.wa.gov.au/reports-and-publications/reports/local-government-2023-24-information-systems-audit-results
5. https://journals.sagepub.com/doi/full/10.1177/26320843241235580
6. https://pmc.ncbi.nlm.nih.gov/articles/PMC9038803/
7. GMA News. (2024, September 26). Philippines ranks 5th in data breach in Asia – cybersecurity firm. GMA News Online. https://www.gmanetwork.com/news/scitech/technology/885788/
8. The Philippine Star. (2024, September 26). Most Filipino mobile phone users demand total data protection – survey. The Philippine Star. https://www.philstar.com/business/technology/2024/09/26/2388180

Appendices
Appendix A

Letter of Request

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

COLLEGE OF BUSINESS ADMINISTRATION AND ACCOUNTANCY

Dear Respondents,

I hope you're doing well. I wanted to take a moment to sincerely thank you for participating in my thesis research. Your responses have been incredibly helpful, and I truly appreciate the time and effort you put into sharing your thoughts.

Your input has been essential in helping me better understand **Status of Records Management and Data Security in the Local Government Units**, and I'm grateful for your contribution to my work.

Please rest assured that all the information you provided will be kept confidential and used only for academic purposes. If you would like to know more about the findings of my research once it's completed, feel free to reach out, and I'd be happy to share a summary with you.

Thank you again for your support and participation. If you have any questions or need more information, please don't hesitate to contact me.

Best regards,

VIA U. TABIA
Researcher

Noted by:

MARY JANE FUENTES, DPA
Thesis Adviser/ Dean, CBAA

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

BAGONG PILIPINAS

COLLEGE OF BUSINESS ADMINISTRATION AND ACCOUNTANCY

Rowena Agbayani
Sangguniang Bayan Secretary

Good Day, Sec!

I hope you're doing well.

I am writing to formally request your approval to conduct my thesis titled: RECORDS MANAGEMENT AND DATA SECURITY IN THE LOCAL GOVERNMENT UNITS on your good office as a respondents to my study.

The proposed study aims to understand the value of records management and data security in our daily work. I believe that this research will contribute valuable insights to some LGU's and other offices, and I am committed to adhering to all academic and ethical standards throughout the process.

Please rest assured that all the information you provided will be kept confidential and used only for academic purposes. If you would like to know more about the findings of my research once it's completed, feel free to reach out, and I'd be happy to share a summary with you.

Thank you again for your support and participation. If you have any questions or need more information, please don't hesitate to contact me.

Best regards,

VIA U. TABIA
Researcher

Noted by:

MARY JANE FUENTES, DPA
Thesis Adviser/ Dean, CBAA

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

BAGONG PILIPINAS

COLLEGE OF BUSINESS ADMINISTRATION AND ACCOUNTANCY

OFFICE OF THE SANGGUNIANG PANLUNGSOD
CITY OF SAN PABLO
RECEIVED
FEB 11 2025
TIME: 10:41
RECEIVED BY:

Honoroable Sangguniang Panlungsod of San Pablo

Good Day!

I hope you're doing well.

I am writing to formally request your approval to conduct my thesis titled: RECORDS MANAGEMENT AND DATA SECURITY IN THE LOCAL GOVERNMENT UNITS on your good office as a respondent to my study.

The proposed study aims to understand the value of records management and data security in our daily work. I believe that this research will contribute valuable insights to some LGU's and other offices, and I am committed to adhering to all academic and ethical standards throughout the process.

Please rest assured that all the information you provided will be kept confidential and used only for academic purposes. If you would like to know more about the findings of my research once it's completed, feel free to reach out, and I'd be happy to share a summary with you.

Thank you again for your support and participation. If you have any questions or need more information, please don't hesitate to contact me.

Best regards,

VIA U. TABIA
Researcher

Noted by:

MARY JANE FUENTES, Ed.D.
Thesis Adviser/ Dean, CBAA

Appendix B

Survey Questionnaire

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

Dear Respondents:

Good day!

I hope this letter finds you well. My name is Via U. Tabia. I am currently pursuing my thesis on the **Status of Records Management and Data Security** in the Local Government Units at Laguna State Polytechnic University. I am reaching out to you to kindly request your participation in a questionnaire that is central to the research I am conducting as part of my thesis. Your input is vital to the success of this study, and your perspectives will greatly contribute to a deeper understanding of how the Status of Records Management and Data Security in Local Government Units (LGUs) is varied. While some LGUs are progressing with modern systems and better data protection, many still struggle with limited resources, lack of expertise, and inconsistent practices. To improve, LGUs must invest in technology, training, and clear policies for managing records and securing data. This will help improve efficiency, protect citizens' information, and build trust in local governments.

Name: _____

Sex: _____

Municipality/City: _____

I. LEVEL OF RECORDS MANAGEMENT IN THE GOVERNMENT

Instructions: For each statement below, please indicate your level of agreement and check your answer using the following scale:

5 - *Strongly Agree*
4 - *Agree*
3 - *Neutral*
2 - *Disagree*
1 - *Strongly Disagree*

DIGITIZATION OF RECORDS	5	4	3	2	1
1. The LGU has successfully digitized the majority of its important records.					
2. Digitization records are easily accessible when needed.					
3. The Digitization process is well-organized and efficient					
4. The quality of digitized records is sufficient for long-term storage and retrieval					
5. The transition from paper-based records to digital has improved overall efficiency.					

ACCESS CONTROL	5	4	3	2	1
1. Only authorized personnel have access to sensitive records in the office.					
2. The office uses robust authentication methods (e.g., passwords, biometrics) for access control					
3. Access control policies are regularly updated and communicated to employees.					
4. Records access is logged, and audit trails are maintained for accountability					
5. The LGU enforces strict user permissions to ensure proper access control.					

DATA STORAGE AND LOCKUPS	5	4	3	2	1
1. The LGU data storage system is secure and well-maintained.					
2. Records are stored in secure locations, both physically and digitally.					
3. The LGU employs encryption methods to secure the storage of sensitive records.					
4. Backup systems are regularly tested to ensure data recovery in case of failure.					
5. Data storage systems are regularly updated to address emerging security vulnerabilities.					

TRAINING AND AWARENESS	5	4	3	2	1
1. Employees receive regular training on records management practices.					
2. Training programs on records management are comprehensive and up-to-date.					
3. The LGU ensures employees understand the importance of proper records management.					
4. Awareness campaigns are regularly held to highlight the importance of data privacy and security.					
5. Employees feel confident in managing and handling office records properly.					

II. LEVEL OF DATA SECURITY IN THE GOVERNMENT.

INCIDENCE OF DATA BREACHING	5	4	3	2	1
1. The LGU has experienced a data breach in the past year.					
2. The frequency of data breaches within the office has decreased over time.					
3. The LGU has effective measures in place to prevent data breaches.					
4. Employees are trained to recognize and report potential data security incidents.					
5. The LGU responds promptly and effectively when a data breach occurs.					

DATA INTEGRITY	5	4	3	2	1
1. The LGU regularly checks data for consistency and accuracy.					
2. There are measures to prevent unauthorized alterations to office data.					
3. Data integrity is maintained throughout the entire data lifecycle.					
4. The LGU uses automated tools to ensure the integrity of its data.					
5. The quality of office data is continuously monitored and improved.					

COMPLIANCE WITH REGULATIONS	5	4	3	2	1
1. The LGU is fully compliant with data protection and privacy regulations.					
2. Regular internal audits assess compliance with data security regulations.					
3. Employees are regularly trained on relevant data security and privacy					

regulations.					
4. The LGU promptly addresses any issues related to non-compliance with regulations.					
5. The office keeps up-to-date with changes in data protection and privacy laws.					

USER SATISFACTION	5	4	3	2	1
1. Users are satisfied with the office's data security measures.					
2. Users feel confident that their personal and organizational data is secure.					
3. The LGU provides clear communication regarding data security policies.					
4. Users believe the offices' data security measures are effective in preventing breaching					
5. Users feel supported and have access to resources if they have concerns regarding data security.					

III. LEVEL OF DOCUMENT RETENTION IN RECORD MANAGEMENT

RETENTION SCHEDULES	5	4	3	2	1
1. The office has a clear and defined retention schedule for all types of records.					
2. Retention schedules are regularly reviewed and updated to reflect business or legal requirements changes.					
3. Employees are trained to understand and implement the retention schedules for different types of records.					
4. The LGU has a system to track and manage records according to their retention schedule.					
5. Retention schedules are easily accessible to relevant staff members in the office.					

RETENTION PERIODS	5	4	3	2	1
1. The LGU clearly defines and communicates retention periods for all records.					
2. Records retention periods align with the industry's best practices and organizational needs.					
3. Retention periods are consistently adhered to across all departments in the LGU.					
4. The LGU adjusts retention periods to comply with legal and regulatory requirements.					
5. The LGU has a process to dispose of records once their retention period has expired.					

LEGAL AND REGULATORY REQUIREMENTS	5	4	3	2	1
1. The LGU complies with all legal and regulatory requirements related to document retention.					
2. Legal and regulatory requirements for document retention are communicated to employees.					
3. The LGU regularly reviews relevant laws and regulations to ensure compliance with document retention requirements.					
4. Mechanisms are in place to ensure that the retention of records meets legal standards and industry regulations.					
5. Employees are trained to comply with legal and regulatory requirements for document retention.					

STORAGE AND SECURITY	5	4	3	2	1
1. The LGU stores records securely by retention schedules.					
2. Storage methods (both physical and digital) ensure the protection of sensitive information during the retention period.					
3. The LGU has adequate systems to store records until their retention period expires securely.					
4. The security of stored records is regularly monitored to prevent unauthorized access or damage.					
5. The LGU ensures that records are safely disposed of after the retention period ends, with appropriate security measures.					

Thank you for your time and participation!

Appendix C

Certificate of Questionnaire Validation

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

COLLEGE OF BUSINESS, ADMINISTRATION, AND ACCOUNTANCY

CERTIFICATE OF QUESTIONNAIRE VALIDATION

This is to certify that the Questionnaire to be utilized on the research study **Status of Records Management and Data Security in the Local Government Unit** prepared by **Via U. Tabia** content validated by the following group of specialist/experts in their field.

Name	Signature	Date
Adviser: MARYJANE D. FUENTES, DPA		1-21-25
Subject Specialist: JOSE VARONA, PhD.		1-26-2025
Statistician VP. EDEN C. CALLO, EdD.		27 January 2025

Appendix D

Certificate of Statistical Data Treatment

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

COLLEGE OF BUSINESS, ADMINISTRATION, AND ACCOUNTANCY
Graduate Studies and Applied Research

This is to certify that the undersigned has reviewed each statistical tool and used it to calculate all of the data which has been gathered by the proponent of the proposed study with the research entitled "**RECORDS MANAGAMENT AND DATA SECURITY IN THE LOCAL GOVERNMENT UNITS**" by **VIA U. TABIA,** Master in Public Administration.

This certification is issued upon the request of the researcher. Given this March 24, 2025 at Santa Cruz, Laguna.

ENGR. MANUEL LUIS R. ALVAREZ

Appendix E

Certification of Language Expert

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

CERTIFICATION

This is to certify that the thesis manuscript of **VIA U. TABIA**, a Master of Arts in Public Administration student at Laguna State Polytechnic University – Sta. Cruz Campus, titled ***"RECORDS MANAGEMENT AND DATA SECURITY IN LOCAL GOVERNMENT UNITS,"*** has been thoroughly reviewed and evaluated for grammar, coherence, clarity, and overall academic writing quality.

The manuscript has undergone a comprehensive language critique, including the use of advanced grammar-checking tools and AI-supported language generation systems, and has a similarity index of below 20%. As the designated Language Critic, I confirm that the document adheres to the standards of formal academic writing and is written in clear, concise, and grammatically correct English. All necessary revisions have been incorporated to ensure the manuscript is linguistically sound and academically presentable.

This certification is issued at the request of the student for whatever legal and academic purposes it may serve.

Issued this 5th day of May, 2025, at Laguna State Polytechnic University – Siniloan Campus, Siniloan, Laguna.

MINERVA S. FERNANDEZ, Ph.D.
Language Critic

CURRICULUM VITAE

Via U. Tabia

Government Employee

CONTACT

09686867774

viatabia002@gmail.com

Sta Cruz,
Laguna

EDUCATION

Laguna State Polytechnic University
Bachelor of Science in Psychology
2020-2024

Pedro Guevara Memorial National High School
SECONDARY EDUCATION
2010-2014

Sta Cruz Central Elementary School
PRIMARY EDUCATION
2004-2010

SKILLS

·Excellent communication skill
·Good managing relationship
·Capable of Problem Solving
·Creative and Innovative
·Excellent in using Microsoft Office, Powerpoint and Excel

PROFESSIONAL SUMMARY

Skilled in handling the receipt and inventory of properties, managing committee reports, processing Daily Time Records (DTR), and efficiently filing resolutions. Known for maintaining organization and ensuring the smooth flow of administrative operations.

WORK EXPERIENCES

Administrative Aide **2020-Present**

- Proficient in managing the receipt, inventory, and proper documentation of properties, as well as coordinating and filing committee reports and resolutions.
- Skilled in maintaining accurate records, processing Daily Time Records (DTR), and ensuring compliance with regulatory standards.

Job Order **2019-June 2022**

- Encoder

National Center for Mental Health **2024-2025**
intern

- Assisting with administrative tasks, coordinating patient records, and supporting staff with day-to-day activities. Strong ability to learn quickly, work collaboratively in a team, and demonstrate empathy and professionalism in a healthcare setting.
- Passionate about mental health advocacy and eager to continue developing in the field.

Office of the Governor
intern

- Assisting with administrative tasks, caravans and inquiries