INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY: APPLIED BUSINESS AND EDUCATION RESEARCH
2024, Vol. 5, No. 8, 3272 – 3300
http://dx.doi.org/10.11594/ijmaber.05.08.26

Research Article

Philippine Social Security System: An Evaluation Of Strategic Approach To Digital Services

Glenn Mhar B. Galang, Elizabeth B. Villa*

De La Salle University Dasmari nas, Philippines

Article history:
Submission 31 July 2024
Revised 08 August 2024
Accepted 23 August 2024

**Corresponding author:*
E-mail:
esbuena@dlsud.edu.ph

ABSTRACT

This study was conducted to assess the digital services of the Philippine Social Security System in terms of processing of personal data, organizational measures, physical measures, and technical measures. The research employed a descriptive-correlational approach, utilizing a questionnaire as the primary data gathering instrument. However, interviews among the 5 heads of the 5 biggest branches of SSS in the NCR were utilized to validate the data taken in the questionnaire among the 3 groups of respondents: BPOs (120), front-liners (180), and clients (1292). For BPOs and front-liners, complete enumeration was used, while convenience sampling was utilized for clients. Weighted mean and one-way ANOVA were used for the treatment of the data. The study revealed that all the indicators in all four variables were, on average, partially implemented. The seriousness of the encountered problems led to a highly recommended assessment of the presented solutions. Further investigation revealed no significant differences in assessment among the three groups of respondents.

The study's findings led to the conclusion that Philippine Social Security requires additional physical and electronic paperwork. Additionally, the Philippine Social Security System shares and exchanges personal data with other parties through digital channels. Furthermore, the corporate orientation course for newly hired or absorbed employees does not include security management, despite its availability. Finally, SSS has yet to use advanced technology to detect fake, altered, and fraudulent documents; hence, it still needs to use advanced technology to formulate a comprehensive data security manual to integrate digital measures against cybercrime.

Therefore, the study's findings and conclusions inform the following recommendations: Firstly, we should archive and retain physical or electronic documents containing personal data in secure and protected record rooms, offsite storage facilities, or receptacles or cabinets, in accordance with the issued policies. Second, only with prior consent or authority from the data subjects, a judicial order, or a data sharing agreement can we use digital platforms to disclose and share personal data with third parties. Third, newly hired or absorbed employees should include data security

How to cite:
Galang, G. M. B. & Villa, E. B. (2024). Philippine Social Security System: An Evaluation Of Strategic Approach To Digital Services. *International Journal of Multidisciplinary: Applied Business and Education Research*. *5*(8), 3272 – 3300. doi: 10.11594/ijmaber.05.08.26

management in their corporate orientation course. Fourth, we should use advanced technology to detect fake, altered, and fraudulent documents. Finally, we should formulate a data security manual to incorporate digital measures against cybercrime.

Keywords: *Philippine Social Security System, Digital Transformation, Fraud, Investigation, Cybercrime, Criminology, Criminal Justice*

Introduction

The use of computers to engage in illegal activities such as fraud, trafficking of child pornography, intellectual property theft, identity theft, and privacy violations is known as cybercrime. With computers playing an essential role in commerce, entertainment, and government, cybercrime has gained significant importance, especially over the internet. Initially, cybercrime was predominantly an issue in the Philippines due to early and widespread adoption of computers and internet. However, in the 21st century, cybercrime has become a global problem, impacting communities worldwide, with few localities left unaffected by some form of cybercrime.

As the world increasingly depends on digital technology, individuals participate in online shopping, streaming movies and music, and obtaining answers to various inquiries with a straightforward internet search. Consequently, people want the government to provide a comparable experience that is easy to use. Government agencies that do not update and plan for the future are already falling behind. Implementing change often necessitates a substantial investment of time.

The rapid and substantial increase of malware in recent years has presented a notable security risk to intelligent systems. Previous static and dynamic analysis methods are ineffective in achieving a high recognition rate and result in significant processing complexity. Machine learning (ML) and deep learning (DL) models, which have been recently developed, can be used effectively to identify and categorize cyberattacks and Malware. (Alzubi, 2023).

According to Granicus (2023), modernization is primarily driven by external causes, especially the government. In a study conducted by Granicus (2023), 48% of surveyed respondents identified a deficiency in digital strategy and tools for involving citizens as their primary technology obstacle. They anticipate intuitive on their cellphones and want that the government offer a similar level of convenience.

As per the International Social Security Association (2019), digital technologies have demonstrated their significant impact in various domains, including healthcare, communication, workplace safety, job hunting, contribution collection, and data sharing. All of them possess the capacity to assist individuals who require aid, such as the elderly who have limited mobility or individuals with disabilities who have limited mobility. It has enhanced the level of service quality, reduced operating expenses, and enhanced the reliability of company procedures.

Digital transformation, as defined by Skog (2019), refers to the ongoing process in which companies create and implement new digital ideas to enhance their products, services, and business models. During the process of digital transformation, the adoption of new products and services may necessitate the utilization of distinct resources and work processes compared to older ones.

In the study of Chang et. al, (2022), Advanced technologies, such as the Internet of Things and core information communication technology frameworks, enable the sharing of information.

A single user-friendly gadget can grant consumers access to all tools with a simple click; nevertheless, the reliability of the information acquired is still uncertain. Misinformation, which encompasses false, harmful, or deceptive information, whether intentional or unintentional, can exacerbate misconceptions. In order to prevent these instances from progressing into criminal activity, a comprehensive financial fraud-awareness model was developed in their study.

The primary objective of the model is to achieve precise fraud detection and classification by employing the natural language processing technique. A chatbot designed to detect and prevent fraudulent activities is created using the model and then deployed on a popular social network platform called LINE. This solution is designed to handle finance-fraud cases and offer anti-fraud recommendations to address anticipated instances of fraud.

Further, the Asian Productivity Organization (2021) emphasizes that recent technological breakthroughs have provided a platform for governments to seek to improve public services. Federal, provincial, and local governments are under pressure to reevaluate their strategies for enhancing service quality. As a result, the digitalization of public sector organizations is one of the most significant transformations occurring globally today. Digital governance is a work in progress that is moving forward at a rapid pace.

Kirilenko & Aleksee (2021) found in their study that the rise of digital technology has led to the emergence of virtual reality, governed by the norms and practices of the networked community. This finding contradicts the notion that digital transformation has solely beneficial impacts. Civil society members are at a higher risk of falling prey to various cybercrimes because they refuse to accept most of the essential regulations imposed by national governments for political reasons. These infractions may encompass computer fraud, inflammatory writings, and fraudulent activities. The study additionally discovered that participant observation, comparative legal analysis, and discourse analysis collectively demonstrate that the digital revolution has increased the difficulty for the government to influence the cultural development of society. Furthermore, criminal organizations have shown a newfound interest in computer technologies.

In another piece of literature, Institutional Asset Manager published an article in 2021 indicating that 23% of all cyberattacks target financial institutions, while the average cost of a single data breach for financial institutions is USD5.72 million. Fifty-three percent of data breaches, according to a separate survey, are financially motivated; therefore, the industry is continuously on the cybercrime radar. In other industries, malicious users exploit social engineering, credential stuffing, and program flaws to get a foothold. However, the financing industry is unique in that these individuals predominantly compromise corporate internal networks.

Financial sector incurred substantial losses due to fraudulent activities, which have emerged as the primary challenge for the industry. Corporations allocate substantial resources to mitigate such fraudulent activities. According to reports, 63.6% of financial institutions employing Automated Fraud prevention technologies effectively thwarted fraudulent activities prior to their occurrence.

Approximately 80% of experts are confidence in the efficacy of Artificial Intelligence (AI)-based platforms for reducing fraud, according to certain estimates. Furthermore, numerous research papers have utilized artificial intelligence (AI) tools to combat fraud. This study employs a systematic literature review methodology to identify the rising domains of fraud detection via artificial intelligence. The researchers have examined 241 scholarly articles that were published throughout the past two decades. The articles in the literature review were sourced from the Scopus database. The meta-analysis and network analysis were conducted, revealing an upward tendency in this study field. The collaboration network between authors and coauthors is studied using the VOS viewer program. K-means clustering was utilized to ascertain the pivotal study domain, and subsequent research domains were also determined (Sood, 2023).

During the pandemic period in the Philippines, the Department of Justice's Office of Cybercrime received 1.2 million cyber tips in 2020, up from just 400,000 the previous year, according to a March 15, 2022, Inquirer's news report. This was an increase from the previous year's total of just 200,000. Internet fraud, sexual abuse and exploitation, cyberbullying, and identity theft are the most prominent types of online criminal activity.

Prior to the COVID-19 pandemic, the Philippines has already been witnessing a surge in cybercrime incidents.

In 2013, the Philippine National Police (PNP) recorded 42 instances of internet fraud, whereas in June 2018, the number of cases increased to 550. Moreover, a Fintech Alliance news piece from 2021 documented numerous cybercrime occurrences throughout the epidemic. Common internet fraud tactics employed by criminals include phishing, which involves the use of deceptive emails that impersonate respectable institutions. The purpose is to get sensitive and private information, such as debit and credit card details, digital banking credentials, and other financial account information. Lito Villanueva, Chairman of Fintech Alliance (2021), highlighted that although there are ample prospects for technologies to facilitate our transition to a digital financial system, these very opportunities are presently being utilized to inflict harm on individuals and the overall economy.

Therefore, it is imperative for individuals to remain vigilant in regards to online transactions and consistently verify any odd messages with the appropriate financial institutions. By doing so, individuals can protect their own assets and, consequently, contribute to a more robust economic recovery by minimizing the risk of cybercriminals impeding progress in the aftermath of the epidemic.

The Philippine Social Security System (SSS), a government institution, is responsible for ensuring the safety and well-being of every Filipino citizen. The SSS's services put every Filipino worker who contributes to the economy in a position of certainty and increased financial security, beginning with membership and continuing through retirement from private employment. Therefore, it is crucial to safeguard both the members' and the institution's interests, as the agency bears the responsibility for the social security of both private employees and employers. The institution has been around and has been protecting the interests of its members who belong to the private labor sector in order to provide its members with decent living, financial conditions, and funding assistance derived from the accumulated dues contributed while they are in service.

However, the SSS Special Investigation Department under the Legal and Enforcement Group has received thousands of complaints from the stakeholders pertaining to their victimization of cyber related crimes.

In a 2019 ABS-CBN news item, the Philippine Social Security System (SSS) issued a warning on a fake Facebook page, promising a giveaway for beneficiaries of the social insurance program. According to Senior Vice President of SSS Voltaire Agas, the organization has never organized a raffle and does not promote such events on social media. Let's not blindly accept what we read on social networking sites, Agas added. Agas also added that members can view official announcements on the SSS's official website.

Therefore, the PNP-ACG and SSS advise the general public to exercise caution when joining social media groups and urge the public to check their website or contact them by phone for any announcements.

As a reputable financial institution, SSS has unfortunately inevitably fallen prey to fraud and deception, particularly identity fraud. This may have led to the incorrect approval of benefits to a fictitious application member or claimant, as well as the loss of funds as a result of fraudulent cash transactions. Whether digital technology facilitates the transaction or not, this remains the case. The integrity of the institution and the public's trust in it could both suffer as a result of this. This type of cybercrime could cost the SSS money, resulting in the agency going bankrupt.

Since there is no record of the number of identity theft or identity fraud cases reviewed by the SSS, its primary concern is preventing false instances. Consequently, SSS places less emphasis on identity-related situations. This illustrates that SSS has a reactive as opposed to a proactive approach to fraud prevention. The vast majority of successful fraud schemes include either theft or fraudulent use of an individual's identity.

Undeniably, identity theft and identity fraud are unavoidable in the modern era due to technological developments. Identity thieves can easily access a person's personal information over the Internet or through the negligence of a person who voluntarily provides it. According to the National Policy Commission, which serves as the nation's watchdog for data privacy and protection, there are 45 million active Internet users and 32 million active mobile internet users.

Republic Act 11032, commonly referred to as the Ease of Doing Business and Efficient Government Service Delivery Act of 2018, simplifies and improves government processes and procedures. The Duterte government has implemented a significant legislation aimed at enhancing the economic competitiveness and facilitating company operations in the Philippines. The legislation, enacted on May 28, 2018, amends the 2007 Anti-Red Tape Act.

The revised legislation simplifies and optimizes all administrative procedures carried out by the government. This policy is applicable to all offices and agencies of the Executive Department, including Local Government Units (LGUs), government-owned or -controlled corporations (GOCCs), and other government instrumentalities, whether in the Philippines or overseas, that provide services relating to commercial and non-business transactions.

Therefore, individuals should remain vigilant when engaging in online transactions and consistently verify the legitimacy of any suspicious messages with the appropriate financial institutions. By doing so, individuals can protect their personal resources and thereby contribute to a more effective economic recovery, minimizing the risk of cybercriminals impeding progress in the aftermath of the epidemic.

With this mandate, the SSS is among the government-owned and controlled corporations that promptly address the objective of simplifying business operations in the country by consolidating digital services and incorporating information and communication technology into its systems and procedures. The objective is to minimize the procedural complexity involved in conducting business transactions within the country. The primary objective of this organization is to promptly satisfy the needs of Filipino workers by offering social security services. The objective is to meet the government's responsibility in carrying out its constitutional duty. The Philippine administration has unequivocally expressed its intention to proceed with reforms and the implementation of digital governance.

In a nation where both SSS members and non-members are susceptible to identity theft or identity fraud, it is crucial for the SSS to establish and enhance its policies against such cybercrimes. This is because the SSS plays a vital role in promoting social justice and ensuring equitable social welfare for all Filipino members. Furthermore, as the SSS moves to digital transactions, it is imperative that they ensure the safety and security of the digital platforms. This is crucial since it is one of the fundamental principles of social justice, ensuring that all Filipino members enjoy equal social benefits. As a criminology practitioner and member of this organization, my role is to protect the SSS from deception and fraudulent manipulations, specifically through identity theft and identity fraud. I believe that it is necessary to establish a protective security system that includes a set of policies, procedures, and advanced technology to accurately identify and match transacting members with their archived records.

Implementing this precaution is crucial in order to protect SSS from the risks of identity theft, deceit, and fraudulent activities. Therefore, this study was done to assess the level of digital transformation in the Philippine Social Security System, focusing on its present policies and procedures, as well as the processing of personal data, organizational measures, physical measures, and technical measures. This study examined the level of data security offered by current legislation and protocols in order to mitigate the risks of identity theft, fraud, and mismanagement.

This study employed a range of criteria to assess the digital services provided by the SSS, including the processing of personal data, organizational measures, physical measures, and technical measures. Personal data processing encompasses a broad spectrum of activities involving personal data, which can be carried out either manually or automatically. Personal data may undergo collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, utilization, transmission, dissemination, availability, alignment, combination, restriction, erasure, or destruction.

Organizational measure refers to the methods employed by an organization to provide its services. These methods encompass various aspects, including policy development, policy implementation, enforcement, regulation, as well as the planning and execution of current and future services. Physical measures currently encompass the utilization of paper-based application forms, physical devices, and security parameters to guarantee the safety and security of individuals involved. On the other hand, technical measures refer to digital-based applications employed in online platforms for registration, cloud storage, and security validation.

While there are several studies on the policies and procedures of the Philippine Social Security System as a financial institution, there is little to no information available regarding the measures being taken by SSS to streamline its digital services and integrate ICT into its systems and procedures. It is also important to consider the potential negative impacts of digital transformation on society, as well as the steps being taken by financial institutions to prevent cyber-attacks and protect their clients' data.

Therefore, the study's results can be used to advocate for improved public administration by continuing the process of digitalization, particularly for the SSS. The SSS plays a crucial role in promoting social justice and protection through its social security services, and it also contributes to the nation's efforts in digital transformation. Stakeholders may transition from manual to digital transactions while mitigating the adverse effects of technology advancement, such as concerns around cybercrime.

Statement of the Problem

The study was conducted to assess the digital transformation in the Philippine Social Security System.

Specifically, it sought to answer the following questions:

1. What is the demographic profile of the respondents in terms of:
   1.1 age,
   1.2 gender,
   1.3 educational attainment,
   1.4 type of membership/employment in the SSS, and
   1.5 years as member/employed in the SSS?
2. How do the three (3) groups of respondents assess the digitization of services in the Philippine Social Security System in terms of:
   2.1 processing of personal data,
   2.2 organizational measures,
   2.3 physical measures, and
   2.4 technical measures?
3. Is there significant difference in the evaluation among the three (3) groups of respondents?
4. What are the difficulties encountered in the digitization of services in the Philippine Social Security System?
5. What counter measures are employed to address the difficulties encountered in the digitization of services in the Philippine Social Security System?
6. What enhancement program could be proposed based on the results of the study?

Hypothesis

There is no significant difference in the evaluation among the three (3) groups of respondents.

Methods

This section provides and examines the methodologies and techniques utilized to collect the necessary data and information for the study. The components encompassed in this study are the Research Design, Respondents, Sampling Techniques, Instruments, Validation of Instruments, Data Gathering Procedure, and Statistical Treatment of Data.

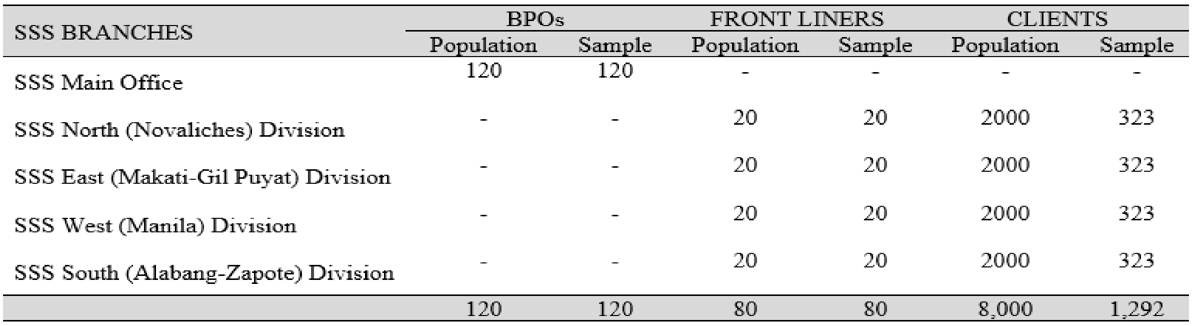
Research Design

The study employed a descriptive-correlational research design. Descriptive research is employed to gather information on the present state of a phenomenon, in order to describe "what exists" and "what is happening" in relation to variables or conditions within a given situation. The objective of descriptive research is to provide a detailed description of the necessary variables. The benefit of this is that it offers a relatively comprehensive overview of the current events at a specific moment. It facilitates the formulation of inquiries for subsequent investigation. Correlational study aims to identify correlations between variables and enable the prediction of future events based on current information. It quantifies two or more variables in their inherent state.

The objective is to ascertain the presence of a correlation between variables. The main benefit of this approach is that it enables the examination of anticipated connections between variables and the ability to make predictions. Furthermore, it has the capability to evaluate these connections in ordinary occurrences. One drawback of this method is that it cannot be utilized to make conclusions regarding the cause-and-effect linkages between the variables.

Respondents of the Study

The study was conducted to evaluate the digitization of services in the Social Security System. Three groups of respondents – BPO, front liners, clients - were used to answer the survey questionnaire developed by the researcher. To validate the responses of the three groups of respondents in the questionnaire, the five managers of the five branches of the SSS were interviewed.



SSS BRANCHES	BPOs		FRONT LINERS		CLIENTS	
	Population	Sample	Population	Sample	Population	Sample
SSS Main Office	120	120	-	-	-	-
SSS North (Novaliches) Division	-	-	20	20	2000	323
SSS East (Makati-Gil Puyat) Division	-	-	20	20	2000	323
SSS West (Manila) Division	-	-	20	20	2000	323
SSS South (Alabang-Zapote) Division	-	-	20	20	2000	323
	120	120	80	80	8,000	1,292

***Total Number of Population (BPO's)**
***Result of Raosoft formula**

The Business Process Owners (BPO) are from the Head Office and are in charge of policy making in the digitalization of SSS services. They are from Member Electronic Services Department, Member Loans Department, Business and Development Loans Department, Sickness Maternity and Disability Department, Pensions Administration Department, and Retirement Death and Funeral Benefits Administration Department. For the front liners, they were taken from the biggest branch from each of the four districts of Metro Manila (North, East, West, and South). They are in charge of the operation of the digital services of the SSS like online member registration and updates, online loans and benefits application, and member assistance. For the clients, they were taken from the biggest branch from each of the four districts of Metro Manila (North, East, West, and South). They are the members and non-members of the Philippine Social Security System who are the primary users of the SSS online services.

Research Instrument

This researcher used self-made questionnaire and interview guide question as instruments of the study. The questionnaire consisted of four parts: first, for the profile; the second, for the evaluation of the digitization; third for the difficulties encountered; and fourth, for the solutions employed. These two instruments were validated by the investigator of the Special Investigation Department, Manager in the Cybercrime Investigation, and head of the Branch Systems and Procedures Department.

Population and Sampling Technique

As the study used 3 groups of respondents – BPO, front liners, clients, and Managers - two sampling techniques were utilized. For the BPOs taken from the Head Office, complete enumeration was utilized. For the front liners taken from the biggest branch from each of the four districts, complete enumeration, likewise, was used. It must be noted that for BPOs and front-liners, there is a guideline that dictates the number of personnel to be employed.

And for the clients taken from the biggest branch from each of the four districts of Metro Manila, three hundred thirty-two (323) clients were computed through the use of Raosoft formula with accepted margin of error of 5% and

95% confidence level from an approximately 2,000 (two thousand) clients per day in each of the biggest branch from each of the four districts of Metro Manila. After which, convenience sampling was used.

Complete counts are complete enumeration or census of individuals within a sampling unit. It is same as total enumeration sampling, which is a type of purposive sampling technique where the researcher chooses to examine the entire population that has a particular set of characteristics.

Data Gathering Procedure

First, the researcher secured approval/permission from the Dean of the College of Criminal Justice Education-Graduate Studies and personnel of the Social Security System in the Head Office to conduct the study.

Second, the researcher complied with all the requirements set by the Institutional Ethics Review Committee (IERC) of De La Salle University - Dasmariñas - edited research proposal, informed consent form, and the tools to be used (interview guide questions and self-made questionnaire) - as mandatory requirements to gain ethics approval.The researcher waited for the approval of the Ethics Committee before he moved on to data gathering. He then floated and retrieved the instruments personally and by via on-line because of the present pandemic. Once he had retrieved the data, he gave it to his Statistician for treatment. After that, he interpreted and analyzed to come up with the findings, conclusions, and recommendations.

Statistical Treatment of Data

The following statistical tolls were used in the treatment of data:

1. **Weighted Mean.** Average weighted mean (AWM) was used to determine the central tendency in relation to the investigation of the respondents on issues being discussed in the study. Average weighted mean refers to the accumulated responses which determine the corresponding weight using the formula.
2. **Mean Ranges, Verbal Interpretation, and Verbal Description.** The researcher utilized four-point rating scale.
3. **One-Way ANOVA**. A one-way ANOVA (Analysis of Variance) compares the means of three or more independent groups to determine if there is a statistically significant difference between the corresponding population means (Zach, 2018).

One-Way ANOVA: The Process

A one-way ANOVA uses the following null and alternative hypotheses:

H0 (null hypothesis): μ1 = μ2 = μ3 = … = μk (all the population means are equal)
H1 (alternative hypothesis): at least one population mean is different from the rest.

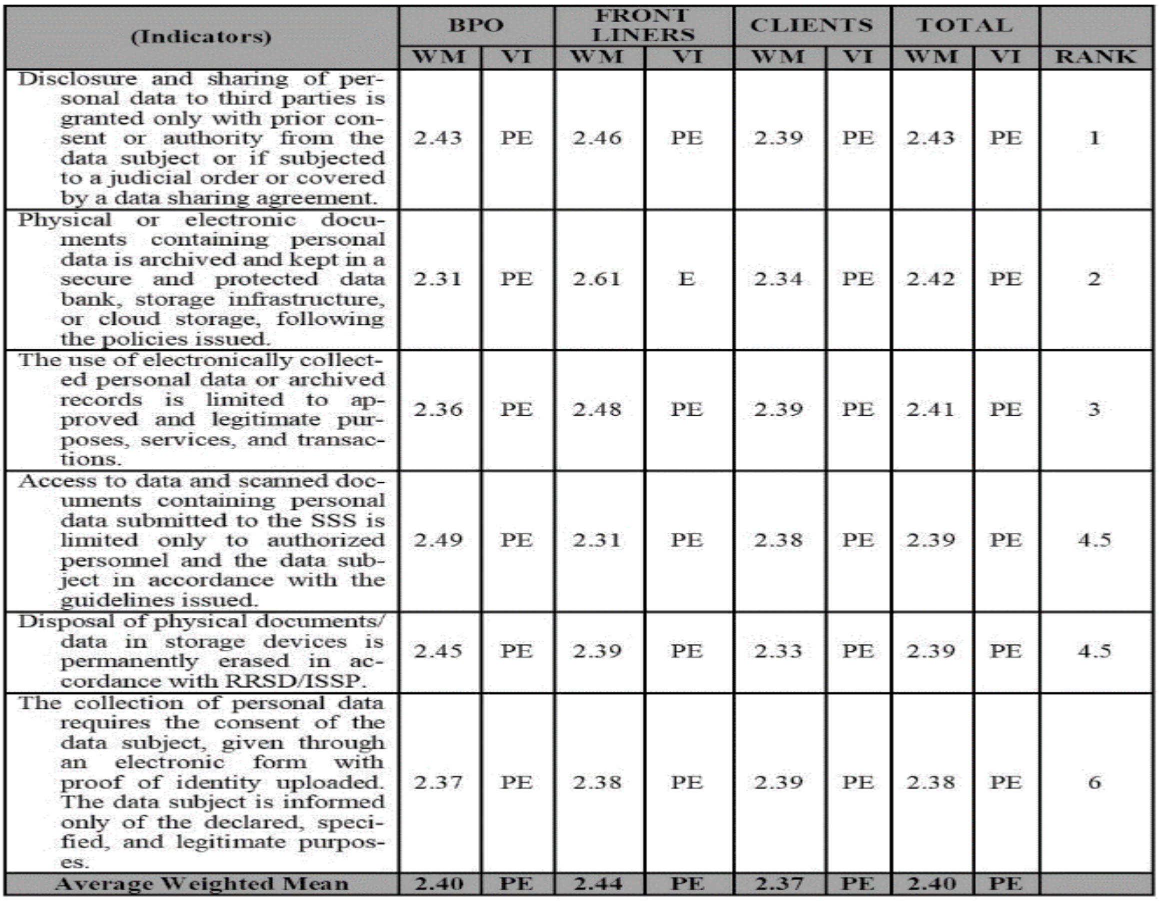
Result and Discussion

This part presents the interpretation and analysis of data gathered through the use of questionnaire and interview. The presentation is done based on how the questions are arranged in the Statement of the Problem.

Problem 2: Respondents' evaluation on the digitization of services

Table 1 displays the respondents' assessment of the digitization of services in the Philippine Social Security System, specifically regarding the handling of personal data. The ratings received resulted in an overall mean of 2.40, which is interpreted as Partially Efficient. This demonstrates that the Philippine Social Security System has partially implemented the digitization of services, with a focus on safeguarding personal data. Only authorized people and Data Subjects are allowed to access data and scanned documents. Personal data is obtained via electronic forms that necessitate verification of identification and is exclusively utilized for lawful intentions. Personal data is meticulously stored and protected in secure data banks or cloud storage, encompassing both physical and electronic documents.

Table 1. Respondents' Evaluation as to the Digitization of Services in the Philippine Social Security System in terms of Processing of Personal Data



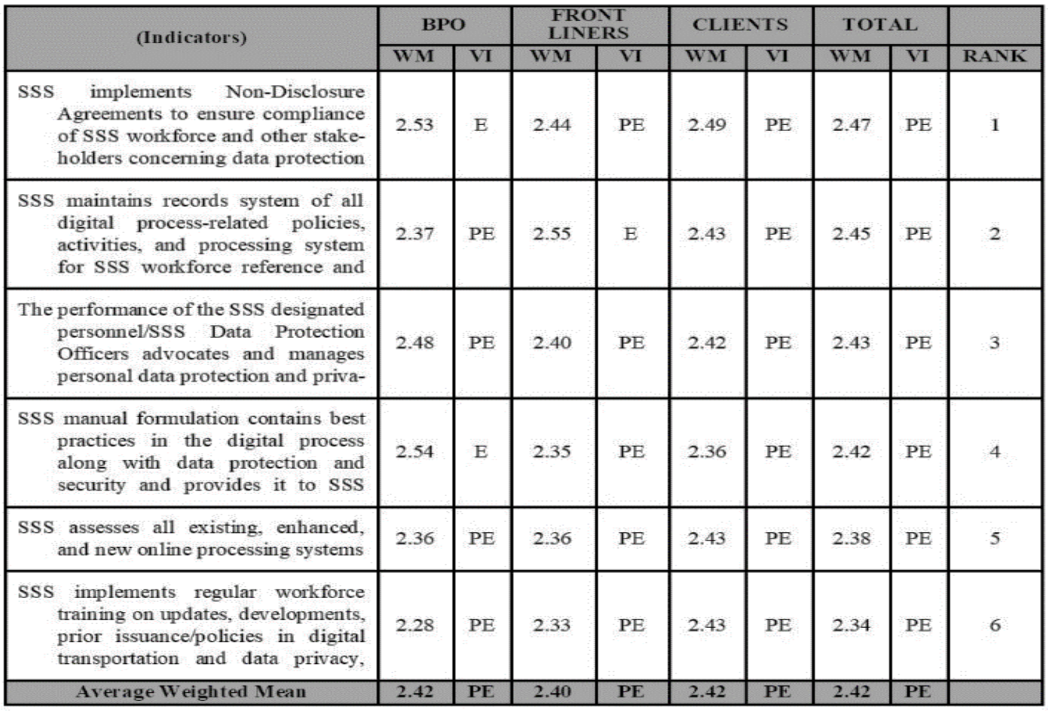
(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
Disclosure and sharing of personal data to third parties is granted only with prior consent or authority from the data subject or if subjected to a judicial order or covered by a data sharing agreement.	2.43	PE	2.46	PE	2.39	PE	2.43	PE	1
Physical or electronic documents containing personal data is archived and kept in a secure and protected data bank, storage infrastructure, or cloud storage, following the policies issued.	2.31	PE	2.61	E	2.34	PE	2.42	PE	2
The use of electronically collected personal data or archived records is limited to approved and legitimate purposes, services, and transactions.	2.36	PE	2.48	PE	2.39	PE	2.41	PE	3
Access to data and scanned documents containing personal data submitted to the SSS is limited only to authorized personnel and the data subject in accordance with the guidelines issued.	2.49	PE	2.31	PE	2.38	PE	2.39	PE	4.5
Disposal of physical documents/ data in storage devices is permanently erased in accordance with RRSD/ISSP.	2.45	PE	2.39	PE	2.33	PE	2.39	PE	4.5
The collection of personal data requires the consent of the data subject, given through an electronic form with proof of identity uploaded. The data subject is informed only of the declared, specified, and legitimate purposes.	2.37	PE	2.38	PE	2.39	PE	2.38	PE	6
Average Weighted Mean	2.40	PE	2.44	PE	2.37	PE	2.40	PE	

It must be noted that under the law RA 10173, otherwise known as the Data Privacy Act of 2012, not all data are covered by the Data Privacy Act. The law does NOT apply to the following: a. Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including: (1) The fact that the individual is or was an officer or employee of the government institution, (2) The title, business address, and office telephone number of the individual, (3) The classification, salary range, and responsibilities of the position held by the individual, and (4) The name of the individual on a document prepared by the individual in the course of employment with the government; b. Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services; c. Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit; d. Personal information processed for journalistic, artistic, literary or research purposes; d. Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority, and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA); e. Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and f. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Table 2 presents the respondents' evaluation as to the digitization of services in the Philippine Social Security System in terms of organizational measure. An overall mean of 2.42 was obtained interpreted as Partially Efficient. It simply means that SSS, at least, has adeptly incorporated digital services into their operations with a strategic approach.

The organization has taken decisive action to safeguard data privacy and security, including the implementation of digital non-disclosure agreements, the creation of comprehensive manuals outlining best practices, and the appointment of dedicated Data Protection Officers.

Table 2. Respondents' Evaluation of the in the Digitization of Services in the Philippine Social Security System in terms of Organizational Measure



(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
SSS implements Non-Disclosure Agreements to ensure compliance of SSS workforce and other stakeholders concerning data protection	2.53	E	2.44	PE	2.49	PE	2.47	PE	1
SSS maintains records system of all digital process-related policies, activities, and processing system for SSS workforce reference and	2.37	PE	2.55	E	2.43	PE	2.45	PE	2
The performance of the SSS designated personnel/SSS Data Protection Officers advocates and manages personal data protection and priva-	2.48	PE	2.40	PE	2.42	PE	2.43	PE	3
SSS manual formulation contains best practices in the digital process along with data protection and security and provides it to SSS	2.54	E	2.35	PE	2.36	PE	2.42	PE	4
SSS assesses all existing, enhanced, and new online processing systems	2.36	PE	2.36	PE	2.43	PE	2.38	PE	5
SSS implements regular workforce training on updates, developments, prior issuance/policies in digital transportation and data privacy,	2.28	PE	2.33	PE	2.43	PE	2.34	PE	6
Average Weighted Mean	2.42	PE	2.40	PE	2.42	PE	2.42	PE	

Furthermore, the SSS maintains meticulous record-keeping systems and regularly conducts evaluations and educational initiatives to ensure the protection of all sensitive information.

The Social Security System (SSS) and its stakeholders emphasize upholding the highest standards of integrity and work ethics while ensuring strict compliance with the Data Privacy law on both traditional and digital platforms.

In pursuit of this objective, the SSS and its stakeholders implement measures to safeguard the confidentiality, integrity, and availability of personal data, thereby promoting trust and confidence in the system.

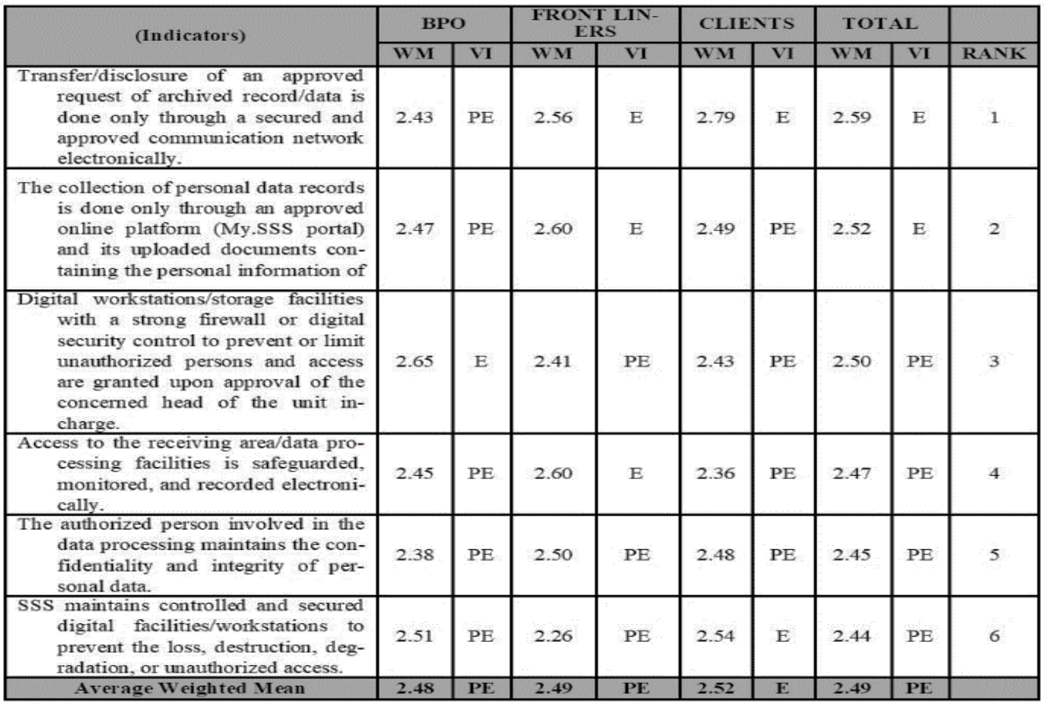
This commitment to ethical practices is essential to the SSS's core values, reflected in the organization's culture, policies, and processes.

To further the discussions on the preceding paragraphs, Šidlauskas (2021) notes that organization must ensure and demonstrate compliance with all the principles of the General Data Protection Regulation, and the appointment of a Data Protection Officer can be one of the measures required to implement the principle of accountability.

According to the General Data Protection Regulation (GDPR), non-compliant companies may face ones of up to 20 million euros or 4% of worldwide turnover and damage claims from violations. Companies stand to lose revenue, as well as endure reputational damage should they breach the GDPR.

The Data Protection Officer must make sure that the organization complies with the GDPR and prevent any infringement on its provisions.

Table 3. Respondents' Evaluation as to the Digitization of Services in the Philippine Social Security Svstem in terms of Phvsical Measure



(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
Transfer/disclosure of an approved request of archived record/data is done only through a secured and approved communication network electronically.	2.43	PE	2.56	E	2.79	E	2.59	E	1
The collection of personal data records is done only through an approved online platform (My.SSS portal) and its uploaded documents containing the personal information of	2.47	PE	2.60	E	2.49	PE	2.52	E	2
Digital workstations/storage facilities with a strong firewall or digital security control to prevent or limit unauthorized persons and access are granted upon approval of the concerned head of the unit in-charge.	2.65	E	2.41	PE	2.43	PE	2.50	PE	3
Access to the receiving area/data processing facilities is safeguarded, monitored, and recorded electronically.	2.45	PE	2.60	E	2.36	PE	2.47	PE	4
The authorized person involved in the data processing maintains the confidentiality and integrity of personal data.	2.38	PE	2.50	PE	2.48	PE	2.45	PE	5
SSS maintains controlled and secured digital facilities/workstations to prevent the loss, destruction, degradation, or unauthorized access.	2.51	PE	2.26	PE	2.54	E	2.44	PE	6
Average Weighted Mean	**2.48**	**PE**	**2.49**	**PE**	**2.52**	**E**	**2.49**	**PE**	

Table 3 presents respondents' evaluation in the digitization of services in the Philippine Social Security System in terms of physical measure.

Based on the scores, an overall Weighted Mean of 2.49 interpreted as Partially Efficient was obtained. This still simply means that SSS relies on digital services with physical measures to ensure data security. The transfer and disclosure of approved archived records and data requests is done only through a secure and authorized communication network. Access to data processing facilities is monitored and recorded electronically. Digital workstations and storage facilities have strong firewalls or digital security controls to prevent unauthorized access, which can only be granted upon approval of the head of the unit in charge.

Personal data records are collected exclusively through the My.SSS portal and uploaded documents. The SSS maintains secured digital facilities to prevent unauthorized access and data loss**.**

In relation to this, Gluck (2023) said that as to physical access security, the Data Center Management (DCM) team must implement operational procedures to restrict physical access to only authorized employees, contractors, and visitors. Temporary or permanent access requests must be tracked using a ticketing system. Badges should either be issued or activated for personnel requiring access after identification verification. Physical keys and temporary access badges must be secured within the security operations center (SOC).

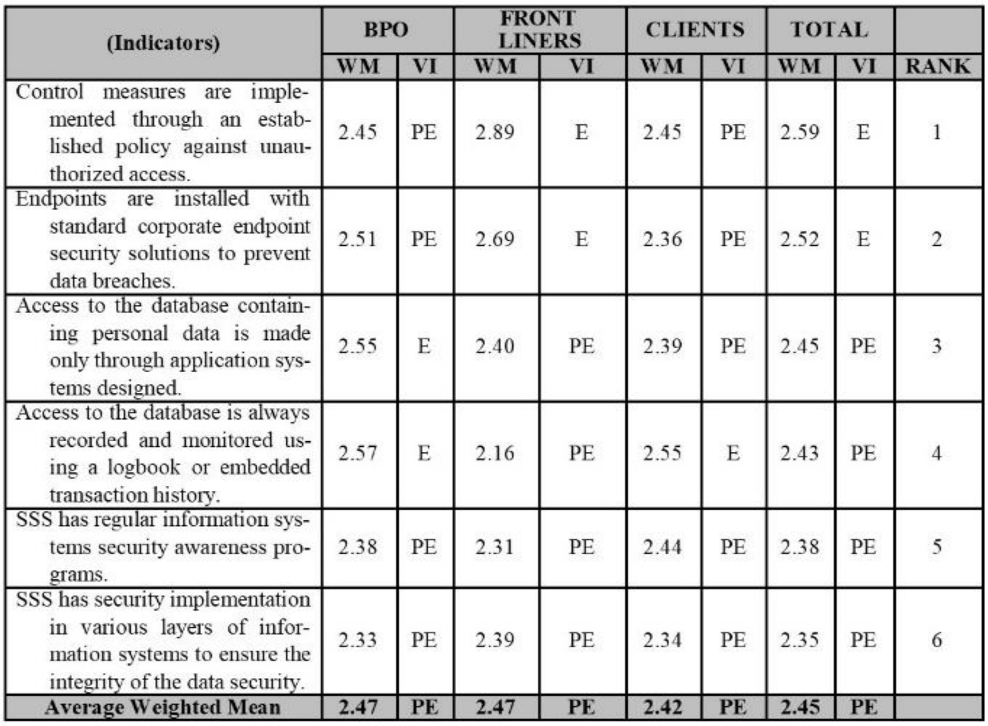
To further support the above discussions, according to the General Data Protection Regulation, all organizations are required to implement physical measures to ensure data security. This includes providing access to premises while maintaining data security. Examples of such measures include installing intruder alarms with access verification, categorizing different areas of buildings based on risk levels (such as server rooms), physically protecting IT equipment, and installing locks in each office.

Table 4 presents the respondents' evaluation on the digitization of services in the Philippine Social Security System in terms of technical measure. Based on the scores, an overall Weighted Mean of 2.45 interpreted as Partially Efficient was obtained.

Although only partially efficient, this still simply means that SSS employs physical measures to the highest level to provide digital services.

Only approved archived records and data requests are disclosed through secure channels. Access to data processing facilities is strictly monitored and recorded. Personnel prioritize the confidentiality and integrity of personal data.

Table 4. Respondents' Evaluation as to the Digitization of Services in the Philippine Social Security System in terms of Technical Measure



(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
Control measures are implemented through an established policy against unauthorized access.	2.45	PE	2.89	E	2.45	PE	2.59	E	1
Endpoints are installed with standard corporate endpoint security solutions to prevent data breaches.	2.51	PE	2.69	E	2.36	PE	2.52	E	2
Access to the database containing personal data is made only through application systems designed.	2.55	E	2.40	PE	2.39	PE	2.45	PE	3
Access to the database is always recorded and monitored using a logbook or embedded transaction history.	2.57	E	2.16	PE	2.55	E	2.43	PE	4
SSS has regular information systems security awareness programs.	2.38	PE	2.31	PE	2.44	PE	2.38	PE	5
SSS has security implementation in various layers of information systems to ensure the integrity of the data security.	2.33	PE	2.39	PE	2.34	PE	2.35	PE	6
Average Weighted Mean	**2.47**	**PE**	**2.47**	**PE**	**2.42**	**PE**	**2.45**	**PE**	

Digital workstations are equipped with robust security controls. Personal data records are collected exclusively through the My.SSS portal and digital facilities are fortified to prevent any unauthorized access.

According to the study entitled "Information System Monitoring Access Log Database on Database Server" by Setiyadi & Setiawan (2018), to generate information system log database access activity on a database server, the system activity of the database access log on the database server can already prepare the track record/log data of each user accessing the database on the server. The system built in this research is still focused on the My.SSS database.

This is because the use of My.SSS for current database is still high. However, the concept of the method offered can also be done for other types of databases that will ultimately increase the security level of a database.

Supporting the preceding discussion, according to International Business Machines

(IBM), data security solutions must be effectively implemented to safeguard an organization's information assets from cybercriminal actions.

To address the risks posed by insider threats and human mistake, which continues to be major contributors to data breaches in the present day, data security must entail implementing methods and technology that improve the organization's ability to monitor the whereabouts and utilization of its vital data.

These tools should ideally possess the capability to implement safeguards such as encryption, data masking, and redaction of sensitive files.

Additionally, they should automate the process of generating reports to speed audits and ensure compliance with regulatory standards.

Problem 3: Test of significant difference

Table 5. Test of Significant Difference in the Evaluation among the Three Groups Respondents in terms of Processing of Personal Data

Group	Mean	Standard Deviation	F-ratio	p-value	Interpretation
BPO	2.4017	0.0665	1.31767	0.297703	Not Significant
Frontline	2.4383	0.1038			
Clients	2.37	0.0276			

The comparison analysis using One-Way ANOVA reveals that the computed F-ratio is 1.32 with p-value of 0.30. Since the p-value is greater than 0.05, the null hypothesis is not rejected.

This means that the three groups of respondents were the same in their evaluation regarding the digitization of services in SSS; hence, there is no significant difference.

Obviously, all the three groups had similar opinions about how well SSS uses technology to process people's personal data. There wasn't any significant difference between their responses.

They all believe that owner's approval must be given and adequately documented to ensure people's data is collected legally. This can be done through a safe and secure digital platform.

In relation to the preceding discussions, the study, entitled “Consent as a Basis of Processing Personal Data on the Internet of Things by Elevant” (2021), found that protection of individuals in relation to the processing of personal data is a fundamental right.

Therefore, in accordance with the General Data Protection Regulation (GDPR), a European regulation on information privacy, processing of personal data is allowed only under a number of legal bases and one of which is consent. In order for consent to be valid, it must be freely given, specific, unambiguous.

Table 6. Test of Significant Difference in the Evaluation among the Three Groups Respondents in terms of Organizational Measure

Group	Mean	Standard Deviation	F-ratio	p-value	Interpretation
BPO	2.4267	0.1054	0.1161	0.89117	Not Significant
Frontline	2.405	0.0812			
Clients	2.4183	0.0293			

The comparison analysis using One-Way ANOVA reveals that the computed F-ratio is 0.12 with p-value of 0.89. Since the p-value is greater than 0.05, the null hypothesis is not rejected. This means that the three groups of respondents were the same in their evaluation of the digitization of services in SSS; hence, there is no significant difference.

With this, it simply means that the three groups of respondents unanimously look at how SSS uses technology to provide services, agreeing that there is not much difference between them.

So, SSS must make sure that people's personal information is kept safe and mist employ people who could be 100% responsible for protecting data and for making sure the system runs smoothly. These people are called data protection officers and assistant data protection officers.

In relation to the preceding discussions, the study, entitled "The Role and Significance of the Data Protection Officer in the Organization" by Šidlauskas (2021) notes that organization must ensure and demonstrate compliance with all the principles of the General Data Protection Regulation, and the appointment of a DPO can be one of the measures required to implement the principle of accountability.

According to the GDPR, non-compliant companies may face ones of up to 20 million euros or 4% of worldwide turnover and damage claims from violations. Companies stand to lose revenue, as well as endure reputational damage should they breach the GDPR. The DPO must make sure that the organization complies with the GDPR and prevent any infringement on its provisions.

Table 7. Test of Significant Difference in the Evaluation among the Three Groups Respondents in terms of Physical Measure

Group	Mean	Standard Deviation	F-ratio	p-value	Interpretation
BPO	2.4817	0.093	0.11607	0.8912	Not Significant
Frontline	2.4883	0.133			
Clients	2.515	0.1479			

The comparison analysis using One-Way ANOVA reveals that the computed F-ratio is 0.12 with p-value of 0.89. Since the p-value is greater than 0.05, the null hypothesis is not rejected.

This means that the three groups of respondents were the same in their evaluation on the digitization of services in SSS; hence, there is no significant difference.

With that, it simply implies that the three groups of respondents provided an equivalent evaluation of the digitization of services in SSS, as measured by physical means. Notably, there exists no considerable difference in their evaluations. It is pertinent to mention that the data collection from clients is an exclusively authorized activity, and only personnel who have been authorized are permitted to undertake this task.

Furthermore, the names of these authorized personnel are made public in the SSS area where data collection takes place.

In relation to the above discussions, according to the General Data Protection Regulation, all organizations are required to implement physical measures to ensure data security. This includes providing access to premises while maintaining data security.

Examples of such measures include installing intruder alarms with access verification, categorizing different areas of buildings based on risk levels (such as server rooms), physically protecting IT equipment, and installing locks in each office.

Table 8. Test of Significant Difference in the Evaluation among the Three Groups Respondents in terms of Technical Measure

Group	Mean	Standard Deviation	F-ratio	p-value	Interpretation
BPO	2.465	0.0959	0.15962	0.8539	Not Significant
Frontline	2.4733	0.2675			
Clients	2.4217	0.0763			

The comparison analysis using One-Way ANOVA reveals that the computed F-ratio is 0.16 with p-value of 0.85. Since the p-value is greater than 0.05, the null hypothesis is not rejected. This means that the three groups of respondents were the same in their evaluation of the digitization of services in SSS; hence, there is no significant difference.

With that, it means that the survey results indicate that all three groups of respondents share the same perspective on the technical aspect of digitized services in SSS. The evaluations do not show any significant differences. To ensure data privacy and security, a layer of protection is implemented in the SSS data system access, which is determined by the Data Protection Officer.

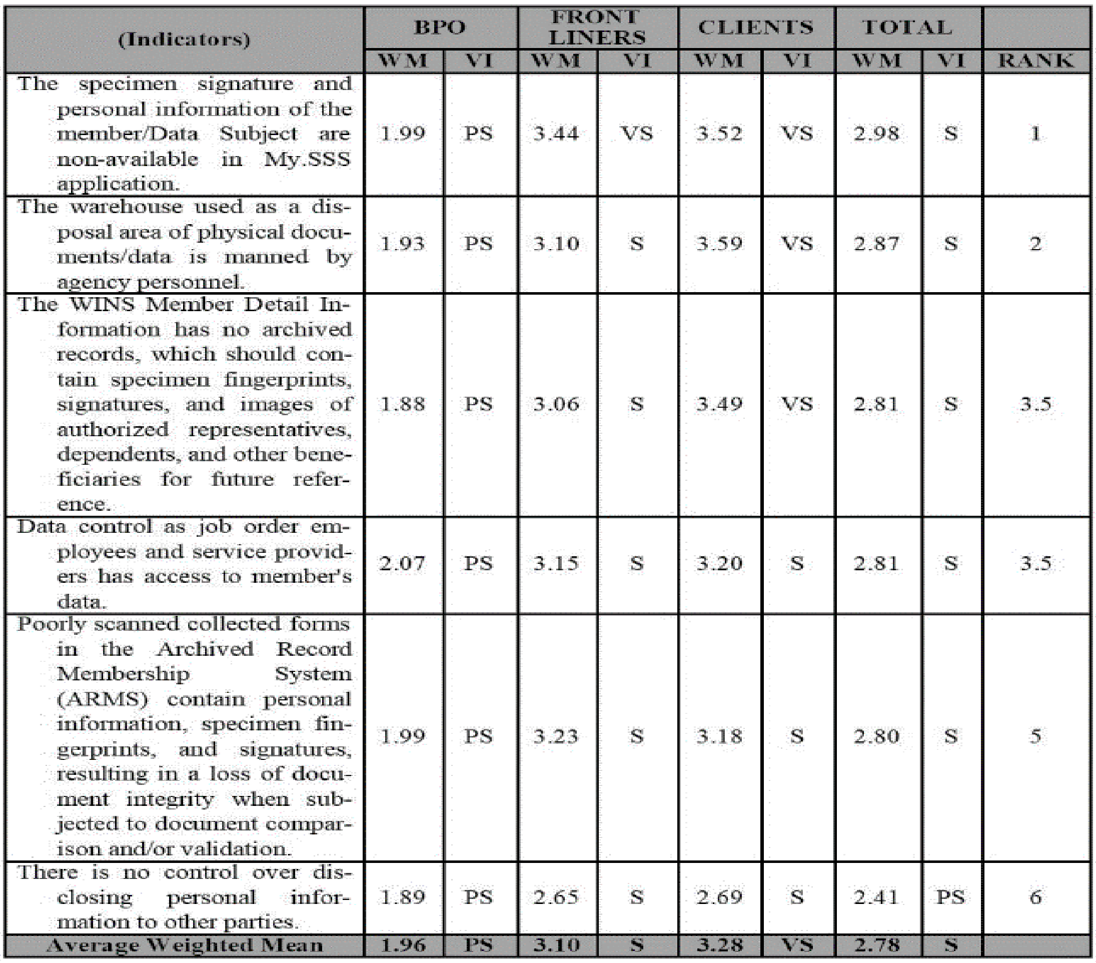
Supporting the previous discussion, according to International Business Machines (IBM), data security solutions must be effectively implemented to safeguard an organization's information assets from cybercriminal actions.

To address the risks posed by insider threats and human mistake, which continues to be major contributors to data breaches in the present day, data security must entail implementing methods and technology that improve the organization's ability to monitor the whereabouts and utilization of its vital data. These tools should ideally possess the capability to implement safeguards such as encryption, data masking, and redaction of sensitive files.

Additionally, they should automate the process of generating reports to speed audits and ensure compliance with regulatory standards.

Problem 4: Difficulties encountered in the digitization of services

Table 9. Respondents' Evaluation as to the Difficulties in the Digital Services of the Philippine Social Security System in terms of Processing of Personal Data



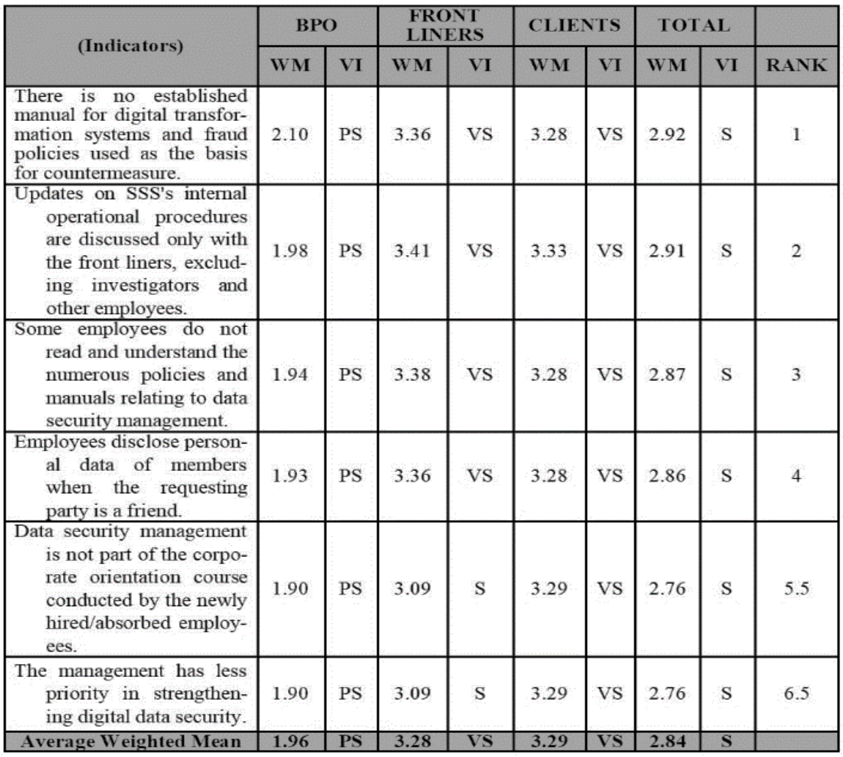
(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
The specimen signature and personal information of the member/Data Subject are non-available in My.SSS application.	1.99	PS	3.44	VS	3.52	VS	2.98	S	1
The warehouse used as a disposal area of physical documents/data is manned by agency personnel.	1.93	PS	3.10	S	3.59	VS	2.87	S	2
The WINS Member Detail Information has no archived records, which should contain specimen fingerprints, signatures, and images of authorized representatives, dependents, and other beneficiaries for future reference.	1.88	PS	3.06	S	3.49	VS	2.81	S	3.5
Data control as job order employees and service providers has access to member's data.	2.07	PS	3.15	S	3.20	S	2.81	S	3.5
Poorly scanned collected forms in the Archived Record Membership System (ARMS) contain personal information, specimen fingerprints, and signatures, resulting in a loss of document integrity when subjected to document comparison and/or validation.	1.99	PS	3.23	S	3.18	S	2.80	S	5
There is no control over disclosing personal information to other parties.	1.89	PS	2.65	S	2.69	S	2.41	PS	6
Average Weighted Mean	1.96	PS	3.10	S	3.28	VS	2.78	S	

Table 9 presents the respondents' evaluation as to the difficulties encountered in the digitization of services in the Philippine Social Security System in terms of processing of personal data.

Based on the scores, an overall Weighted Mean of 2.78 interpreted as Serious was obtained. This means that although SSS employs digital services to process personal data, still, there is lack of control when it comes to disclosing of personal information. Physical document disposal is carried out in warehouses which are manned by agency personnel. However, the WINS Member Detail Information lacks archived records, such as fingerprints and signatures of authorized representatives, dependents, and other beneficiaries. Job order employees and service providers have access to members' data, which can lead to data control issues. Poorly scanned forms in the Archived Record Membership System (ARMS) containing personal information, fingerprints, and signatures can cause document integrity loss. Likewise, the specimen signature and personal information of the member or data subject are not available online.

According to the Organization for Economic Co-operation and Development (OECD), (2019), lack of common approaches and rules for sharing data across countries, particularly personal and other confidential data, has limited cross-border data access and sharing. This remains an issue despite the wide recognition of the need for international arrangements and legal interoperability as articulated in the Principle on International access and use of the OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information (hereafter the OECD PSI Recommendation) (OECD, 2008). The principle calls for seeking greater consistency in access regimes and administration to facilitate cross-border use and implementing other measures to improve cross-border interoperability, including when there have been restrictions on non-public users.

Table 10. Respondents' Evaluation as to the Difficulties in the Digital Services of the Philippine Social Security System in terms of Organizational Measure



(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
There is no established manual for digital transformation systems and fraud policies used as the basis for countermeasure.	2.10	PS	3.36	VS	3.28	VS	2.92	S	1
Updates on SSS's internal operational procedures are discussed only with the front liners, excluding investigators and other employees.	1.98	PS	3.41	VS	3.33	VS	2.91	S	2
Some employees do not read and understand the numerous policies and manuals relating to data security management.	1.94	PS	3.38	VS	3.28	VS	2.87	S	3
Employees disclose personal data of members when the requesting party is a friend.	1.93	PS	3.36	VS	3.28	VS	2.86	S	4
Data security management is not part of the corporate orientation course conducted by the newly hired/absorbed employees.	1.90	PS	3.09	S	3.29	VS	2.76	S	5.5
The management has less priority in strengthening digital data security.	1.90	PS	3.09	S	3.29	VS	2.76	S	6.5
Average Weighted Mean	**1.96**	**PS**	**3.28**	**VS**	**3.29**	**VS**	**2.84**	**S**	

Table 10 presents the respondents' evaluation on the difficulties encountered in the digitization of services in the Philippine Social Security System in terms of organizational measure. Based on the scores, an overall Weighted Mean of 2.84 interpreted as Serious was obtained. This simply means that Philippine Social Security System's digital services have not met satisfactory standards. There are lack of emphasis on data security management, absence of manuals for digital transformation systems or fraud policies, and insufficient awareness among employees regarding data security policies. The management appears to have little regard for digital data security, and internal procedural updates are not communicated to investigators and other personnel. It is crucial to take necessary measures to address these issues and guarantee the safety of users.

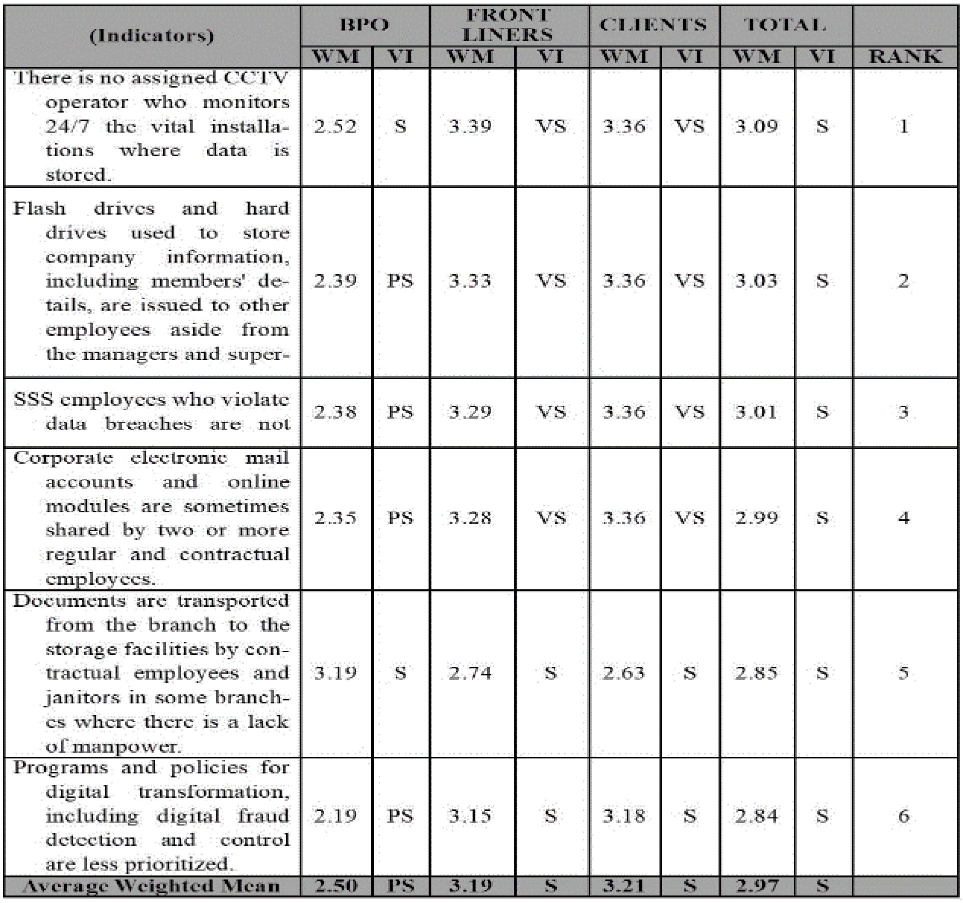
According to Sbriz (2021), in organizations, the topic of enterprise risk management presents a twofold problem: the calculation of the level of risk and effective communication to top management. An accurate risk evaluation loses all its effectiveness if it is not properly understood by managerial executives with decision-making power. For effective communication, it is necessary to accurately represent the situation, connecting the business processes well known to top managers with their most significant threats. Knowing how to describe information security risk to top management efficiently is essential to aid decision-making and ensure an organization is secure. Once the risk is communicated, mitigation proposals can be further examined, detailed, and discussed.

Table 11 presents the respondents' evaluation on the difficulties encountered in the digitization of services in the Philippine Social Security System in terms of physical measure.

Based on the scores, an overall mean of 2.97 interpreted as Serious was obtained. This simply means that in the digitization of Philippine Social Security system, there are security risks associated with it. There is no dedicated CCTV operator. Sharing of electronic accounts and using of flash drives that can pose threats to the security of the system are sometimes present.

The implementation of digital transformation programs and policies to detect fraud has not been prioritized adequately.

Table 11. Respondents' Evaluation as to the Difficulties in the Digital Services of the Philippine Social Security System in terms of Physical Measure



(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
There is no assigned CCTV operator who monitors 24/7 the vital installations where data is stored.	2.52	S	3.39	VS	3.36	VS	3.09	S	1
Flash drives and hard drives used to store company information, including members' details, are issued to other employees aside from the managers and super-	2.39	PS	3.33	VS	3.36	VS	3.03	S	2
SSS employees who violate data breaches are not	2.38	PS	3.29	VS	3.36	VS	3.01	S	3
Corporate electronic mail accounts and online modules are sometimes shared by two or more regular and contractual employees.	2.35	PS	3.28	VS	3.36	VS	2.99	S	4
Documents are transported from the branch to the storage facilities by contractual employees and janitors in some branches where there is a lack of manpower.	3.19	S	2.74	S	2.63	S	2.85	S	5
Programs and policies for digital transformation, including digital fraud detection and control are less prioritized.	2.19	PS	3.15	S	3.18	S	2.84	S	6
Average Weighted Mean	2.50	PS	3.19	S	3.21	S	2.97	S	

Furthermore, some branches experience lack of manpower, and documents are transported by contractual employees and janitors, which can also lead to security risks.

According to Southekal (2022), the amount of data generated by businesses today is unprecedented. As this growth of data continues, so do the opportunities for organizations to derive value from data.

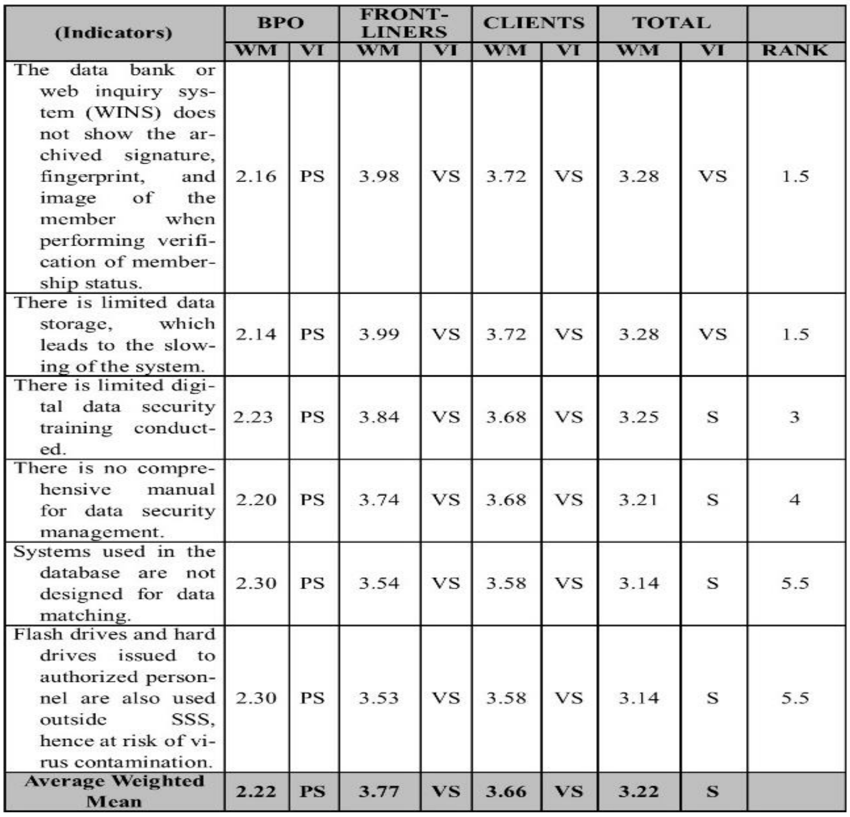
A report from MIT says that digitally mature firms are 26% more profitable than their peers. The McKinsey Global Institute indicates that data-driven organizations are 23 times more likely to acquire customers and 19 times more profitable than peers. But deriving value from data is an evolutionary process, just like the business itself. The needs of businesses constantly change; organizational capabilities continuously mature; data sets grow, improve, and sometimes even degrade; and the technological capabilities to capture, store, and process the data improve over time.

The DX programs and the MDM solutions, if managed well by applying the above three rules, can play a pivotal role in managing change and improving business performance.

Table 12 presents the respondents' evaluation on the difficulties encountered in the digitization of services in the Philippine Social Security System in terms of technical measure. Based on the scores, an overall Weighted Mean of 3.22 marked as Serious was obtained. This only goes to show that the Philippine Social Security System faces significant technical challenges in its digitization of services that require immediate attention. The current system lacks adequate data storage, digital data security training, and comprehensive manuals for data security management. Moreover, the database systems used are not designed for data matching, and the data bank or web inquiry system does not display archived signatures, fingerprints, and images of members.

Additionally, flash drives and hard drives provided to authorized personnel can be used outside of SSS, leaving them vulnerable to virus contamination. It is imperative to take prompt and decisive action to resolve these issues and ensure the efficient operation of the system.

Table 12. Respondents' Evaluation as to the Difficulties in the Digital Services of the Philippine Social Security System in terms of Technical Measures



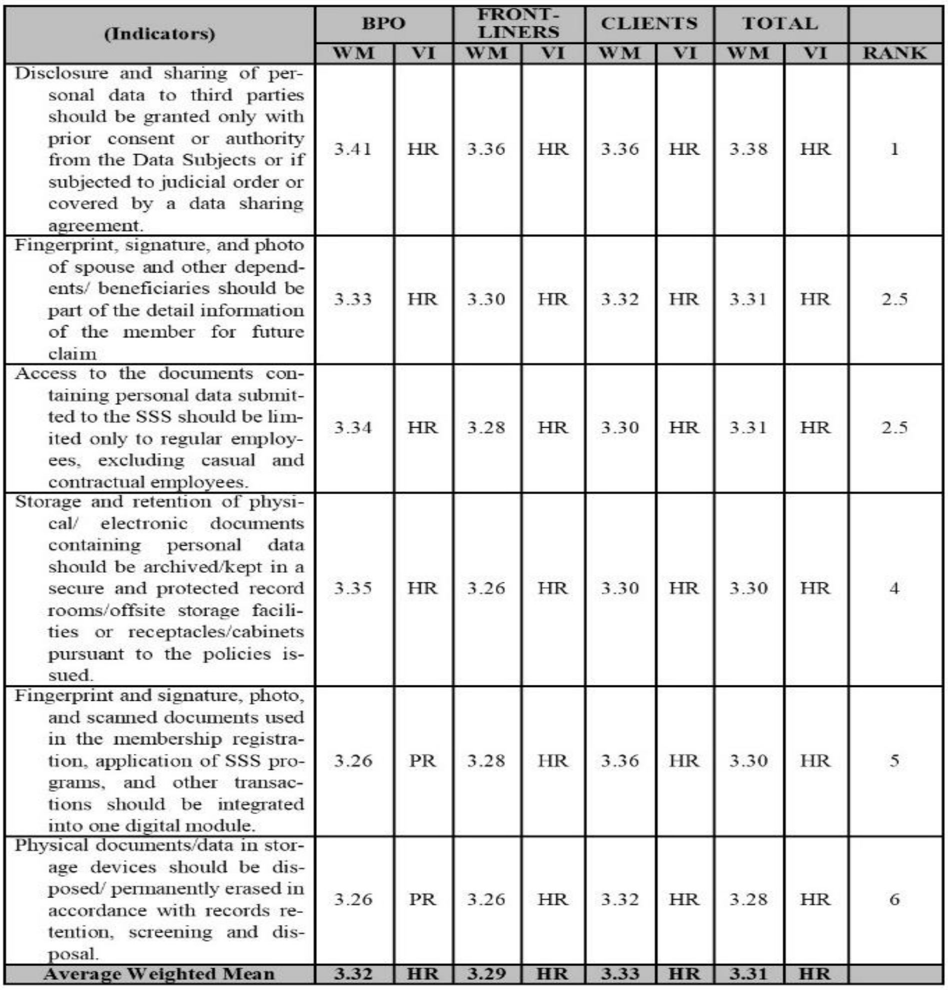
(Indicators)	BPO		FRONT-LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
The data bank or web inquiry system (WINS) does not show the archived signature, fingerprint, and image of the member when performing verification of membership status.	2.16	PS	3.98	VS	3.72	VS	3.28	VS	1.5
There is limited data storage, which leads to the slowing of the system.	2.14	PS	3.99	VS	3.72	VS	3.28	VS	1.5
There is limited digital data security training conducted.	2.23	PS	3.84	VS	3.68	VS	3.25	S	3
There is no comprehensive manual for data security management.	2.20	PS	3.74	VS	3.68	VS	3.21	S	4
Systems used in the database are not designed for data matching.	2.30	PS	3.54	VS	3.58	VS	3.14	S	5.5
Flash drives and hard drives issued to authorized personnel are also used outside SSS, hence at risk of virus contamination.	2.30	PS	3.53	VS	3.58	VS	3.14	S	5.5
Average Weighted Mean	**2.22**	**PS**	**3.77**	**VS**	**3.66**	**VS**	**3.22**	**S**	

According to Belanger (2022), many companies expose themselves to many security threats since their USB security programs lack adequate measures to ensure data security. In a recent survey, it was found that approximately 58% of organizations lack safe listing and USB port control software for managing flash drive usage. The same survey found that only 47% of businesses require their employees to encrypt data stored in USB drives. Furthermore, 53% of companies lack appropriate controls for detecting and preventing users from downloading sensitive data onto unauthorized USB devices.

While at least 90% of employees worldwide use USB devices for work-related reasons, it is worrying that more than half of companies do not allow flash drives or use USB port controls to manage USB connections or encrypt data stored in flash drives.

Problem 5: Counter measures to the difficulties encountered

Table 13. Respondents' Evaluation as to the Counter Measures to Address the Difficulties Encountered in the Digital Services of the Philippine Social Security System in terms of Processing of Personal Data



(Indicators)	BPO		FRONT-LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
Disclosure and sharing of personal data to third parties should be granted only with prior consent or authority from the Data Subjects or if subjected to judicial order or covered by a data sharing agreement.	3.41	HR	3.36	HR	3.36	HR	3.38	HR	1
Fingerprint, signature, and photo of spouse and other dependents/ beneficiaries should be part of the detail information of the member for future claim	3.33	HR	3.30	HR	3.32	HR	3.31	HR	2.5
Access to the documents containing personal data submitted to the SSS should be limited only to regular employees, excluding casual and contractual employees.	3.34	HR	3.28	HR	3.30	HR	3.31	HR	2.5
Storage and retention of physical/ electronic documents containing personal data should be archived/kept in a secure and protected record rooms/offsite storage facilities or receptacles/cabinets pursuant to the policies issued.	3.35	HR	3.26	HR	3.30	HR	3.30	HR	4
Fingerprint and signature, photo, and scanned documents used in the membership registration, application of SSS programs, and other transactions should be integrated into one digital module.	3.26	PR	3.28	HR	3.36	HR	3.30	HR	5
Physical documents/data in storage devices should be disposed/ permanently erased in accordance with records retention, screening and disposal.	3.26	PR	3.26	HR	3.32	HR	3.28	HR	6
Average Weighted Mean	**3.32**	**HR**	**3.29**	**HR**	**3.33**	**HR**	**3.31**	**HR**	

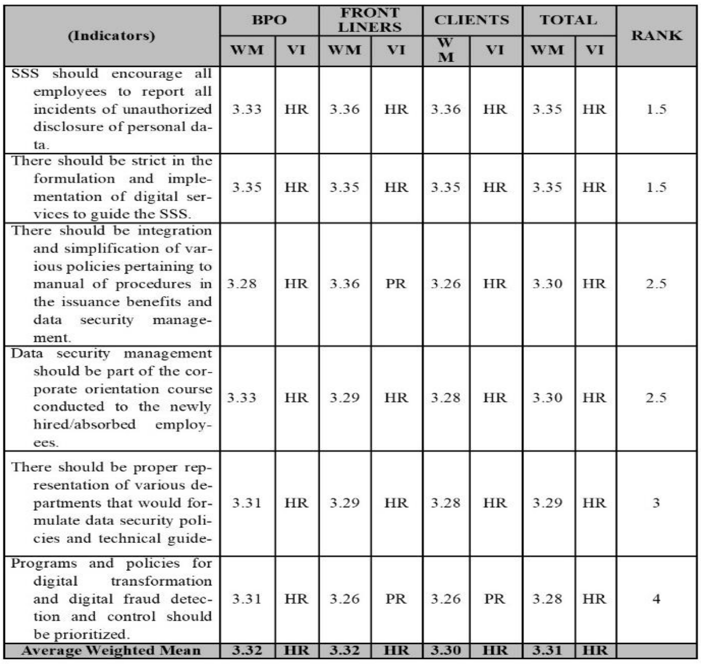
Table 13 presents the respondents' evaluation as to the proposed measures in the digitization of services in the Philippine Social Security System in terms of processing of personal data. Based on the scores, an overall Weighted Mean of 3.31 was obtained marked as Highly Recommended. It must be noted that it is crucial that digital platforms prioritize the protection of personal data and ensure that information is only shared with third parties when authorized by the Data Subjects, a judicial order, or data-sharing agreement. To simplify processes like membership registration, SSS program applications, and other transactions, a digital module must be created immediately to integrate fingerprint, signature, photo, and scanned documents. Only regular employees should have access to the document containing personal data submitted to the SSS, excluding casual and contractual employees. To safeguard important personal data, physical and electronic records must be archived and kept in secure and protected record rooms or offsite storage facilities under strict policies. For future claims, spouses', dependents', and beneficiaries' fingerprints, signatures, and photos must be taken as a crucial part of their detailed information.

Lastly, it is of utmost importance that physical documents and data in storage devices are properly disposed of or permanently erased by RRSD/ISSP to ensure that no personal data is compromised.

According to Kablawi (2022), typically, when an organization realizes it is in possession of data that are no longer required, it is because employees have not been accessing those data on a daily basis, which can result in overlooking data protection measures and making data vulnerable to breach. Certain regulations require organizations to enforce a retention policy for deleting data. To be in compliant with those regulations, enterprises must take data disposal seriously and abide by the data subject's right to have their personal information deleted if they withdraw their consent for the organization to use and process their data.

In addition to compliance, understanding the importance of data disposal can help organizations protect personal data from being leaked via data breaches, which, in turn, prevents the organization's reputation from being damaged and saves the cost of remediation efforts and/or additional storage space.

Table 14. Respondents' Evaluation as to the Proposed Measures to Address the Difficulties encountered in the Digital Services of the Philippine Social Security System in terms of Organizational Measures



(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		RANK
	WM	VI	WM	VI	W M	VI	WM	VI	
SSS should encourage all employees to report all incidents of unauthorized disclosure of personal data.	3.33	HR	3.36	HR	3.36	HR	3.35	HR	1.5
There should be strict in the formulation and implementation of digital services to guide the SSS.	3.35	HR	3.35	HR	3.35	HR	3.35	HR	1.5
There should be integration and simplification of various policies pertaining to manual of procedures in the issuance benefits and data security management.	3.28	HR	3.36	PR	3.26	HR	3.30	HR	2.5
Data security management should be part of the corporate orientation course conducted to the newly hired/absorbed employees.	3.33	HR	3.29	HR	3.28	HR	3.30	HR	2.5
There should be proper representation of various departments that would formulate data security policies and technical guide-	3.31	HR	3.29	HR	3.28	HR	3.29	HR	3
Programs and policies for digital transformation and digital fraud detection and control should be prioritized.	3.31	HR	3.26	PR	3.26	PR	3.28	HR	4
Average Weighted Mean	**3.32**	**HR**	**3.32**	**HR**	**3.30**	**HR**	**3.31**	**HR**	

Table 14 presents the respondents' evaluation as to the proposed measures in the digitization of services in the Philippine Social Security System in terms of organizational measure.

Based on the scores, an overall Weighted Mean of 3.31 was obtained marked as Highly Recommended. Basing on the score, the proposed measures for digitizing services in the Philippine Social Security System received a highly commendable recommendation in terms of organizational measures. It is imperative that SSS management fosters an environment where employees feel comfortable reporting any incidents of unauthorized personal data disclosure. To ensure proper representation of various departments that formulate data security policies and technical guidelines, SSS must develop and implement digital services without any further delay. Moreover, digital security management should be an integral part of the corporate orientation course for newly hired or absorbed employees. Policies related to manual procedures for benefit issuance and data security management should be streamlined and integrated immediately. Finally, priority should be given to programs and policies focused on digital transformation, as well as digital fraud detection and control, as they are of utmost importance.

According to Hani (2021), the complexities of state-sponsored terrorism, professional criminals, and basement bad actors are becoming more difficult to comprehend, track, expose, and prevent. In today's world, detecting fraud requires a comprehensive approach that matches data points with activities to determine what is abnormal.

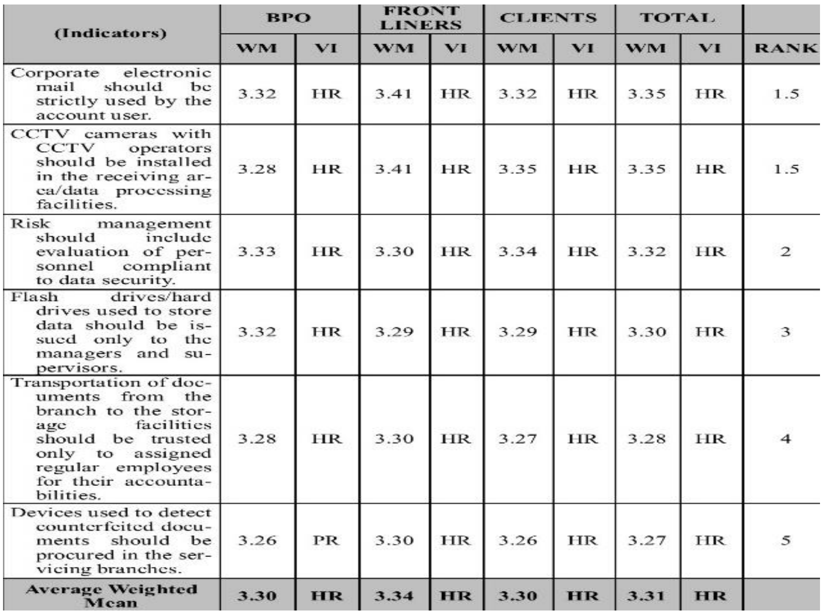
An international tech giant behemoth has unveiled details of its upcoming AI-powered chip designed to bring deep learning inference to enterprise workloads to help address fraud in real-time and to identify and stop a variety of fraud attacks and crime quickly and accurately while improving customer and citizen experiences.

The Artificial Intelligence chip includes on-chip acceleration for AI inference during a transaction. The breakthrough of the new on-chip hardware acceleration, which took three years to develop, is intended to help customers achieve business insights at scale across banking, finance, trading, insurance applications, and customer interactions.

Table 15 presents the respondents' evaluation as to the proposed measures in the digitization of services in the Philippine Social Security System in terms of physical measure. The measures mentioned received weighted means ranging 3.31 to 3.27, all interpreted as Highly Recommended.

But ranking them would place indicators Corporate electronic mail should be strictly used by the account user and CCTV cameras with CCTV operators should be installed in the receiving area/data processing facilities on top with WM of 3.35 while indicator CCTV cameras with CCTV operators should be installed in the receiving area/data processing facilities with WM of 3.27 would be at the bottom. To this end, CCTV cameras should be installed, and operators be assigned in the receiving area and data processing facilities.

Table 15. Respondents' Evaluation as to the Proposed Measures to Address the Difficulties encountered in the Digital Services of the Philippine Social Security System in terms of Physical Measures



(Indicators)	BPO		FRONT LINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
Corporate electronic mail should be strictly used by the account user.	3.32	HR	3.41	HR	3.32	HR	3.35	HR	1.5
CCTV cameras with CCTV operators should be installed in the receiving area/data processing facilities.	3.28	HR	3.41	HR	3.35	HR	3.35	HR	1.5
Risk management should include evaluation of personnel compliant to data security.	3.33	HR	3.30	HR	3.34	HR	3.32	HR	2
Flash drives/hard drives used to store data should be issued only to the managers and supervisors.	3.32	HR	3.29	HR	3.29	HR	3.30	HR	3
Transportation of documents from the branch to the storage facilities should be trusted only to assigned regular employees for their accountabilities.	3.28	HR	3.30	HR	3.27	HR	3.28	HR	4
Devices used to detect counterfeited documents should be procured in the servicing branches.	3.26	PR	3.30	HR	3.26	HR	3.27	HR	5
Average Weighted Mean	**3.30**	**HR**	**3.34**	**HR**	**3.30**	**HR**	**3.31**	**HR**	

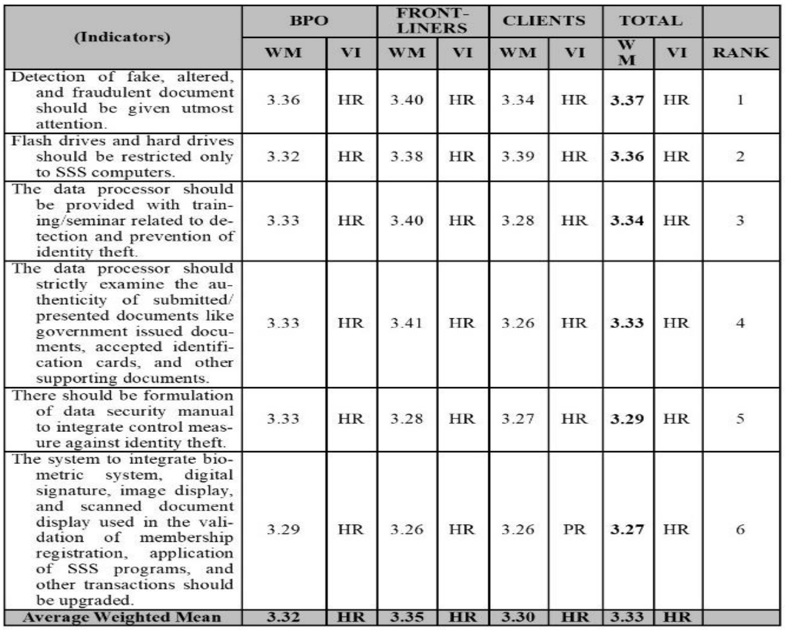
The corporate email system should be strictly used by authorized account users only. It is imperative that the transportation of documents from the branch to the storage facilities is entrusted only to assigned regular employees who will be held accountable. Flash drives and hard drives used to store data should be restricted to managers and supervisors. Risk management must include evaluating personnel compliance with data security policies. Finally, it is recommended that the servicing branches procure devices that can detect counterfeit documents.

According to Northlak (2023), fighting counterfeit documents requires international collaboration and information sharing among governments, organizations, and law enforcement agencies. Sharing knowledge, best practices, and intelligence on emerging counterfeit techniques enhances collective efforts to combat this threat. Collaborative databases and secure communication channels facilitate swift information exchange, enabling stakeholders to stay vigilant and respond efficiently.

NorthLark takes a comprehensive approach to combatting counterfeit documents by integrating advanced security features, optical and digital verification, ML and AI, document forensics, and international collaboration. In addition, NorthLark has developed its own facial biometric identification and verification AI technology and has a dedicated team of experts.

This allows NorthLark to strengthen its capabilities in identifying and countering counterfeit documents, further mitigating risks, safeguarding operations, and maintaining trust, by continuously investing in research.

Table 16. Respondents' Evaluation as to the Proposed Measures to Address the Difficulties encountered in the Digital Services of the Philippine Social Security System in terms of Technical Measures



(Indicators)	BPO		FRONTLINERS		CLIENTS		TOTAL		
	WM	VI	WM	VI	WM	VI	WM	VI	RANK
Detection of fake, altered, and fraudulent document should be given utmost attention.	3.36	HR	3.40	HR	3.34	HR	**3.37**	HR	1
Flash drives and hard drives should be restricted only to SSS computers.	3.32	HR	3.38	HR	3.39	HR	**3.36**	HR	2
The data processor should be provided with training/seminar related to detection and prevention of identity theft.	3.33	HR	3.40	HR	3.28	HR	**3.34**	HR	3
The data processor should strictly examine the authenticity of submitted/ presented documents like government issued documents, accepted identification cards, and other supporting documents.	3.33	HR	3.41	HR	3.26	HR	**3.33**	HR	4
There should be formulation of data security manual to integrate control measure against identity theft.	3.33	HR	3.28	HR	3.27	HR	**3.29**	HR	5
The system to integrate biometric system, digital signature, image display, and scanned document display used in the validation of membership registration, application of SSS programs, and other transactions should be upgraded.	3.29	HR	3.26	HR	3.26	PR	**3.27**	HR	6
Average Weighted Mean	**3.32**	**HR**	**3.35**	**HR**	**3.30**	**HR**	**3.33**	**HR**	

Table 16 presents the respondents' evaluation as to the proposed measures in the digitization of services in the Philippine Social Security System in terms of technical measure. Based on the scores, an overall Weighted Mean of 3.33 marked as Highly Recommended was obtained. This result only shows that technical measures can solve the problems at all times. In order to detect fake, altered, and fraudulent documents, advanced technology needs to be employed.

Data processors should be provided with training and seminars to prevent identity theft.

A data security manual should be formulated to integrate digital measures against cybercrimes.

The use of flash drives and hard drives should be restricted to SSS computers only.

Data processors should thoroughly examine the authenticity of submitted or presented documents such as government-issued documents, accepted identification cards, and other supporting documents. Additionally, the system should be upgraded to integrate biometric systems, digital signatures, image display, and scanned document display for the validation of membership registration, SSS program application, and other transactions.

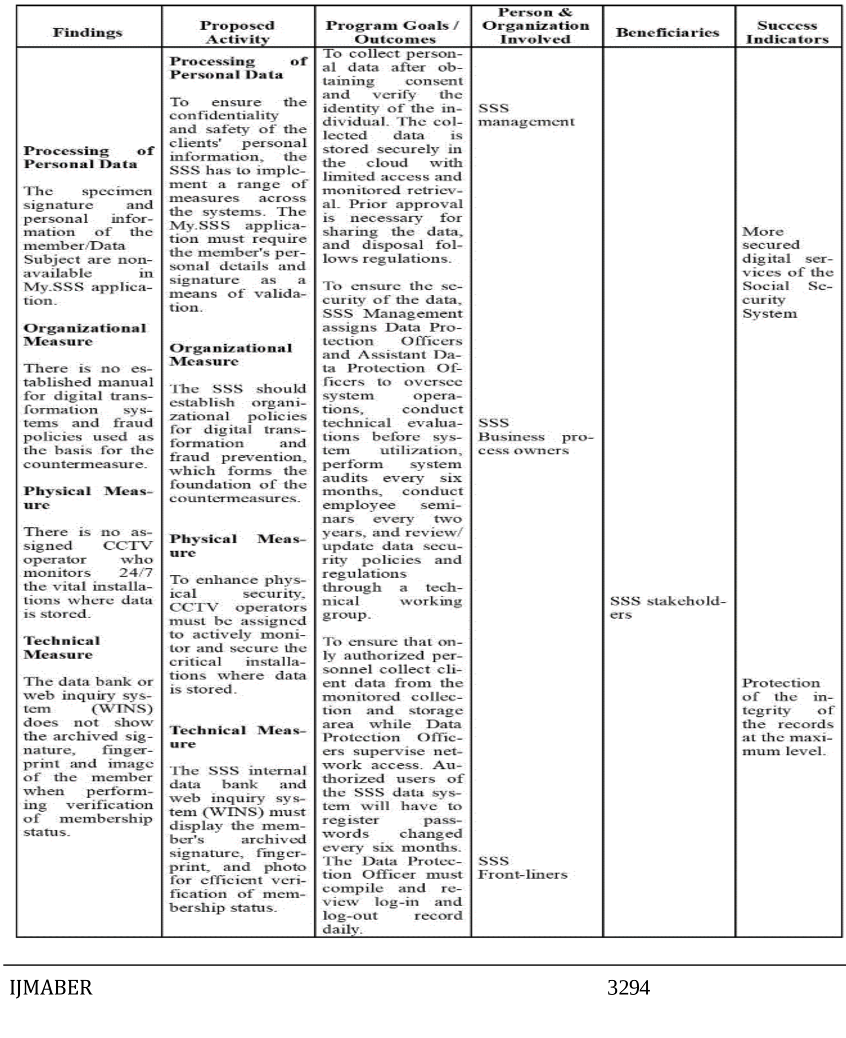
According to Ponti (2021), the SSS reported that the pandemic combined with their digitalization efforts to mitigate the impact had resulted in a surge in SSS electronic transactions. The agency said that transactions through the SSS's electronic channels accounted for 75% of the total in 2020, up from 35% in the previous year. Manual transactions, in turn, dropped from 65% of the total in 2019 to just 25% in 2020. The agency also registered 11.14 times jump in the download of its mobile app in 2018 from the 3.12 million downloads as of end-December 2019.

Meanwhile, lawmakers in the country have urged the SSS and other agencies to continue to invest more aggressively in boosting their "computing capacities" so that they can deliver superior services to the public over the digital space. Agencies should continue to improve and expand their transactions so that their respective members can conveniently do them online.

Problem 6: Proposed integrated policy for strategic approach

This study was conducted to assess the digitization of services in the Social Security System in terms of processing of personal data, organizational measures, physical measures, and technical measure. And based on the findings of the study, an integrated policy for strategic approach to digitization was proposed.

Integrated Policy for Strategic Approach to Digital Services in the Philippine Social Security System



Findings	Proposed Activity	Program Goals / Outcomes	Person & Organization Involved	Beneficiaries	Success Indicators
Processing of Personal Data The specimen signature and personal information of the member/Data Subject are non-available in My.SSS application. **Organizational Measure** There is no established manual for digital transformation systems and fraud policies used as the basis for the countermeasure. **Physical Measure** There is no assigned CCTV operator who monitors 24/7 the vital installations where data is stored. **Technical Measure** The data bank or web inquiry system (WINS) does not show the archived signature, fingerprint and image of the member when performing verification of membership status.	**Processing of Personal Data** To ensure the confidentiality and safety of the clients' personal information, the SSS has to implement a range of measures across the systems. The My.SSS application must require the member's personal details and signature as a means of validation. **Organizational Measure** The SSS should establish organizational policies for digital transformation and fraud prevention, which forms the foundation of the countermeasures. **Physical Measure** To enhance physical security, CCTV operators must be assigned to actively monitor and secure the critical installations where data is stored. **Technical Measure** The SSS internal data bank and web inquiry system (WINS) must display the member's archived signature, fingerprint, and photo for efficient verification of membership status.	To collect personal data after obtaining consent and verify the identity of the individual. The collected data is stored securely in the cloud with limited access and monitored retrieval. Prior approval is necessary for sharing the data, and disposal follows regulations. To ensure the security of the data, SSS Management assigns Data Protection Officers and Assistant Data Protection Officers to oversee system operations, conduct technical evaluations before system utilization, perform system audits every six months, conduct employee seminars every two years, and review/update data security policies and regulations through a technical working group. To ensure that only authorized personnel collect client data from the monitored collection and storage area while Data Protection Officers supervise network access. Authorized users of the SSS data system will have to register passwords changed every six months. The Data Protection Officer must compile and review log-in and log-out record daily.	SSS management SSS Business process owners SSS Front-liners	SSS stakeholders	More secured digital services of the Social Security System Protection of the integrity of the records at the maximum level.

Based on the findings of the study, the following conclusions were drawn.

1. Additional physical and electronic paperwork, including personal data, is required by the Philippine Social Security System. It must be archived/appropriately stored in a secured record room/offsite storage facilities or receptacles/cabinets, according to policies.
2. Through digital channels, the Philippine Social Security System reveals and exchanges personal data with other parties. It has limited control over those granted only with the previous consent or authorization of the Data Subjects, or if subject to a judicial order or covered by a data-sharing agreement.
3. Data security management is available in the Philippine Social Security System, but it is not included in the corporate orientation course for newly hired/absorbed employees.
4. The Philippine Social Security System has CCTV cameras installed and assigned CCTV operators in the receiving area/data processing facilities.
5. The Philippine Social Security System does yet to use advanced technology to detect fake, altered, and fraudulent documents.
6. SSS still has to use advanced technology to formulate a comprehensive data security manual to integrate digital measures against cybercrimes.

Based on the findings and conclusions of the study, the researcher strongly recommends the following:

1. Storage and retention of physical / electronic documents containing personal data should be archived/kept in a secured and protected record rooms/offsite storage facilities or receptacles/cabinets pursuant to the policies issued.
2. Using digital platform to disclose and share personal data to third parties should be granted only with prior consent or authority from the Data Subjects or if subjected to judicial order or covered by a data sharing agreement.
3. Data security management should be part of the corporate orientation course conducted to the newly hired/absorbed employees.
4. More CCTV cameras with assigned CCTV operators should be installed in the receiving area/data processing facilities.
5. Detection of fake, altered, and fraudulent document should be done through the aid of advance technology.
6. Formulation of data security manual to integrate digital measure against cybercrimes should be done

References

Acopiado, I. (2022). Digital payment adoption during the COVID-19 pandemic in the Philippines. Retrieved December 02, 2022, from https://philjournalsci.dost.gov.ph/images/pdf/pjs_pdf/vol151no3/adoption_of_digital_payment_during_pandemic_in_the_Phils_.pdf

Adomela, O. (2021). Towards an effective Information Assurance and Risk Management (IA&RM) guide: A case study. Retrieved June 01, 2022, from https://www.researchgate.net/publication/351587268_Towards_an_Effective_Information_Assurance_and_Risk_Management_IARM_Guide_A_Case_Study

Alokluk, J. (2019). Archiving and document management at Tabiah University: A case study. Retrieved May 01, 2021, from https://www.researchgate.net/publication/336012392

Alzubi, O.A., Qiqieh, I. & Alzubi, J.A. Fusion of deep learning based cyberattack detection and classification model for intelligent systems. Cluster Comput 26, 1363–1374 (2023). https://doi.org/10.1007/s10586-022-03686-0

Amhag, L., Hellstrom, L., & Stigmar, M. (2019). Teacher educators' use of digital tools and needs for digital competence in higher education. Journal of Digital Learning in Teacher Education, 35(4), 203–220. Retrieved December 02, 2023, from https://doi.org/10.1080/21532974.2019

.1646169 and challenges for leaders in the emerging countries in response to COVID-19 pandemic.

Basantes, A., Cabezas, M., & Casillas, S. (2020). Digital competences relationship between gender and generation of university professors. International Journal on Advanced Science Engineering Information Technology, 10(1), 205–211.

Basilotta, V., García-Valcárcel, A., Casillas, S., & Cabezas, M. (2020). Evaluación de competencias informacionales en escolares y estudio de algunas variables influyentes. Revista Complutense De Educación, 31(4), 517–528. Retrieved December 02, 2022, from https://doi.org/10.5209/rced.65835

Basolitta, V. et al. (2022). Teachers' digital competencies in higher education: a systematic literature review. Retrieved December 02, 2022, from https://educationaltechnologyjournal.springeropen.com/articles/10.1186/s41239-021-00312-8

Belanger, C. (2022). Pulsar security: USB security risks|When flash drives become dangerous. Retrieved December 2, 2022, from https://blog.pulsarsecurity.com

Betz, A. (2012). The experiences of adult/child identity theft victims. Iowa State University. Retrieved December 02, 2022, from https://dr.lib.iastate.edu/entities/publication/0ed04671-6774-478f-a112-30822839b61e

Bird & Bird (2019). Big data, issues, & opportunities: Data sharing agreements. Retrieved October 10, 2020, from https://www.twobirds.com

Bolpagni, R. Gavina, & D. Ribeiro (Eds.), Industry 4.0 for the built environment: method-

Cabero, J. (2020). Aprendiendo del tiempo de la COVID-19. Revista Electrónica Educare, 24(Suppl.1), 4–6. Retrieved October 10, 2023, from https://doi.org/10.15359/ree.24-s.

Cabero, J., & Palacios, A. (2020). Marco Europeo de Competencia Digital Docente «DigCompEdu» y cuestionario «DigCompEdu Check-In». EDMETIC, Revista De Educación Mediática y TIC, 9(1), 213–234. Retrieved October 10, 2023, from https://doi.org/10.21071/edmetic.v9i1.12462

Cabero, J., Barroso, J., & Palacios, A. (2021). Digital competences of educators in health sciences: Their relationship with some variables. Educación Médica, 22(2), 94–98. Retrieved October 10, 2023, from https://doi.org/10.1016/j.edumed.2020.11.014

Cabero, J., Barroso, J., Palacios, A., & Llorente, C. (2020). Marcos de competencias digitales para docentes universitarios: Su evaluación a través del coeficiente competencia experta. Revista Electrónica Interuniversitaria De Formación Del Profesorado, 23(2), 1–18. Retrieved October 10, 2023, from https://doi.org/10.6018/reifop.413601

Caena, F. & Redecker, C. (2019). Aligning teacher competence frameworks to 21st century challenges: The case for the European digital competence. Framework for educators (DigCompEdu). European Journal of Education, 54(3), 1–14. Retrieved October 10, 2023, from https://doi.org/10.1111/ejed.12345

Casado-Aranda, L.-A., Sánchez-Fernández, J., & Viedma-del-Jesús, M. I. (2020). Analysis of the scientific production of the effect of COVID-19 on the environment: A bibliometric study. Environmental Research, 193, 1–12. Retrieved October 10, 2023, from https://doi.org/10.1016/j.envres.2020.110416

Casado-Aranda, L.-A., Sánchez-Fernández, J., Montoro-Ríos, F. J., & Horcajadas, M. I. A. (2021). Evaluation of the work-integrated learning methodology: Teaching marketing through practitioner experience in the classroom. Mathematics, 9(17), 2164. Retrieved October 10, 2023, from https://doi.org/10.3390/math9172164

Cham, T. et al. (2022). Digitalization of public service delivery in Asia. Retrieved June 19, 2022, from https://link.springer.com/article/10.1057/s41270-022-00167-6

Chang, JW., Yen, N. & Hung, J.C. Design of a NLP-empowered finance fraud awareness model: the anti-fraud chatbot for fraud detection and fraud classification as an instance. J Ambient Intell Human Comput 13, 4663–4679 (2022). https://doi.org/10.1007/s12652-021-03512-2

Choi, P. & Xavier, D. (2021). Digitalization of public service delivery in Asia. Retrieved June 19, 2022, from https://www.apo-tokyo.org/papers

DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adult. Innovation in Aging, 5(4), 1–11. Retrieved June 19, 2022, from https://doi.org/10.1093/GERONI/IGAB043 digital transformation: How to lead service employees effectively during the COVID-19

Durmaz, O., Hawrami, S. S., & Hamasaeed, A. M. (2022). The suitable leadership for industry4.0. Retrieved June 21, 2023, from Journal of Global Economics and Business, 3(8), 113–124.

Eberl, J. K., & Drews, P. (2021). Digital leadership–mountain or molehill? Retrieved June 21, 2023, from A literature review. In international conference on Wirtschaftsinformatik (pp. 223–237).

Elevant, I. (2021). Consent as a basis of processing personal data in the Internet of Things. Retrieved May 5, 2024, from https://helda.helsinki.fi/server/api/core/bitstreams/c054519f-50a3-4f4b-b526d0eb2fa13be8/content.

Emerging Science Journal, 5, 21–36. Leadership compass: Six competencies for digital transformation entrepreneurship. International

Fabian, N. (2022). Digital transformation and organizational implications. Retrieved June 29, 2022, from https://research.rug.nl/en/publications/digital-transformation-and-organizational-implications

Fabito, B. et al. (2018). Data Privacy Act of 2012: A case study approach to Philippine government agencies compliance. Retrieved June 29, 2022, from https://www.researchgate.net/publication/327281053

Forsell, T. (2020). "You're kind of a student, but at a distance": Problematic school absenteeism from the perspective of students, parents, and school staff." Retrieved February 10 2022, from http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-155437

Gfrerer A.E. et al. (2021) Digital needs diversity: Innovation and digital leadership from a female managers perspective. In Schallmo D.R.A., Tidd J. (eds) Digitalization, Management for Professionals. Retrieved February 10, 2022, from Springer, Cham, 335-349.

Gudergan, G. et al. (2021), Digital Leadership - Which leadership dimensions contribute to digital transformation success. Retrieved February 10, 2022, from 2021 IEEE International Conference on Engineering, Technology and Innovation, Cardiff, 1- 8.

Guzman, V. et al. (2020), Characteristics and skills of leadership in the context of industry. Retrieved February 10, 2022, from Procedia Manuf. Shangai, 43, 543–550.

Hai, T. N., Van, Q. N., & Tuyet, M. N. T. (2021). Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. Retrieved June 21, 2023, from Emerging Science Journal, 5, 21–36.

Hani, A. (2021). Adopting AI-powered technology for fraud prevention in the Philippines. Retrieved June 21, 2022, from https://opengovasia.com/adopting-ai-powered-technology-for-fraud-prevention-in-the-philippines/

Heredia, J., Castillo-Vergara, M., Geldes, C., Gamarra, F. M. C., Flores, A., & Heredia,W. (2022). How do digital capabilities affect firm performance? The mediating role of technological capabilities in the 'new normal.' Retrieved June 21, 2023, from Journal of Innovation & Knowledge, 7(2),100171.

Hinterhuber, A. et al. (2021). Managing digital transformation: Understanding the strategic process (1st ed.). Routledge. Retrieved June 21, 2022, fromhttps://doi.org/10.4324/9781003008637

Ilzan, A. et al. (2023) Understanding the phenomenon and risks of identity theft and fraud on social media. Retrieved August 20, 2022, from https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0256822 In International conference on Wirtschaftsinformatik (pp. 223–237).

Ioannou, A. et al. (2021) Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis. Retrieved August 20, 2022, from https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0256822 Journal of Entrepreneurial Behavior & Research.

Kane, G.C., Nguyen-Phillips, A., Copulsky, J., & Andrus, G. (2019), How digital leadership is(n't) different. MIT Sloan Management Review, 60(3), 34-39.

Karippur, N. K. & Balaramachandran, P. R. (2022). Retrieved June 21, 2023, from Antecedents of effective digital leadership of enterprises in Asia Pacific

Kazım, F. A. B. (2019), Digital transformation and leadership style: A multiple case study. Journal of International Business, 3(1), 24–33.

Khando, K. et al. (2022). The emerging technologies of digital payments and associated challenges: A systematic literaturereview. Retrieved December 28, 2022, from https://www.researchgate.net/publication/366700399_The_Emerging_Technologies_of_Digital_Payments_and_Associated_Challenges_A_Systematic_Literature_Review

Klein, M. (2020). Leadership characteristics in the era of digital transformation. Retrieved August 20, 2023, from Business & Management Studies: An International Journal (BMIJ), 8(1), 883–902.

Klein, M. (2020). Leadership characteristics in the era of digital transformation. Retrieved June 21, 2023, from

Kokot, K., Kokotec, I. Đ., & Čalopa, M. K. (2021), Impact of leadership on digital transformation. Retrieved August 20, 2023, from 2021 IEEE Technology & Engineering Management Conference- Europe (TEMSCON-EUR), Dubrovnik, 1-6.

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. Sage Open, 11(3). https://doi.org/10.1177/21582440211047576Lawry, C. (2019). The vital importance of digitizing non-disclosure agreements. Retrieved August 28, 2021, from https://www.swipedon.com/blog/digitizing-non-disclosure-agreements

Lee, C.-H., Wang, D., Desouza, K., & Evans, R. (2021). Digital transformation and the new normal in China: How can enterprises use digital technologies to respond to COVID-19? Retrieved June 21, 2023, from Sustainability, 13(18), 10195.

McCarthy, P., Sammon, D., & Alhassan, I. (2021). Digital transformation leadership characteristics: A literature analysis. Retrieved August 28, 2023, from Journal of Decision Systems, 1-30.

Mihardjo L., Sasmoko S., Alamsjah F., & Djap E. (2019), Digital leadership role in developing business model innovation and customer experience orientation in industry 4.0. Retrieved August 28, 2021, from Management Science Letters, 9, 1749–1762.

Mishra, A. (2022). Cybersecurity enterprises policies: A comparative study. Retrieved January 17, 2023, from https://pubmed.ncbi.nlm.nih.gov/35062504

Mohamed, A. et al. (2022). A systematic literature review for authorization andaccess control: Definitions, strategies and models. Retrieved August 10, 2023,from https://www.emerald.com/insight/content/doi/10.1108/IJWIS-04-2022-0077/full/html

Morgan, B., & Papadonikolaki, E. (2022). Digital leadership for the built environment. In M. Bolpagni, R. Gavina, & D. Ribeiro (Eds.), Industry 4.0 for the built environment: Method-ologies, technologies, and skills (pp. 591–608). Springer. Retrieved June 21, 2023, from https://doi.org/10.1007/978-3-030-82430-3_2514 .

Normal in China: How can enterprises use digital technologies to respond to COVID-19? of enterprises in Asia Pacific ologies, technologies and skills (pp. 591–608). Springer. https://doi.org/10.1007/978-3-030-

On business agility during COVID-19 era. Procedia Computer Science, 197, 326–335. pandemic. Journal of Service Management, 32(1), 71–85.

Phillip, J. & Aguilar, M. G. (2021). Students' perceptions of leadership skills necessary for digital transformation. Retrieved August 10, 2023, from Journal of Education for Business, 1-13.

Porfírio, J. A., Carrilho, T., Felício, J. A., & Jardim, J. (2021). Leadership characteristics and digital transformation. Retrieved August 28, 2021, from Journal of Business Research, 124, 610-619.

Prakasa, Y., Raharjo, K., & Wiratama, I. (2020), transformational leadership and digital maturity. Retrieved August 28, 2021, from The Mediating Role of Organizational Culture, Proceedings of the 2nd Annual International Conference on Business and Public Administration (AICOBPA 2019), Malang, 224-229.

Promsri, D. C. (2019). The developing model of digital leadership for a successful digital transformation. Retrieved August 10, 2023, from GPH- International Journal of Business Management (IJBM), 2(8), 1-8.

Promsri, C. (2019). The developing model of digital leadership for a successful digital transformation. Retrieved June 21, 2023, from GPH-International Journal of Business Management, 2(08), 1–8.

Pu, W. et al. (2022). To disclose or not to disclose: An evaluation of the effects of information control and social network transparency. Retrieved July 01, 2023, from https://www.sciencedirect.com/science/article/abs/pii/S0167404821003333

Sacolick, I. (2023). Digital transformation challenges and 14 ways to solve them. Retrieved June 20, 2023, from https://www.techtarget.com/searchcio/tip/3-biggest-digital-transformation-challenges-and-how-to-solve-them

Sağbaş, M. et al. (2022). Digital leadership: A systematic conceptual literature review. Retrieved January 23, 2023, from https://www.researchgate.net/publication/358729671_Digital_Leadership_A_Systematic_Conceptual_Literature_Review

Saglam, R. et al. (2022). Personal information: Perceptions, types, and evolution. Retrieved January 23, 2023, from https://doi.org/10.1016/j.jisa.2022.103163

Saputra, N., Sasanti, N., Alamsjah, F., & Sadeli, F. (2022). Strategic role of digital capability

Saputra, N., Sasanti, N., Alamsjah, F., & Sadeli, F. (2022). Strategic role of digital capability on business agility during COVID-19 era. Retrieved June 21, 2023, from Procedia Computer Science, 197, 326–335.

Sbriz, L. (2021). Communicating information-security risk simply and effectively, Part 1. Retrieved June 19, 2022, from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6

Schiuma G., Schettini E., Santarsiero F., & Carlucci, D. (2021), The transformative leadership compass: Six competencies for digital transformation entrepreneurship, Retrieved January 23, 2023, from International Journal Of Entrepreneurial Behavior & Research

Schiuma, G., Schettini, E., Santarsiero, F., & Carlucci, D. (2021). The transformative leadership compass: Six competencies for digital transformation entrepreneurship. Retrieved June 21, 2023, from International Journal of Entrepreneurial Behavior & Research.

Schmitt, E. (2019). Identity theft resource guide information system monitoring access log database on database server. Retrieved June 21, 2021, https://dn790009.ca.archive.org

Shah, S. S. & Patki, S. M. (2020), Getting traditionally rooted Indian leadership to embrace digital leadership: Challenges and way forward. Retrieved January 23, 2023, from LMX, Leaders Education Personal Interdisciplinary, 2, 29–40.

Šidlauskas, A. (2021). The role and significance of the data protection officer in the organization. Retrieved May 5, 2024, from https://www.researchgate.net/publication/351874824_The_Role_and_Significance_of_the_Data_Protection_Officer_in_the_Organization

Skog, D. (2019). The dynamics of digital transformation: The role of digital innovation, ecosystems, and logics in fundamental organizational. Retrieved June 21, 2021, https://www.researchgate.net/publication/330539207

Sood P., Sharma C., Nijjer S., Sakhuja S. 2023 International Journal of System ssurance Engineering and Management 14(6), pp.2120-2135

Southekal, P. (2022). Data prioritization in digital transformation programs. Retrieved January 20, 2023, from https://www.forbes.com/sites/forbestechcouncil Sustainability, 13(18), 10195.

Sy, F. et al. (2021). Philippine privacy commission issues: Data sharing agreement guidelines. Retrieved January 21, 2022, from https://www.zicolaw.com/resources/alerts/philippine-privacy-commission-issues-data-sharing-agreement-guidelines/

Tabuena, A. et al. (2022). A literature review on digital marketing strategies and its impact on online business sellers during the COVID-19 crisis. Retrieved December 15, 2022, from https://www.researchgate.net/publication/360454336_A_Literature_Review_on_Digital_Marketing_Strategies_and_Its_Impact_on_Online_Business_Sell ers_During_the_COVID-19_Crisis technological capabilities in the 'new normal.' Journal of Innovation & Knowledge, 7(2),

Tierney, M. (2021). Data security explained: Challenges and solutions. Retrieved February 15, 2022, from https://blog.netwrix.com/2021/07/26/data-security

Torres, Q. (2021). Philippines: New circular on data sharing agreements issued by the National Privacy Commission. Retrieved June 21, 2022, from https://insightplus.bakermckenzie.com transformation. GPH-International Journal of Business Management, 2(08), 1–8.

Treceñe, J. (2021). The digital transformation strategies of the Philippines from 1992 to 2022: A review. Retrieved March 15, 2022, from https://www.researchgate.net/publication/348958893_The_Digital_Transformation_Strategies_of_the_Philippines_from_1992_to_2022_A_Review

Turillazi, A. et al. (2022). Investigating accessibility of social security system (SSS) mobile application: A structural equation modeling approach. Retrieved June 21, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007389.

W. (2022). How do digital capabilities affect firm performance? The mediating role of

Yıkılmaz, I & Sürücü, L. (2021), Dijital Çağda Liderliğin Yeni Yüzü: Dijital Liderlik. İçinde, İ. Tarakçı, B. Göktaş (Ed.), Dijital Gelecek Dijital Dönüşüm-2, Retrieved June 21, 2023, from İstanbul: Efe Akademi, 301-317.

Yıkılmaz, İ. (2021a), Covid 19 pandemic as a digital transformation catalyst, Hamza Şimşek Marcel Mečiar (Eds.) The Social and Economic Impact of Covid–19: Rapid Transformation of the 21st Century Society. Retrieved June 21, 2023, from IJOPEC: London, 119-139.

Yung-Tsan, J. et al. (2022). Investigating accessibility of social security system (SSS) mobile application: A structural equation modeling approach. Retrieved June 21, 2023, from https://www.mdpi.com/2071-1050/14/13/7939 reconfiguration of social and moral orders in the Philippines. Journal of Southeast Asian Studies, 51(1–2), 5–24. https://doi.org/10.1017/s0022463420000211