ISSN No:-2456-2165

A Web-Based Data P rivacy Compliance Management System Centered on the Data Privacy Act of 2012 For Business Process Outsourcing Companies

Francis Tovi Kyl C. Meneses

A Research Project Presented to the Faculty of
School of Computing Holy Angel University

In partial fulfillment of the requirements for the
Professional Science Master's Degree in Cybersecurity

Francis Tovi Kyl C. Meneses
July 2022

APPROVAL SHEET

This Capstone Project entitled "A Web-based Data Privacy Compliance Management System centered on the Data Privacy Act of 2012 for Business Process Outsourcing Companies" prepared and submitted in partial fulfillment of the requirements for the degree Professional Science Masters in Cybersecurity, has been examined and recommended for acceptance and oral examination.

Prof. Avigail P. Magbag

Adviser

ORAL EXAMINATION

Approved by the committee of oral examiners on
July 14, 2022

Major Carlos Ely C.Tingson
Panel Chairman

Dr. Marlon I. Tayag
Panel Member

Prof. Kevin Aldrin G. Espinosa
Panel Member

APPROVAL

Accepted and approved in partial fulfillment of the requirements for the degree in Professional Science Masters in Cyber security.

Dr. Alma Theresa D. Manaloto
GS Program Coordinator

Dr. Francisco D. Napalit
Dean, School of Computing

ACKNOWLEDGEMENT

This project would not have been possible without the support of many people. Many thanks to my adviser, Prof. Avigail P. Magbag, who read my numerous revisions and helped make sense of the confusion. Also, thank to my panel members, Dr. Marlon Tayag, Major Carlos Ely Tingson, and Prof. Kevin Aldrin Espinosa, for the helpful comments and suggestions.

Big thanks to Dr. Alma Manaloto for her guidance during my proposal defense and for providing instructions as I move forward. Thank you toMr. Karlo Bathan for the help he extended during the creation of the system.

I would be remiss in not mentioning my family, especially my parent and siblings. Their belief in me has kept my spirits and motivation high during this process. I would also like to thank my dog for all the entertainment and emotional support.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

BPO – Business Process Outsourcing
CMS – Compliance Management System
DPA – Data Privacy Act of 2012
DPS – Data Processing System
DPO – Data Protection Officers
NPC – National Privacy Commission
PIA – Privacy Impact Assessment

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The Philippines serves as a leading destination for business process outsourcing (BPO), and as it ensures its position as a top BPO outsourcing destination, compliance with the Data Privacy Act of 2012 is a must. However, data privacy compliance is never easy; factors such as awareness, budget, and time constraints hamper organizations' compliance. Since manual reviews and internal audits of data privacy compliance activities are time-consuming, resource-intensive, and lack coverage, some BPO companies have chosen to use information systems to address the issues. Nevertheless, there is evidence that organizations are struggling to find the appropriate tools and guidance on compliance management systems (CMS). The researcher developed a standardized web-based CMS to address the issues mentioned. A mixed-method exploratory design was utilized for data collection and analysis. An interview was conducted with 3 DPOs from 3 BPOs to determine the beneficial and lacking features of current systems. The same participants with 60 other employees from the 3 BPOs, validated and verified the developed system and compared its efficiency and effectiveness with the existing systems. It was concluded that the existing CMS the participants used has missing features that could help in their day-to-day tasks, difficult to navigate, not user-friendly, and too broad and general. The results revealed that the respondents rated the Web-based Data Privacy Compliance Management System better than the existing system in terms of effectiveness and efficiency. The developed system was also validated and verified based on the initial scope of the system. To further help with the organization's compliance, an expansion to target participants aside from BPO, incorporating GDPR, CCPRA, and other privacy laws, and integrating good practices such as IAPP can be considered.

CHAPTER 1

INTRODUCTION

The Philippines is a leading destination for business process outsourcing (BPO) (Bodwell et al., 2016). In 2019, the BPO industry was the second-largest contributor to the Philippine economy, providing U.S. $26 billion (Rosales, 2020) and employing at least 1.3 million people in over 1,000 firms, mainly located in urban regions (Reed, Ruehl & Parkin, 2020).

BPO exists in a variety of shapes and sizes, and nearly any process can now be outsourced. BPO services include accounting, human resources, customer service, sales, marketing, administration, information technology, research, manufacturing, and shipping. This can assist businesses in saving resources. However, it is not without concerns, one of which being data privacy and security. However, it comes with several risks, and one of these is data privacy and security (Abelis, 2021).

Data privacy and security is one of the major issues that companies face due to ineffective third-party controls and IT security threats. Companies dealing with user data or sensitive information are legally limited to how much and whom they can share the data with. Business-sensitive information can also leak more easily since the companies do not have direct oversight over the BPO team. Thus, the need for strict data security is at an all-time high (Santaman, Sethumadhavan, Virendra, and Axelrod, 2011).

The National Privacy Commission (NPC) chairman Raymond Liboro said in an interview with news outlet Philstar Global, "the BPO industry is among the high-risk sectors in terms of data breaches and cyber security threats." Chairman Liboro added, "the BPO industry recognizes that data privacy is crucial in today's business environment, trust is becoming a big factor, and privacy equates to trust" (The Philippine Star, 2017). As the Philippines ensures its position as a leading BPO outsourcing destination, the Implementing Rules and Regulations (IRRs) of the Data Privacy Act of 2012 have significant impacts, particularly on the IT and the BPO industry. Due to the fact that this law applies to all activities involving the processing of personal data, both of natural and juridical persons. This law aims at protecting all disclosed information, regardless matter how sensitive, private, or personal it may be.

Data privacy regulations have had a significant influence on BPO firms. One example is their adherence to transparency requirements. Transparency is an essential component of any data protection legislation. It is particularly important to the sector because of the fiduciary connection between BPO companies and their principals. The establishment of strong privacy management programs has been another significant influence created by data privacy policies. While most BPO firms have a strong information security structure, the same cannot be said for data privacy (Ayson, 2022).

In an article he published for the Manila Bulletin, Liboro made it clear that the BPO sector as a whole is a pillar of our developing economy and needs support and protection. He emphasized the significance of the DPA of 2012 and the reasons it is essential for the BPO sector in the Philippines. The existence of this regulation, he continued, clearly specifies the obligations of organizations like BPOs in assuring the safety of personal data. This is advantageous because it reduces the possibility of finger-pointing in the event of a data breach and it enables industry participants to plan and implement processes.

Organizations worldwide are investing heavily in regulatory compliance these days (Braganza & Franken, 2007). A study by the Ponemon Institute (2009) shows that data privacy and protection shortcomings can cause irreversible damage to a company's balance sheet, not to mention its brand, reputation, and customer base trust. It also states that organizations that exhibit a "culture of caring" for data privacy and protection are far less likely to experience security breaches.

The NPC posted an article about an incident with four online lending apps on their official website. The apps have been subject to various complaints of unauthorized use of personal data that resulted in harassment and shaming of borrowers. Because of this, the NPC ordered the closure of all four companies and made Google LLC remove the apps from the Google Play Store (National Privacy Commission, 2021). These types of incidents could happen to any organization, and penalties are much heavier for those who do not comply with the Data Privacy Act of 2012.

Regulatory compliance has become a critical concern for many industries worldwide, and funding to achieve compliance has skyrocketed in response (Abdullah et al., 2009). Executing data privacy compliance in the Philippines is never easy; it was found that factors such as awareness, budget, and time constraints are hampering the compliance of organizations with the Data Protection Act of 2012 (Fabito et al., 2018). In practice, corporations create review systems and undertake internal audits to verify compliance with these data privacy regulatory standards. However, manual reviews and audits are time-consuming, resource-intensive, lack coverage, and thus, inherently do not scale well in companies (Sen et al., 2021). Because of this, organizations are using compliance management systems (CMS) to help with their regulatory responsibilities. CMSs establish systematic, checklist-like processes by which managers seek to improve their organizations' compliance with government regulations. Organizations with certain types of CMSs in place experience fewer compliance violations and show improvements in risk management (Coglinese et al., 2020).

The market offers a variety of compliance management systems. There is a centralized dashboard on these platforms. Risk and incident management, policy management, a data repository, and data breach notification are the majority of their shared features. These CMSs frequently focus on the region- or country-specific data privacy regulation they support. Nevertheless, evidence suggests that organizations struggle to find the appropriate tools and guidance on compliance management systems (Abdullah et al., 2009).

A number of BPO companies have already invested in these CMSs which made the data privacy-related tasks automated and easier to perform. However, the features offered by these CMSs in the market are not specifically tailored to the needs of the companies in the Philippines which means that they do not merely adhere to the Data Privacy Act of 2012. Furthermore, DPOs from the BPO organizationsstated that there are significant elements that could be added to their existing system which might improve their work and compliance. These lacking major features include ticketing systems, user guidance, compliance report, to-do list, privacy impact assessment, inventory of data processing systems, analytics, access for non-privacy personnel, data breach management, news – information dissemination, notification, and access control.

Compliance can be a challenge for companies; however, it gives a competitive advantage to those that make an effort to comply. Considering that one of the major goals of the law was to create confidence in the country's IT and BPO industries, compliance will greatly benefit BPOs by attracting more foreign investors. Customer trust and increased revenue are some of the benefits of adhering to the law.

Every organization may have its unique processes that are incorporated into their compliance practices which are reflected in the information systems (IS) they have in place. Choosing appropriate IS to support BPO companies' compliance with the Data Privacy Act of 2012 posed some challenges. To address these concerns, the development of a standardized web-based compliance management system is proposed. Beneficial and deficient features of the compliance management systems utilized by BPOs will be taken into consideration to standardized compliance in relation to the Data Privacy Act.

A. Problem Statement

An article by CCAP (2018) states that the NPC strictly enforces compliance with the Data Privacy Act, particularly among BPO firms. The commission is also planning to inspect each government agency and BPO to see if there is a Data Protection Officer (DPO) who ensures that the required privacy measures are in place. Violators will face the necessary regulatory penalties if this is not accomplished or if a security breach is proven to be intentionally omitted or concealed.

BPO companies have already invested in compliance management systems to adjust to regulatory requirements. These investments are needed for organizations to stay in business (Perskow, 2003; Anon et al., 2007), as non-compliance with government and legal requirements can have serious consequences. While some BPO firms have decided to incorporate IS into their support architecture, anecdotal evidence indicates that enterprises have difficulty locating relevant tools and features in compliance management systems (Abdullah et al., 2009).

To comply with the law while also adapting to the fast-paced digital economy, the development of a web-based Data Privacy Compliance Management System focusing on the Data Privacy Act of 2012 is deemed to benefit BPOs. The Data Privacy Compliance Management System addressed the NPC's thirty-two (32) point checklist (Lansigan R., n.d.) (Appendix E) and five (5) pillars of compliance (Paguia R., n.d.)

The study aimed to contribute to the development of a standardized Data Privacy Compliance Management System for BPOs while incorporating the beneficial features as well as addressing the identified shortcomings of existing compliance systems. This in return allows better compliance which gives a competitive edge regarding data protection and privacy, which can help minimize damage (Liboro, 2017).

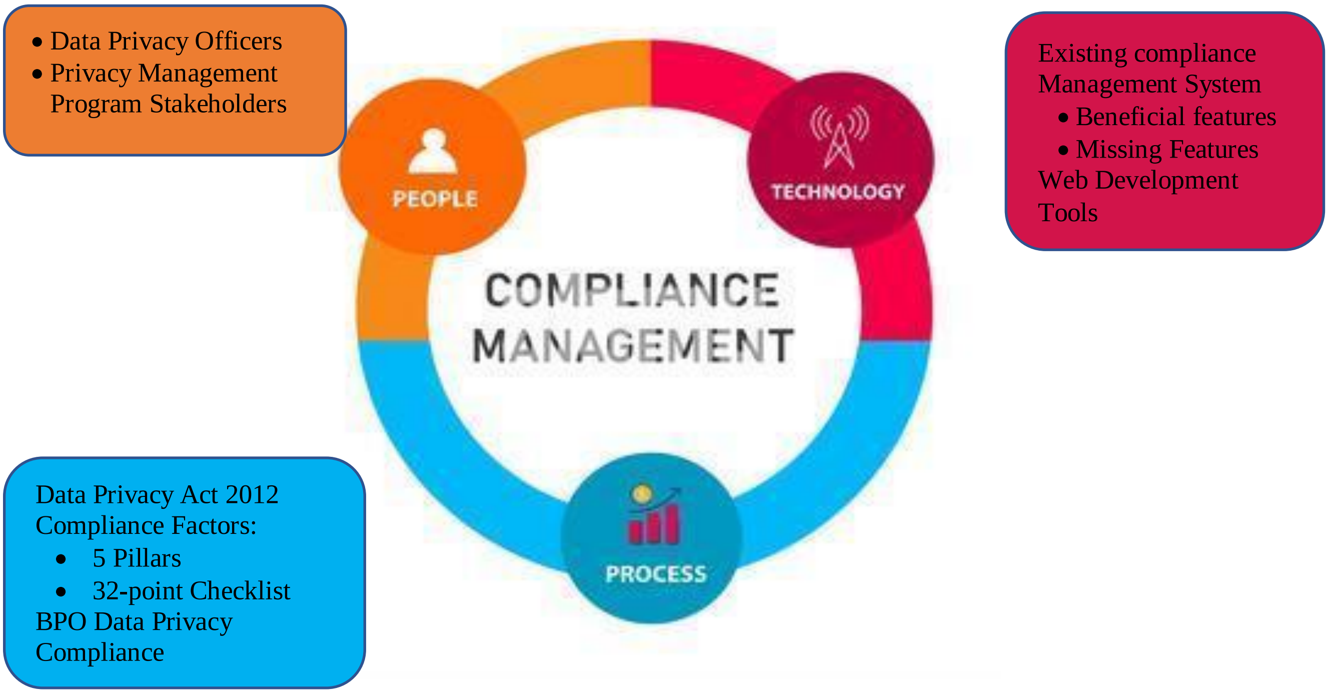
B. Conceptual framework

As shown in Figure 1, the researcher adopted a framework from Information Technology Infrastructure Library (ITIL) to conceptualize the compliance management system for data privacy. It is divided into three areas: people, process, and technology, which are key elements in implementing compliance management in any company (Bilings, 2018).

The first area is people. This area consists of the BPO employees interviewed, such as Data Protection Officers (DPO) and stakeholders in the privacy management program of each company. The people were also the ones who tested the proposed system. Overall, feedback from the people was important, especially in defining the beneficial features of the proposed system and determining whether the system is better than the existing one in terms of efficiency and effectiveness.

The second area is the process. This area explains how the system processes data. The proposed system is built specifically for compliance with the Data Privacy Act of 2012; because of this, the features are heavily reliant on how actual data privacy compliance works. Part of the process is compliance factors in the Data Privacy Act of 2012, such as the five pillars of data privacy and the 32-point checklist.

The last area is technology. Part of this area is the existing systems the participants currently use in their respective organizations. These systems were critical in creating the proposed system because they served as a basis for their beneficial features and shortcomings.



- Data Privacy Officers
- Privacy Management Program Stakeholders

Existing compliance Management System
- Beneficial features
- Missing Features

Web Development Tools

Data Privacy Act 2012 Compliance Factors:
- 5 Pillars
- 32-point Checklist

BPO Data Privacy Compliance

Fig. 1: Conceptual Framework

Note: By Artnahla, 2016

C. Objectives

This study aimed to develop and standardize a Web-based Compliance Management System centered on the Data Privacy Act of 2012 for Business Process Outsourcing companies. Specifically, this study targets to:

- determine the beneficial and deficient features of the compliance management systems used by the three (3) BPO companies;
- validate and verify the developed Web-based Compliance Management System; and
- evaluate the effectiveness and efficiency of use between the standardized compliance management system and the companies' existing systems.

D. Scope and Delimitations

A web-based compliance management system to address the requirements of the Data Privacy Act of 2012, which aims to cover the data privacy concerns of BPO companies, was developed. The system was evaluated using two factors: verification and validation.

The study's findings focused on the benefits and shortcomings of current compliance management systems and how to incorporate missing features to create a standardized web-based management system that will address compliance to the NPC’s five (5) pillars and its thirty-two (32) point checklist.

However, this system's access is limited to web browsers, and the system features are only intended for the use of BPO companies.

E. Significance of the Study

The standardized Data Privacy Compliance Management System will be a significant undertaking that will aid BPO companies in complying with and raising awareness of the Data Privacy Act of 2012.

Privacy Professionals. The system will significantly help automate the day-to-day activities of in-house privacy professionals in the BPO sector. It will also guide the organization's compliance with the Data Privacy Act of 2012 and other mandatory requirements such as breach notification, among others.

Employees. The system will serve as a training environment for employees to access information about data privacy regulations, announcements, and security tips. The system will also serve as the primary contact method for submitting data subject requests, and complaints, and invoking data subject rights.

BPO industry. The system's design and features will benefit the industry by serving as a standardized compliance management system, potentially leading to a higher compliance rate.

Future researcher. The study's findings will help them learn more about a Data Privacy Compliance Management system and its effectiveness. It could also be used as a guide in developing a more advanced system in the future.

CHAPTER 2

METHOD

A. Research Design

This study employed a mixed-method exploratory design for data collection and analysis. The exploratory design is used in studies where the goal is to investigate an occurrence, in this case, the beneficial and deficient features of a compliance management system, where instruments are unavailable and no guiding framework or theory exists (Creswell, Plano Clark, Gutmann, & Hanson, 2003). This design is particularly useful in studies like this one, where important variables are identified in the early first-phase qualitative data collection to be studied further in the quantitative phase and where these variables are unknown. The first phase will identify beneficial and deficient features of current BPO compliance systems, while validation and verification will be measured quantitatively.

B. Participants

Purposive sampling is utilized to select study participants from three (3) BPO companies that meet the inclusion criteria. Companies must have an existing compliance management system to ensure that participants have experience using the system and can identify beneficial and deficient features. The companies' Data Protection Officers (DPO) served as respondents in the qualitative interview, in validating and verifying the system and determining the significant differences between the standardized system and their company's existing system.

For the validation and verification of the developed compliance management system and the comparison of the existing systems of the company and the developed system in terms of efficiency and effectivity, sixty (60) employees from the three BPO companies were also included. These participants must have worked in the BPO company for at least one year and are identified as stakeholders in their companies' privacy management program; this ensures that they are already familiar with the company's internal controls, policies, and privacy compliance activities.

C. Data

This section includes all the details of the data gathering tools, instruments, and techniques described in the research design.

D. Instruments

For the initial phase identified in the research design, a structured interview was conducted to ascertain the aspects of the existing compliance management system at the BPO company. The questions used during the interview were crafted based on the study's objectives. In particular, the questions were centered on the Data Protection Officers' (DPOs) information and the existing system used by the BPOs. The questions were evaluated and validated by a data privacy expert with five (5) years of industry and five (5) years of academic experience (Appendix C). The questions were validated based on their clarity, balance, use of jargon, application to praxis, and relationship to the problem or goals of the study.The questions covered information about the participant's existing compliance management systems (Appendix D).

An evaluation checklist was also used to validate and verify the web-based compliance management system. This rating technique is based on Nuria's research (2005). It is a scoring sheet that is a two-part checklist for verification and validation when evaluating any web-based system (Appendix F).

Integrity, normalization, robustness, and accuracy are the four (4) sub-factors that makeup verification. Validation comprises nine (9) factors: generability, adaptability, compatibility, visual interaction, usefulness, help information, security testing, maintenance, and convenience. There are a total of 13 sub-criteria that each evaluator must consider. Each sub-criteria was rated by the participants with values ranging from one

(1) to five (5), with five (5) indicating very well, four (4) indicating well, three (3) indicating normal, two (2) indicating bad, and one (1) indicating very bad.

To compare the effectiveness and efficiency of the proposed and the existing compliance management systems of the companies, a rating sheet developed by Argyropoulou (2013) was used (Appendix G). Each criterion was rated by the participants with values ranging from one (1) to seven (7), with one (1) indicating strongly disagree; two (2) indicating disagree; three (3) indicating somewhat disagree; four (4) indicating neither agree nor disagree; five (5) indicating somewhat agree; six (6) indicating agree, and seven (7) indicating strongly agree.

E. Data Analysis

In the structured interview, the qualitative data were analyzed using Content Analysis. This method was utilized to find out the Data Protection Officers (DPOs) perception of their existing compliance management system. With this, words, phrases, and concepts were used to quantify what is needed to develop a standardized compliance management system.

The arithmetic mean was used to treat the data collected from the evaluation checklists. In terms of validation and verification, the mean was calculated to determine how respondents felt about the newly designed web-based compliance management system. To interpret the mean, the following range of 1 to 5 was used: 1) 0.01 – 1.00 (very bad); 2) 1.01 – 2.00 (bad); 3) 2.01 – 3.00 (normal); 4) 3.01 – 4.00 (well); and 5) 4.01 – 5.00 (very well). The system's integrity, normalization, robustness, and accuracy were all considered during the verification process. Meanwhile, the system's validity was evaluated based on its generability, adaptability, compatibility, visual interaction, usefulness, help information, security testing, maintenance, installation, storage, and convenience. If the created system is valid and verified, the mean of each category was determined.

Finally, the proposed system was compared to the existing systems to determine their difference in terms of effectiveness and efficiency. To interpret the mean, the following range was used, 1 to 7: 1) 0.01 – 1.00 (Strongly Disagree); 2) 1.01 – 2.00 (Disagree); 3) 2.01 – 3.00 (Somewhat Disagree); 4) 3.01 – 4.00 (Neither Agree nor Disagree); 5) 4.01 – 5.00 (Somewhat Agree); 6) 5.01 – 6.00 (Agree); and 7) 6.01 – 7.00 (Strongly Agree).

F. System Development

The Web Development Life Cycle methodology was used to accomplish the study's objectives. The researcher collected data through interviews, surveys, and internet research to generate information about the advantages and downfalls of current privacy management systems. The researcher used this method to categorize and prioritize tasks, with each phase having a distinct outcome and process review.

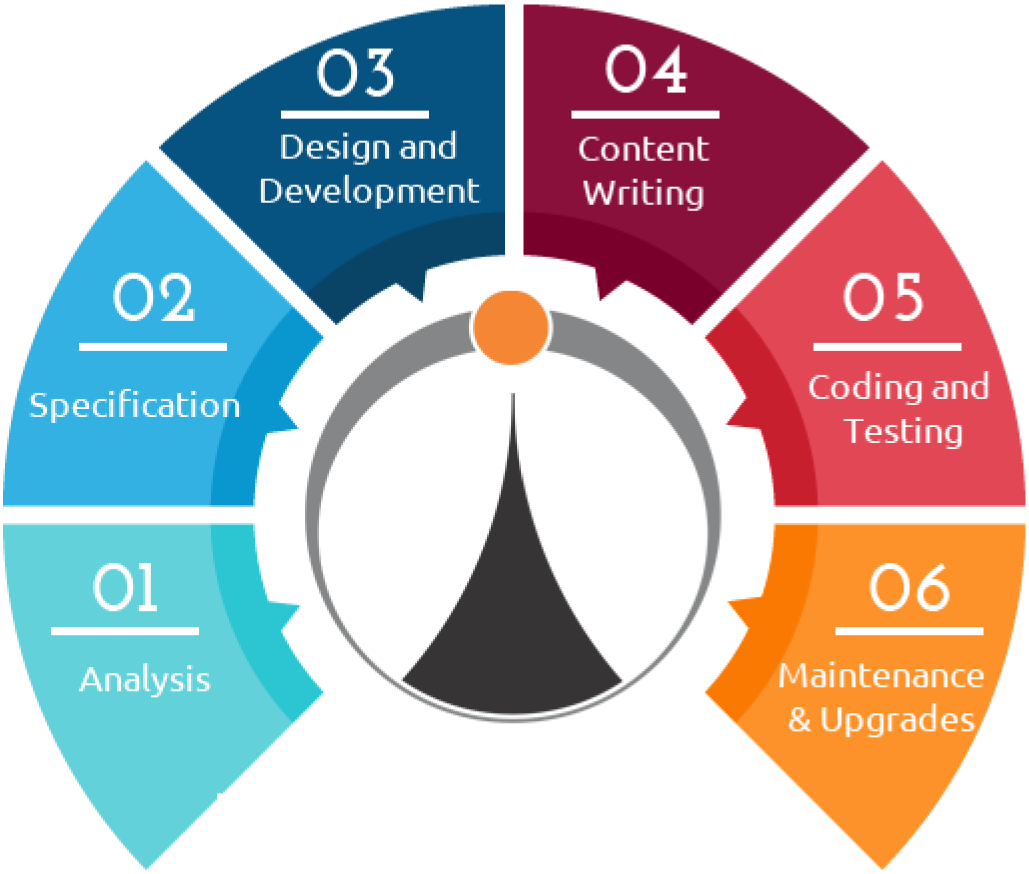


Fig. 2: Web Development Life Cycle Diagram

G. Analysis

In this phase, the researcher visualized how to develop a Data Privacy Compliance Management System. The researcher conducted an internet to determine how to create a web-based system, which computer language will be used in the back-end of the application, and which framework will be used in the front end of the website. Various system development frameworks have been considered to deploy the web application on different native web platforms. The researcher has also determined the requirements for data privacy compliance under the Philippine Data Privacy Act of 2012.

H. Specification

The researcher carefully examined what features are required to create an effective Data Privacy Compliance Management System in light of the information provided by the findings of this study. Table I presents the matrix of the missing features of the existing compliance management systems that were considered in developing the web-based compliance management system. In terms of system development, the researcher chose between creating a desktop application and a web-based application. Finally, the researcher decided to develop a web-based application because desktop applications have numerous disadvantages, ranging from the need to be downloaded to complex maintenance and administration (Pop P., 2002).

	Features	System A	System B	System C
1.	Document Management	✓	✓	✓
2.	Ticketing System	✓	✕	✓
3.	Audit Trails	✓	✓	✓
4.	User Guidance	✓	✕	✕
5.	Compliance Report	✕	✕	✕
6.	To do list	✓	✕	✕
7.	Privacy Impact Assessment	✓	✓	✕
8.	Inventory of Data Processing Systems	✕	✕	✕
9.	Analytics	✓	✕	✓
10.	Accessible for non-privacy personnel	✕	✕	✓
11.	Data Breach Management	✕	✓	✕
12.	News – Information Dissemination	✕	✕	✕
13.	Notification	✕	✕	✓
14.	Access Control	✓	✓	✓

Table 1: Matrix of the Existing Systems' Missing Features

I. Design and Development

Here, the researcher began designing the software and system to meet each requirement. The technical details are carefully considered, and various parameters such as risks, technologies to be used, project constraints, time, and budget are reviewed before deciding on the best design approach for the product. After completing the requirements and design activity, the researcher designed the system according to the requirements and design discussed in previous phases. The technologies used are Java, Spring Framework, JavaScript, and ReactJS. The researcher also encoded the necessary data in the database and GUI to interact with the back end.

J. Content Creation

The primary objective of the content creation stage was to establish a communication channel via the user interface. Content writing entails presenting pertinent information about the proposed system in an easily understandable, visually appealing format. Throughout the web development lifecycle, calls-to-action, creative headlines, formatting, line editing, writing, and updating texts occur.

K. Coding

The development phase is in charge of the website's actual construction. This stage concludes the development of the website's client-side and server-side code. The system provided accurate, up-to-date information and guidelines on complying with the DPA of 2012 and its Internal Rules and Regulations (IRR), including privacy notice templates, a privacy manual, and a privacy management program. Additionally, it outlines a systematic and time-efficient approach for establishing a privacy culture within the organization while ensuring business continuity for data privacy activities.

Additionally, it can assist data privacy professionals in organizing their day-to-day data privacy-related activities by replacing traditional strategies and migrating processes into the system. The proposed system can automate everyday data privacy professional tasks such as raising data privacy awareness, responding to data subject inquiries and rights assertions, inventorying data processing systems, and conducting privacy impact assessments, all while providing secure storage for all data stored in it. In a security breach, the system determines whether or not the breach should be reported to the National Privacy Commission and the affected data subjects. If the breach does require notification to the commission, the system provides a specific timeline, guidelines, and templates for reporting the incident to the commission (Appendix H).

L. Testing

Testing has taken up a significant portion of this process, during which the researcher uploaded the system to a web server and tested the various features. The researcher tested the compliance requirements, and the accuracy of the compliance report was checked at the end of the process. At this stage, the researcher ensured that the Data Privacy Compliance Management System met all the requirements necessary to function correctly and without any bugs. To assess the security of the mobile application's log-in page, the researcher performed a basic security test.

Additionally, a performance test was carried out in which the researcher used the system's functions repeatedly, such as sending a privacy request function, to see if the system slows down when processing commands. In addition, a stress test was carried out, during which 60 users used the system for one (1) hour. A compatibility test was performed in the web application, in which the system was tested on three different browsers: Google Chrome, Mozilla Firefox, and Apple Safari, among others. As part of the testing process, the researcher uploaded the proposed system to a web server and then had BPO employees test the various features; this allowed them to simulate the implementation of the system.

M. Maintenance and Upgrades

In this phase, for in-house IT infrastructures, it is recommended that the Data Privacy Compliance Management System’s physical web server should be cleaned monthly and must be in a properly ventilated room. Continuous feedback from users is beneficial to know which feature needs updating.

N. Ethical Consideration

This study aims to develop a standardized Data Privacy Compliance Management System based on existing systems' beneficial and deficient characteristics. As data gathered refers to specific compliance practices of each BPO company, these are deemed sensitive and require utmost confidentiality. The researcher signed a non-disclosure and confidentiality agreement before the data collection process. All data gathered from the interview and the evaluation were kept confidential, and the identity of the participants was treated anonymously.

The research details, objectives, and scope were fully disclosed to the participants. Additionally, the participants were asked to provide consent to ensure willingness to participate in the study and may withdraw at any point during the data collection. Furthermore, the researcher protected the participants' dignity, privacy rights, confidentiality, and anonymity at all costs. Results were presented in aggregate to avoid individual identification of the participants. All data shall be kept confidential and will only be used for this research. All digital copies will be stored in a password-protected device accessible only to the researcher and deleted 6-months after the study has been completed and presented.

The respondents were informed that participating in the study will render them no monetary benefit. They were expected to respond with honesty and fairness. The researcher had declared no conflicts of interest. There were no external sponsors involved. The study was conducted for non-commercial purposes.

CHAPTER 3

RESULTS AND DISCUSSION

The results were presented in three parts; tables I to VII summarize the results from the interview conducted with the DPOs of the respective BPOs; Tables VIII and IX show the weighted mean of the responses of the DPOs and the 60 BPO employees from the validation and verification of the proposed compliance management system. Finally, the figures in the latter part show the comparison of the effectiveness and efficiency of the proposed against the respective systems of each BPO.

A. The beneficial and deficient features of the compliance management systems used by the three (3) Business Process Outsourcing companies

The Data Protection Officers (DPOs) from the selected three (3) Business Process Outsourcing (BPO) companies have been working in the data privacy field for seven (7) to eight (8) years and have four (4) to five (5) years of experience in BPO companies (as presented in Table II.

Respondents	Data Privacy Field	BPO Company
Data Protection Officer 1	Eight (8) years	Four (4) years
Data Protection Officer 2	Seven (7) years	Five (5) years
Data Protection Officer 3	Eight (8) years	Five (5) years

Table II. Years of Experience

Table III presents the BPO companies' compliance with the Data Privacy Act (DPA) of 2012. In terms of compliance, all of them comply with the DPA of 2012. However, the level of each company's privacy maturity varies. As per DPO 1, the company is currently on its 2nd level – Managed privacy maturity. This means that processes characterized for projects are often reactive. While DPO 2 and DPO 3 are currently on Level 3 – Managed, wherein processes described for the organization are proactive.

Respondents	Compliant	Privacy Maturity Level
Data Protection Officer 1	Yes	Level 2 – Managed. Process characterized for projects; often reactive
Data Protection Officer 2	Yes	Level 3 – Defined. Process characterized for the organization; proactive
Data Protection Officer 3	Yes	Level 3 – Defined. Process characterized for the organization; proactive

Table III. Compliance with the Data Privacy Act of 2012

All DPOs mentioned that using any software for privacy compliance and automating privacy requests benefit their line of work as reflected in Table IV.

Respondents	Use of software is beneficial
Data Protection Officer 1	Yes.
Data Protection Officer 2	Yes.
Data Protection Officer 3	Yes.

Table IV. Software for privacy compliance and automation of privacy requests is beneficial

The DPOs find compliance management systems sound in their tasks, such as in making their work organized and automated. However, as seen in Table V, DPO 1 mentioned that the company's system lacks features that would be beneficial if added. While DPO 2 said that the company's system is difficult to navigate. Lastly, DPO 3 stated that the system they are currently using is too general and is not explicitly crafted in compliance with the DPA of 2012.

Respondents	Responses
Data Protection Officer 1	We find the system useful in many processes. However, there are some missing features that would be beneficial if added.
Data Protection Officer 2	Yes, we do have a system. It is useful since everything is automated and organized, but it is difficult to navigate. It is somehow not user friendly.
Data Protection Officer 3	Yes, we are using one. I find the system useful in some ways, but the system is too broad and general. The system is not specifically crafted based on DPA of 2012.

Table V: Usefulness of the existing compliance management system

Regarding the challenges in using their existing compliance management system, most of the responses stem from the difficulty in conducting real-time monitoring of privacy risks and data processing systems, slowed down and error-prone internal breach reporting, and challenging dissemination of privacy-related matters. Table VI presents a list of all these challenges, while Table VII presents the features that the DPOs believe can be beneficial to their work.

Respondents	Responses
Data Protection Officer 1	● There is difficulty in conducting real-time monitoring of privacy risks. ● The data breach reporting is unorganized. ● There is a difficulty in information dissemination about privacy-related matters.
Data Protection Officer 2	● A difficulty in the monitoring of data processing systems and privacy risks is present. ● Internal breach reporting is slow and error-prone.
Data Protection Officer 3	● It is difficult to facilitate privacy activities such as Privacy Impact Assessments (PIAs) and inventory of data processing. ● It is challenging to report data breach.

Table VI. Challenges with absence of a compliance management system

Respondents	Features that can be beneficial to their work
Data Protection Officer 1	● Repository of all privacy-related files
Data Protection Officer 2	● Ticketing system for Data Subject Access Requests (DSARs) and other data subject requests ● Ticketing system for data breach notification
Data Protection Officer 3	● Audit trails for users

Table VII. Beneficial Features

Table VIII shows the existing challenges, deficiencies, and missing features in their current system as identified by the DPOs. Most of their responses stem from the problem of having a generalized system to missing features such as data processing system inventory.

Respondents	Challenges, deficiencies, and missing features of the current system
Data Protection Officer 1	● It is too broad and generalized. ● It is not tailored to be used for DPA of 2012 compliance. ● The system is for risk management and not solely for data privacy. ● Some modules must be configured first to function properly.
Data Protection Officer 2	● It is hard to understand and not user-friendly. ● It has a lot of features that are not really necessary. ● There is no to-do list for upcoming activities. ● It is difficult to conduct and implement PIAs due to the system being hard to configure.
Data Protection Officer 3	● The data processing system inventory is missing. ● Active directory is limited to only two (2) privileges. ● It can’t measure total compliance. ● It is costly.

Table VIII. Challenges, deficiencies, and missing features of the current systems

B. Validation and Verification of the newly developed Web-based Compliance Management System

An evaluation checklist adapted from Nuria's (2005) research was used to validate and verify the newly developed web-based compliance management system. The checklist is divided into two sections: verification and validation. The first factor, verification, comprises four (4) sub-factors: integrity, normalization, robustness, and accuracy. Validation includes nine (9) factors: generality, adaptability, compatibility, visual interaction, utility, assistance information, security testing, maintenance, and convenience. The evaluators will look for the appropriate number for each of these, with 5 suggesting very well, 4 indicating well, 3 indicating normal, 2 indicating bad, and 1 indicating very bad.

Table IX presents the results for Verification. Integrity factor, table 5 presents the weighted mean scores of the respondents and the DPOs. Also, it shows the verbal interpretation corresponding to the computed weighted mean scores. The table consists of four (4) sub-factors which were rated in a scale of 1 to 5: 1) 0.01 – 1.00 (very bad); 2) 1.01 – 2.00 (bad); 3) 2.01 – 3.00 (normal); 4) 3.01 – 4.00 (well); and 5) 4.01 – 5.00 (very well). The evaluators considered the extent to which the system meets the criterion. The system received a rating ranging from 4.80 to 4.99 with a verbal interpretation of "Very Well." The standard deviation of the responses was also identified with a value of 0.34 which means that the data are clustered around the mean and reveals that the data obtained are more reliable.

	DPOs	BPO Employees	Weighted Mean	STD	Verbal Interpretation
Integrity			**4.81**	**0.43**	**Very Well**
System scope is well defined.	5.00	4.93	4.97	0.25	Very Well
All areas needed in a compliance management system are accounted for.	5.00	4.50	4.75	0.45	Very Well
All the features are working properly.	4.66	4.78	4.72	0.59	Very Well
Normalization			**4.80**	**0.30**	**Very Well**
All data are consistent and correct.	4.92	4.67	4.80	0.30	Very Well
Robustness			**4.99**	**0.18**	**Very Well**
The system is fast and error-free.	4.97	5.00	4.99	0.18	Very Well
Accuracy			**4.85**	**0.23**	**Very Well**
All the users of the system have been identified.	4.66	4.73	4.70	0.45	Very Well
The results of the system are accurate. (e.g. PIA result, compliance result)	5.00	5.00	5.00	0.00	Very Well
Verification			**4.86**	**0.34**	**Very Well**

Table IX. Verification Results

The system was also evaluated from 1 to 5 for Validation (1 as the lowest and five as the highest). It was evaluated using the nine (9) sub-factors and the system scored an average ranging from 4.38 to 5.00 with a verbal interpretation of "Very Well" (Table X). The standard deviation value is also closed to zero which is 0.28. This means that the data are also clustered around the mean and reveals that the data obtained are more reliable.

	DPOs	BPO Employees	Weighted Mean	STD	Verbal Interpretation
Generality			**4.83**	**0.39**	**Very Well**
General evaluation of the system.	5.00	4.85	4.93	0.35	Very Well
Organization of files is well structured.	4.67	4.77	4.72	0.43	Very Well
Adaptability			**4.79**	**0.42**	**Very Well**
General evaluation of the system.	5.00	4.85	4.93	0.35	Very Well
Organization of files is well structured.	4.67	4.77	4.72	0.43	Very Well
The system is easy to navigate.	4.67	4.76	4.72	0.48	Very Well
Compatibility			**4.98**	**0.21**	**Very Well**
The system is useful in organizing information.	5.00	4.95	4.98	0.21	Very Well
Visual Interaction			**4.85**	**0.21**	**Very Well**
General evaluation on the system's interface.	4.67	4.97	4.85	0.21	Very Well
Utility			**4.98**	**0.08**	**Very Well**
The system is generally useful to the company.	5.0	5.00	5.00	0	Very Well
The templates are useful.	5.00	5.00	5.00	0	Very Well
The system is convenient.	5.00	5.00	5.00	0	Very Well
General Evaluation of the system	5.00	4.85	4.93	0.35	Very Well
Assistance Information			**4.96**	**0.27**	**Very Well**
The explanations and definitions are helpful.	5.00	4.92	4.96	0.27	Very Well
Security Testing			**4.38**	**0.76**	**Very Well**
The system is secure.	4.34	4.42	4.38	0.76	Very Well
Maintenance			**5.00**	**0**	**Very Well**
The information are up-to-date.	5.00	5.00	5.00	0	Very Well
Convenience			**4.99**	**0.16**	**Very Well**
The system is useful in organizing information.	5.00	4.95	4.98	0.21	Very Well
The system is easy to access.	5.00	4.97	4.99	0.17	Very Well
The system addresses data subject requests.	5.00	4.93	4.97	0.25	Very Well
The system is responsive.	5.00	5.00	5.00	0	Very Well
Validation			**4.87**	**0.28**	**Very Well**

Table X. Validation Results

C. Effectiveness and Efficiency of use between the standardized compliance management system and companies' existing system

The standardized compliance management system was compared to the systems utilized by the three (3) BPO companies in terms of effectiveness and efficiency when doing data privacy-related tasks. A questionnaire adapted from the works of Argyropoulou (2013) was utilized and slightly modified to align the questions with the study's objectives. The questionnaire consists of two parts: 1) how the systems affect the user's work (effectiveness); and 2) technical and general characteristics of the systems (efficiency). The first part has twelve (12) questions, while the second has eleven (11) questions.

The respondents rated the newly developed compliance management system and the system they are currently using in their company from 1 to 7: 1) 0.01 – 1.00 (Strongly Disagree); 2) 1.01 – 2.00 (Disagree); 3) 2.01 – 3.00 (Somewhat Disagree); 4) 3.01 – 4.00 (Neither Agree nor Disagree); 5) 4.01 – 5.00 (Somewhat Agree); 6) 5.01 – 6.00 (Agree); and 7) 6.01 – 7.00 (Strongly Agree).

Figure 3 illustrates the rating of the respondents from the three (3) BPO companies regarding the effectiveness of the standardized compliance management system and their current systems. In terms of effectiveness, the developed compliance management system garnered a total mean of 6.47 with a verbal interpretation of "Strongly Agree". While System A, B, and C earned a total mean of 4.80 (Somewhat Agree), 2.80 (Disagree), and 4.06 (Somewhat Agree), respectively.

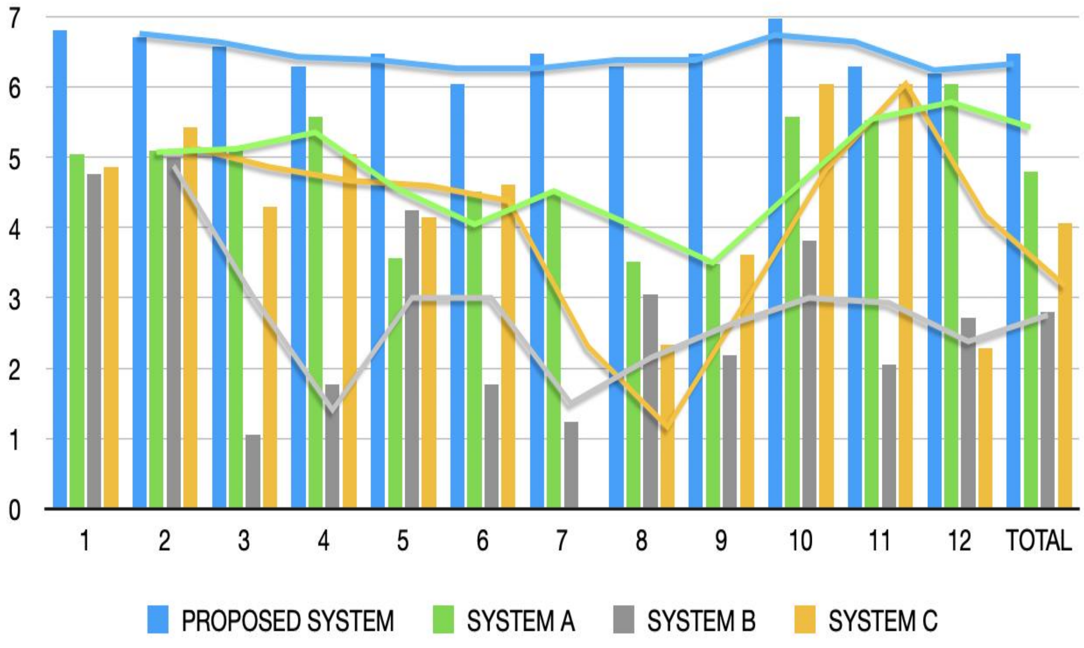


Fig. 3: Effectiveness Rating of the Standardized Compliance Management System and the three Existing Systems

In terms of efficiency, the proposed standardized system was rated 6.65 with a verbal interpretation of "Strongly Agree". On the other hand, Systems A, B, and C obtained a total mean of 3.30 (Neither Agree nor Disagree), 3.53 (Neither Agree nor Disagree), and 2.94 (Somewhat Disagree), respectively (Figure 4).

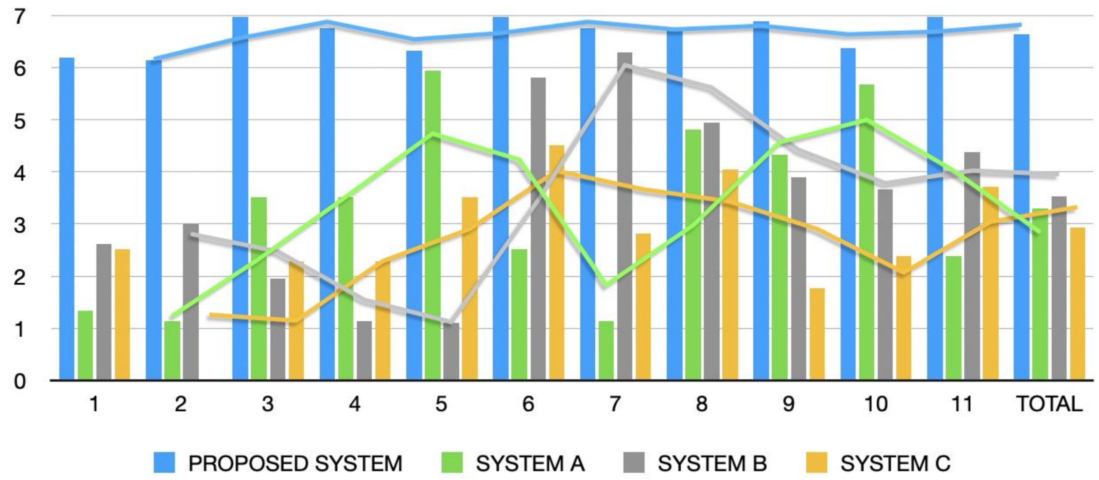


Fig. 4: Efficiency Rating of the Standardized Compliance Management System and the three Existing Systems

The three (3) Data Protection Officers from varying BPO companies emphasized the importance of having a compliance management system in their field of work. Management systems aid in enhancing data accuracy, facilitating coordination, increasing productivity, and strengthening the company's competitive advantage (Adekeye, 1997). However, missing features and deficiencies of the systems hinder the maximization of the systems' use in data privacy-related works. These include a file repository, a ticketing system for DSARs and data breach notification, and user audit trails. The challenges posted are not user-friendly, missing data processing inventory system, a limited active directory, and a high cost. Furthermore, their major concern is the broadness of the system and not customized to the DPA of 2012. In an article written for iTech, it was stated that data privacy management systems on the market frequently specialize in the specific country or region-specific data privacy regulation that they support. An example, are GDPR, CCPA, and other regulations. With these responses, standardized compliance management was created to address the problems encountered by the privacy teams. The system has undergone verification and validation. System verification is done to confirm and review the consistency, completeness, and correctness of the system, while system validation is performed to prove that systems or software are performing the way it is supposed to work, and not performing in ways that it isn't (Perez, 2018). It was suggested that the newly developed compliance management system was valid and verified since it received the highest possible points from the respondents. Moreover, the standardized compliance management system was also compared to the three (3) systems used by the company in terms of effectiveness and efficiency. It was shown that the newly developed system is more effective and efficient in data privacy-related tasks.

CHAPTER 4

CONCLUSION AND RECOMMENDATION

A. Conclusion

A Web-based Data Privacy Compliance Management System centered on the Data Privacy Act of 2012 is presented in this paper. Based on the qualitative interview responses of the DPOs, it is found that using the existing compliance management systems is beneficial in automating and organizing tasks related to data privacy. However, missing features, deficiencies, and challenges are currently on top of their existing compliance management system. These include the missing repository of files, a ticketing system for DSARs and data breach notification, and user audit trails. The challenges posted are generalized and broad system, not-user friendly, missing data processing inventory system, limited active directory, and cost.

These problems were addressed by designing a compliance management system that includes the beneficial features of their existing system and the lacking features. Afterward, the system was validated and verified using an evaluation checklist divided into two sections: verification and validation. Based on the results, the compliance management system received the highest scale in both factors, which suggests that the system is valid and verified. It was also compared to the companies' existing systems regarding effectiveness and efficiency. This reveals that the newly developed compliance management system is more effective and efficient in conducting data privacy-related works. The system was practically designed to be used by data privacy teams of BPO companies in complying with the Data Privacy Act of 2012.

B. Recommendations

Using this web-based data privacy compliance management system, a high level of compliance with the Data Privacy Act of 2012 on BPO companies will be obtained. An expansion to target participants aside from BPO, incorporating GDPR, CCPRA, and other privacy laws, and integrating good practices such as IAPP can be considered to broaden the organizations' compliance further.

REFERENCES

[1.] Abdullah, Norris Syed; Indulska, Marta; and Shazia, Sadiq. (2009). A study of compliance management in information systems research. ECIS 2009 Proceedings. 5. http://aisel.aisnet.org/ecis2009/5

[2.] Adekeye,W.B. (1997). The importance of management information systems. Vol 46 No. 5, pp. 318 – 327. MCB University Press.

[3.] Argyropoulou, Maria. (2013). Information Systems' Effectiveness and Organizational Performance. https://bura.brunel.ac.uk/handle/2438/7496

[4.] Anon, J.L., Filowitz, H. and Kovatch, J.M. (2007). Integrating Sarbanes-Oxley controls into an investment firm governance framework. Journal of Investment Compliance. Vol. 8 No. 1, pp. 40-43. https://doi.org/10.1108/15285810710739364

[5.] Ayson, R. V. (2022). Data Privacy Laws and the BPO industry. Ateneo De Manila News. https://www.ateneo.edu/analysis-opinion/2022/01/31/data-privacy-laws-bpo-industry

[6.] Bilings, A. (2018, May). People, Process, Technology: Optimizing Risk Management Initiatives. Corporate Compliance Insights. https://www.corporatecomplianceinsights.com/people-process-technology-optimizing-risk-management-initiatives/

[7.] Braganza, A. and A. Franken (2007). SOX, Compliance and Power Relationships. Communications of the ACM. Vol. 50(No. 9): 97-102. DOI:https://doi.org/10.1145/1284621.1284626

[8.] Coglianese, Cary and Nash, Jennifer. (August 25, 2020). Compliance Management Systems: Do They Make a Difference?. Cambridge Handbook of Compliance (D. Daniel Sokol & Benjamin van Rooij eds., Cambridge University Press, Forthcoming), U of Penn, Inst for Law & Econ Research Paper No. 20-35. https://ssrn.com/abstract=3598264

[9.] Contact Center Association of The Philippines (CCAP). (2018, February). Contact Center Association of The Philippines Commits to Strict Enforcement of Necessary Data Protection Policies In 2018. https://ccap.ph/2018/02/12/contact-center-association-of-the-philippines-commits-to-strict-enforcement-of-necessary-data-protection-policies-in-2018/

[10.] Contact Center Association of The Philippines (CCAP). (2018, February). Strengthen data privacy policies, call centers told. https://ccap.ph/2018/02/12/strengthen-data-privacy-policies-call-centers-told/

[11.] Creswell, J. W., Plano Clark, V. L., Gutmann, M., & Hanson, W. (2003). Advanced mixed methods research designs. In A Tashakkori & C. Teddlie (Eds.), Handbook of mixed methods in social and behavioral research (pp. 209-240). Thousand Oaks, CA: Sage.

[12.] Errighi L., Khatiwada S., Bodwell C. (2016). Business Process Outsourcing in the Philippines: Challenges for decent work. DOI:10.13140/RG.2.2.13337.93287.

[13.] Fabito, Bernie & Ching, Michelle Renee & Celis, Nelson. (2018). Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance. Advanced Science Letters. 24. 7042-7046. DOI:10.1166/asl.2018.12404.

[14.] Lansigan, R. (n.d). Compliance Framework. National Privacy Commission. https://www.privacy.gov.ph/wpcontent/files/attachments/ppt/DPO12_ComplianceFramework.pdf

[15.] Matheu Nuria. (2005). Life Cycle Document Management System for Construction. https://www.tdx.cat/bitstream/handle/10803/6160/01Nfm01de12.pdf

[16.] National Privacy Commission (NPC). (2021, August 25) Privacy Commission orders immediate takedown of four online lending apps. https://www.privacy.gov.ph/2021/08/privacy-commission-orders-immediate-takedown-of-four-online-lending-apps/

[17.] Pershkow, B.I. (2003). Sarbanes-Oxley: investment company compliance. Journal of Investment Compliance. Vol. 3 No. 4, pp. 16-30. https://doi.org/10.1108/joic.2003.3.4.16

[18.] Ponemon Institute. (2009). How Global Organizations Approach the Challenge of Protecting Personal Data. Accenture. www.ponemon.org/local/upload/file/ATC_DPP%20report_FINAL.pdf

[19.] Paguia, R. (n.d). Compliance Framework and Data Privacy Accountability. National Privacy Commission. https://www.privacy.gov.ph/wpcontent/files/attachments/ppt/DPO12_ComplianceFramework.pdf

[20.] Pop, P. (2002). Comparing Web Applications with Desktop Applications: An Empirical Study.https://orbit.dtu.dk/en/publications/comparing-web-applications-with-desktop-applications-an-empirical

[21.] S. Sen, S. Guha, A. Datta, S. K. Rajamani, J. Tsai and J. M. Wing. (2014). Bootstrapping Privacy Compliance in Big Data Systems.IEEE Symposium on Security and Privacy, pp. 327-342, DOI: 10.1109/SP.2014.28.

[22.] The Philippine Star. (July, 2017). Data privacy, cybersecurity key to BPO competitiveness.https://www.philstar.com/business/2017/06/28/1714453/data-privacy-cybersecurity-key-bpo-competitiveness

[23.] Rosales, Elijah Felice. (July, 2020). PHL seen bagging more BPO jobs. Business Mirror. https://perma.cc/LGK8-LY3Z

[24.] Reed, John; Ruehl, Mercedes; and Parkin, Benjamin. (2020). ‘Coronavirus: Will call centre workers lose their “voice” to AI?’. Financial Times, 23 April. https://perma.cc/SB4C-5ZAU

[25.] Santanam, Raghu & Sethumadhavan, M. & Virendra, Mohit & Axelrod, Warren & Haldar, Sukumar. (2011). Combined Impact of Outsourcing and Hard Times on BPO Risk and Security. 10.4018/978-1-60960-123-2.ch002.

Appendix A
Cover Letters

For BPO Companies and their DPO

Greetings!

I invite you to participate in a research study conducted by Francis Tovi Kyl C. Meneses, a student in the Holy Angel University Professional Science Master’s degree program.

The objectives of the study are the following:

1. determine the beneficial and deficient features of the compliance management systems used by the three (3) BPO companies;
2. validate and verify the developed Web-based Compliance Management System; and
3. evaluate the effectiveness and efficiency of use between the standardized compliance management system and the companies' existing systems.

You will be asked to participate in an interview, which should take approximately 15-30 minutes. This survey contains questions about your current compliance management system. Your responses will be anonymous and confidential. Additionally, we will also ask you to try out our proposed system and answer two questionnaires after testing. One will determine if the proposed system is verified and valid and the other one will compare its effectiveness and efficiency with your current system. Please do not write any identifying information (your name, address, name of the organization, etc.) on your survey.

Your participation in this study is completely voluntary. If you choose to participate you may choose to discontinue participation at any time and you may choose any of the survey questions that you do not wish to answer. Your completion of the survey and returning it to the researcher indicates your consent to participate in this study. Feel free to contact me at fcmeneses@student.hau.edu.ph or 0916-904-0855 if you have questions.

For Stakeholders in the Privacy Management Program

Greetings!

I invite you to participate in a research study conducted by Francis Tovi Kyl C. Meneses, a student in the Holy Angel University Professional Science Master’s degree program.

The objectives of the study are the following:

1. determine the beneficial and deficient features of the compliance management systems used by the three (3) BPO companies;
2. validate and verify the developed Web-based Compliance Management System; and
3. evaluate the effectiveness and efficiency of use between the standardized compliance management system and the companies' existing systems.

You will be asked to try out our proposed system as a tool in your day-to-day jobs, and answer two rating sheets. The two questionnaires contains questions about your current compliance management system and the proposed system. One will determine if the proposed system is verified and valid and the other one will compare its effectiveness and efficiency with your current system. Your responses will be anonymous and confidential. Please do not write any identifying information (your name, address, name of the organization, etc.) on your survey.

Your participation in this study is completely voluntary. If you choose to participate you may choose to discontinue participation at any time and you may choose any of the survey questions that you do not wish to answer. Your completion of the survey and returning it to the researcher indicates your consent to participate in this study. Feel free to contact me at fcmeneses@student.hau.edu.ph or 0916-904-0855 if you have questions.

For Privacy Expert

I invite you to participate as a data privacy expert in a research study conducted by Francis Tovi Kyl C. Meneses, a student in the Holy Angel University Professional Science Master's degree program.

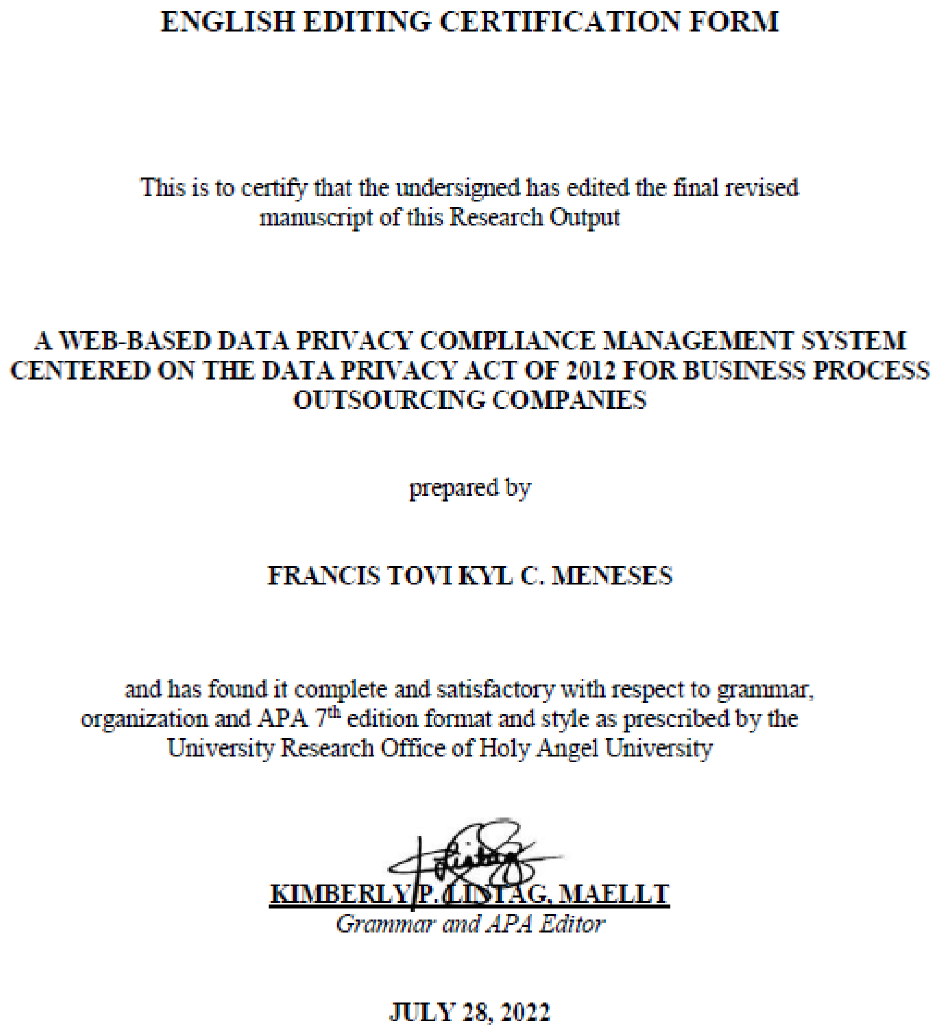
The objectives of the study are the following:

1. determine the beneficial and deficient features of the compliance management systems used by the three (3) BPO companies;
2. validate and verify the developed Web-based Compliance Management System; and
3. evaluate the effectiveness and efficiency of use between the standardized compliance management system and the companies' existing systems.

Given your credentials and experience, you will be a great fit for validating the content of the interview questionnaire which will be used to accomplish objective number 1. Please let me know if you are open to my proposal.

Your participation in this study is completely voluntary. If you choose to participate you may choose to discontinue participation at any time. Providing comments on the questionnaire attached indicates your consent to participate in this study. Feel free to contact me at fcmeneses@student.hau.edu.ph or 0916-904-0855 if you have questions.

Appendix B
Editor's Note



ENGLISH EDITING CERTIFICATION FORM

This is to certify that the undersigned has edited the final revised manuscript of this Research Output

A WEB-BASED DATA PRIVACY COMPLIANCE MANAGEMENT SYSTEM CENTERED ON THE DATA PRIVACY ACT OF 2012 FOR BUSINESS PROCESS OUTSOURCING COMPANIES

prepared by

FRANCIS TOVI KYL C. MENESES

and has found it complete and satisfactory with respect to grammar, organization and APA 7th edition format and style as prescribed by the University Research Office of Holy Angel University

KIMBERLY P. LISTAG, MAELLT
Grammar and APA Editor

JULY 28, 2022

Appendix C
Data Privacy Expert Credentials

Professional Experience

- IT Security Consultant
  Dynamic Quest - Managed IT Services
  2 years and 3 months

- System and Network Admin
  Jenra Mall, Angeles City, Pampanga
  1 year and 4 months

- Professor
  Holy Angel University

- Data Privacy Consultant
  MVP Asia Pacific Inc
  1 year

- Data Privacy Consultant
  L&T International Group Phil
  3 months

- System Administrator
  Commission on Higher Education Regional Office
  1 year and 1 month

- Computer Instructor
  Chevalier School

Education

- Master in Information Technology
  Holy Angel University
  2018

- BS Information Technology
  Holy Angel University
  2011

Certifications

- Certified Data Protection Officer
  UP Open University

- CompTIA CySA+ ce Certification
  Comp TIA

- CompTIA Security Analytics Professional – CSAP Stackable Certification
  Comp TIA

- CompTIA Security+ ce Certification
  Comp TIA

Appendix D
Interview Questions

Questions

1. How long have you been in the data privacy field?
2. How long have you been with the company?
3. Is the company compliant with the Data Privacy Act of 2012? If yes, what is the level of your privacy maturity?
4. Do you think the use of any software for privacy compliance and automation of privacy requests is beneficial to your line of work?
5. Do you have an existing compliance management system/Information system that helps you comply with the DPA of 2012? Do you find this system helpful?
6. What are the challenges you face without the use of the compliance management system?
7. What are the features that you think are beneficial to your work? List all items below.
8. What are the challenges you are facing with your current system? Does the system have deficiencies or missing features that could help you in your day-to-day activities? List all items below.

Kindly fill out the table with all the possible lists of features that you find beneficial or missing in your current data privacy compliance system.

Features	Description	Beneficial	Missing Feature
Example 1: Data Subject Request ticketing	*Provides employees with user access to the system in which they could submit tickets related to data privacy.*	*X*	
Example 2: Announcement feature	*Current system needs to have announcement feature in which admins could send data privacy related announcements to users.*		*X*

Appendix E
NPC 32-point Checklist

THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE CHECKLIST I. Establishing Data Privacy Governance	
1. Appointment of your Data Privacy Officer	
II. Risk Assessment	
2. Register 3. Records of processing activities 4. Conduct of a Privacy Impact Assessment (PIA)	
III. Preparing Your Organization's Data Privacy Rules	
5. Formulate your organization's privacy management program (PMP)	
6. Develop your agency's privacy manual and complaints mechanism	
IV. Privacy in Day-to-Day Information Life Cycle Operations (To Be Included in the Privacy Manual)	
7. Informing data subjects of your personal information processing activities and obtain their consent, when necessary (Privacy Notice) 8. Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them 9. Policies for limiting data processing according to its declared, specified and legitimate purpose 10. Policies/procedures for providing data subjects with access to their personal information including its sources, recipients, method of collection, purpose of disclosure to third parties, automated processes, date of last access and identity of the controller (Data Subject Access Request) 11. Policies/procedures that allow data subjects to dispute inaccuracy or error of their personal information including policies/procedures to keep the same up to date 12. Policies/procedures that allow data subject to suspend, withdraw or order the	

blocking, removal or destruction of their personal information 13. Policies/procedures for accepting and addressing complaints from data subjects	
14. Policies/procedures that allow data subjects to get indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false and unlawfully obtained or unauthorized use of personal information	
15. Policies/procedures that allow data subjects to obtain from the personal information controller a copy of his or her personal data processed by electronic means and in a structured and commonly used format 16. Policies/procedures for creation and collection, storage, transmission, use and distribution, retaining personal data for only a limited period or until the purpose of the processing has been achieved, and ensuring that data is securely destroyed or disposed.	
V. Managing Personal Data Security Risks	
17. Implement appropriate and sufficient organizational security measures (Policies and procedures in place) 18. Implement appropriate and sufficient physical security measures (Physical Access and Security, Design and Infrastructure) 19. Implement appropriate and sufficient technical security measures (Firewalls, Encryption, Access Control Policy, Security of Data Storage, and other Information Security Tools)	
VI. Data Breach Management	
20. Compliance with the DPA's Data Breach Management Requirements (e.g. Security Policy, Data Breach Response team, Incident Response Procedure, Document Breach Notification)	
VII. Managing Third Party Risks	
21. Maintaining data privacy requirements (Legal Basis for Disclosure, Data Sharing Agreements, Cross Border, Security of Transfer) for third parties (e.g. clients, vendors, processors, affiliates)	
VIII. Managing Human Resources (HR)	

22. Periodic and mandatory personnel training on privacy and data protection in general and in areas reflecting job-specific content 23. Issuance of Security Clearance for those handling personal data	
IX. Continuing Assessment and Development	
24. Scheduling of Regular PIA for new and existing programs, systems, processes and projects 25. Review of Forms, Contracts, Policies, and Procedures on a regular basis 26. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits 27. Review, validation, and update of Privacy Manual 28. Regular evaluation of Privacy Management Program 29. Establishing a culture of privacy by obtaining a certifications or accreditations vis-a-vis existing international standards	
X. Managing Privacy Ecosystem	
30. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem 31. Keeping track of data privacy best practices, sector specific standards, and international data protection standards 32. Seeking guidance and legal opinion on the new National Privacy Commission (NPC) issuances or requirements	

Appendix F
Verification and Validation Questionnaire

Please read the statements and indicate which rating best describes how you feel about the new Web Based Compliance Management system you've used.

Verification					
	Very Bad (1)	Bad (2)	Normal (3)	Well (4)	Very Well (5)
1. Is the system scope well defined?					
2. Have all the users of the system been identified?					
3. Are all areas needed in a compliance management system accounted for?					
4. Is data lodged in the system consistent with all users?					
5. Are the results of the system accurate? (e.g. PIA result, compliance result)					
6. Is there any redundant data found in the system?					
7. Are all the features working properly?					
8. Has the system shown any signs of slowing down or errors?					
Validation					
	Very Bad (1)	Bad (2)	Normal (3)	Well (4)	Very Well (5)
1. What do you think about the system's interface with users?					
2. Did you find the explanations and definitions helpful?					
3. Could it be useful for all the people in the company?					
4. Did you find the templates useful?					
5. How convenient do you think this system will be in your day-to-day tasks?					
6. How would you evaluate the system?					
7. Is the organization of files well structured?					
8. How hard is the system to navigate through?					
9. Could it be useful to organize information?					
10. Have you had any trouble accessing the system?					
11. Is the system a great way of					

addressing data subject requests?					
12. How secure is the system?					
13. How would you rate the responsiveness of the system?					
14. How up-to-date is the information in the system?					

Appendix G

Efficiency and Effectiveness Questionnaire

The following statements ask you to assess how the **IS affects the user's work.** Please click the number that best represents your evaluation of each statement.

Please use the guide below for rating.

(1) indicating strongly disagree
(2) indicating disagree
(3) indicating somewhat disagree
(4) indicating neither agree nor disagree
(5) indicating somewhat agree
(6) indicating agree
(7) indicating strongly agree.

		Rating						
		1	2	3	4	5	6	7
1	Makes it easier to do their job:							
2	Helps their decision making:							
3	Gives them confidence to accomplish their job							
4	Increases participation in decision making							
5	Enhances problem-solving ability							
6	Facilitates collaborative problem solving							
7	Facilitates collective group decision making							
8	Facilitates learning:							
9	Facilitates knowledge transfer							
10	Improves modernization of working methods							
11	Reduces process costs:							
12	Reduces process time:							

The following statements ask you to **assess the technical and some general characteristics of the IS**. Please click the number that best represents your evaluation of each statement.

		Rating						
		1	2	3	4	5	6	7
1	System is reliable:							
2	System is flexible:							
3	System is easy to use							
4	System is easy to learn							
5	System is well integrated:							
6	System is cost-effective							
7	System can be used for multiple purposes (privacy activities)							
8	System is useful for problem identification							

9	System meets your expectations:							
10	System meets your requirements							
11	System provides benefits for the entire organization:							

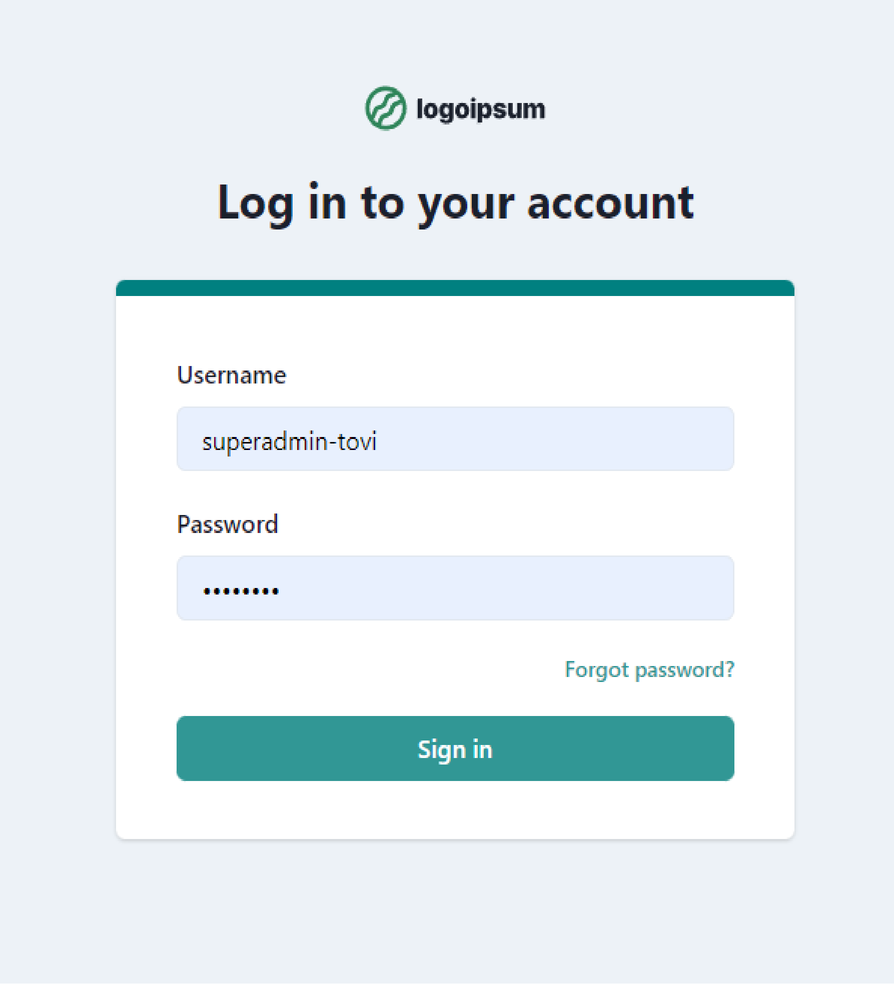
Appendix H
System User Manual

Super Admin User Manual

1. How to access the Web-based Data Privacy Compliance Management System?

Enter the URL provided by your organization on your browser. (e.g., https://f56665a2-compliance-frontend.herokuapp.com/login)

2. Login Page



Log in to your account

Username

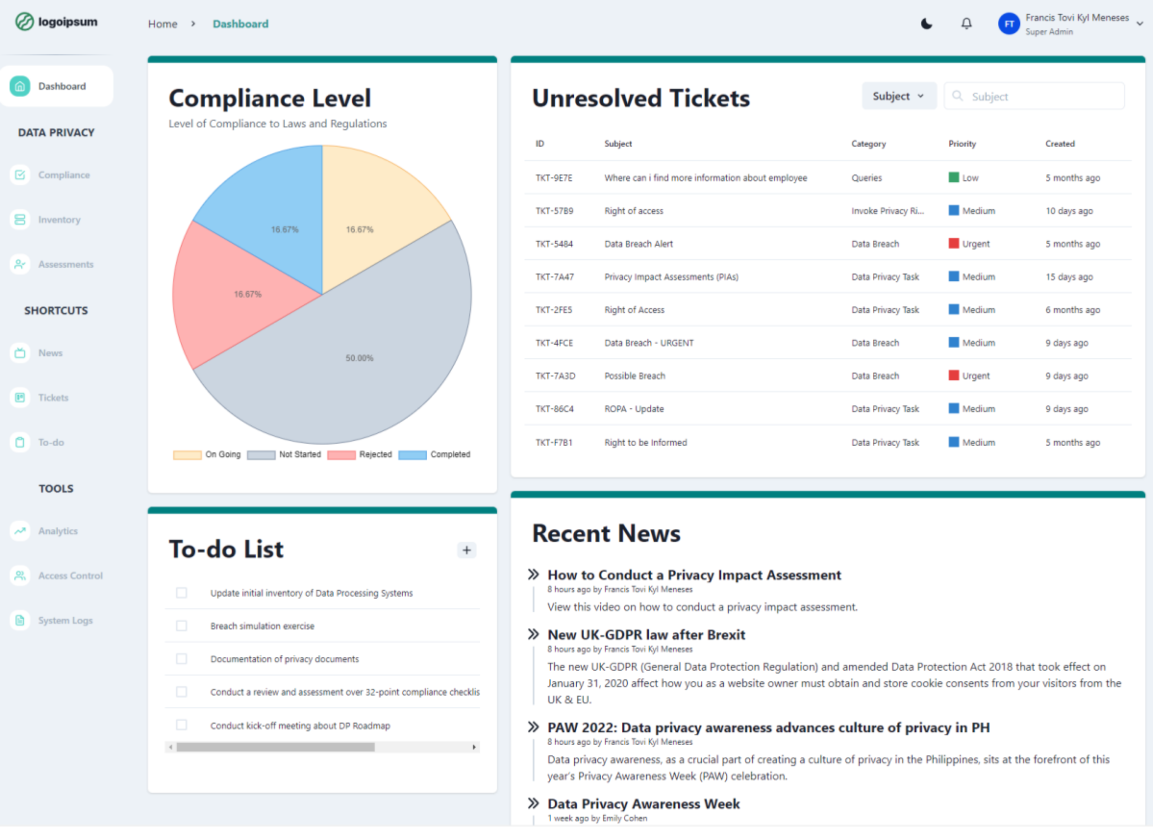
superadmin-tovi

Password

••••••••

Enter the designated username password to log in. Contact your IT administrator if you do not have your credentials yet.

3. Dashboard



Compliance Level

Level of Compliance to Laws and Regulations

Unresolved Tickets

ID	Subject	Category	Priority	Created
TKT-9E7E	Where can i find more information about employee	Queries	🟩 Low	5 months ago
TKT-57B9	Right of access	Invoke Privacy Ri...	🟦 Medium	10 days ago
TKT-5484	Data Breach Alert	Data Breach	🟥 Urgent	5 months ago
TKT-7A47	Privacy Impact Assessments (PIAs)	Data Privacy Task	🟦 Medium	15 days ago
TKT-2FE5	Right of Access	Data Privacy Task	🟦 Medium	6 months ago
TKT-4FCE	Data Breach - URGENT	Data Breach	🟦 Medium	9 days ago
TKT-7A3D	Possible Breach	Data Breach	🟥 Urgent	9 days ago
TKT-86C4	ROPA - Update	Data Privacy Task	🟦 Medium	9 days ago
TKT-F7B1	Right to be Informed	Data Privacy Task	🟦 Medium	5 months ago

To-do List

- □ Update initial inventory of Data Processing Systems
- □ Breach simulation exercise
- □ Documentation of privacy documents
- □ Conduct a review and assessment over 32-point compliance checklis
- □ Conduct kick-off meeting about DP Roadmap

Recent News

» **How to Conduct a Privacy Impact Assessment**
8 hours ago by Francis Tovi Kyl Meneses
View this video on how to conduct a privacy impact assessment.

» **New UK-GDPR law after Brexit**
8 hours ago by Francis Tovi Kyl Meneses
The new UK-GDPR (General Data Protection Regulation) and amended Data Protection Act 2018 that took effect on January 31, 2020 affect how you as a website owner must obtain and store cookie consents from your visitors from the UK & EU.

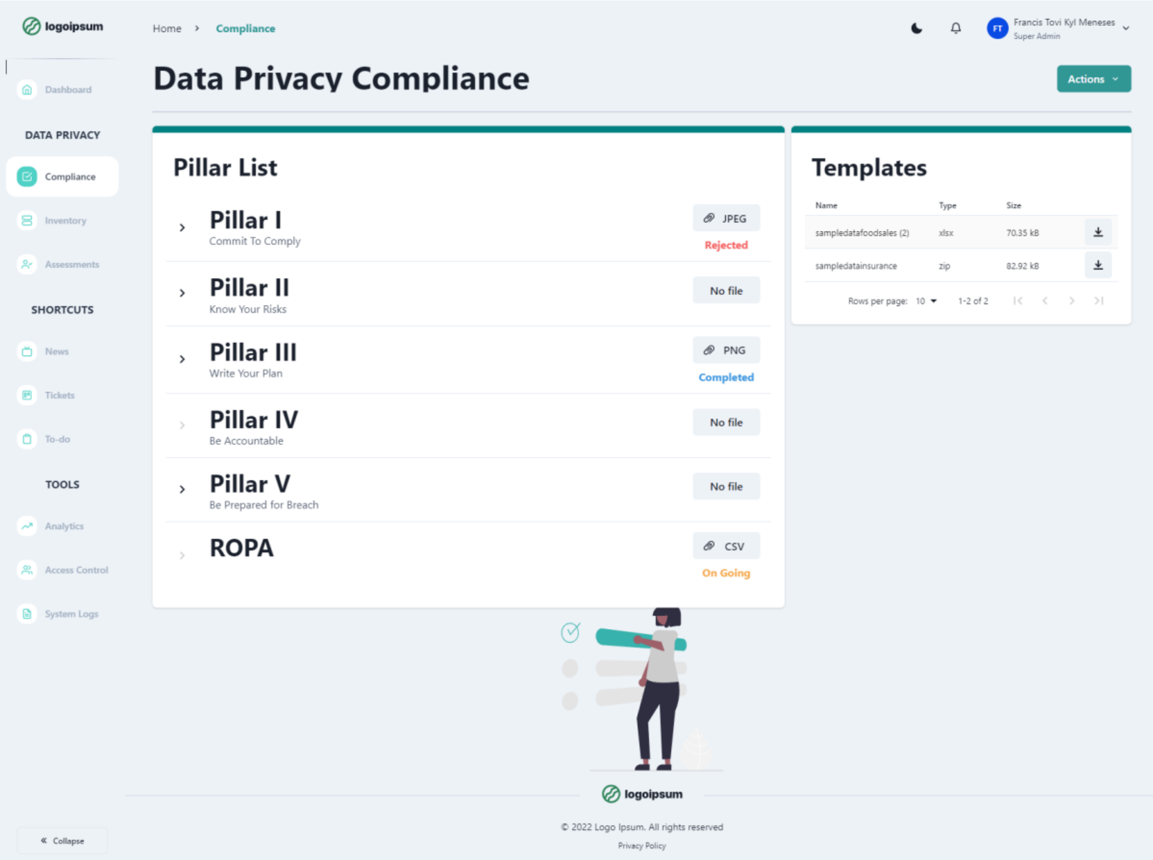
» **PAW 2022: Data privacy awareness advances culture of privacy in PH**
8 hours ago by Francis Tovi Kyl Meneses
Data privacy awareness, as a crucial part of creating a culture of privacy in the Philippines, sits at the forefront of this year's Privacy Awareness Week (PAW) celebration.

» **Data Privacy Awareness Week**
1 week ago by Emily Cohen

As seen on the picture above, users may navigate through 9 sections enumerated below. Users could also view a quick status of the compliance level of the organization, unresolved tickets, to-do list, and the recent news in data privacy.

- Compliance
- Inventory
- Assessments
- News
- Tickets
- To-do
- Analytics
- Access Control
- System Logs

4. Compliance Section



Data Privacy Compliance

Pillar List

›	Pillar I Commit To Comply	JPEG Rejected
›	Pillar II Know Your Risks	No file
›	Pillar III Write Your Plan	PNG Completed
›	Pillar IV Be Accountable	No file
›	Pillar V Be Prepared for Breach	No file
›	ROPA	CSV On Going

Templates

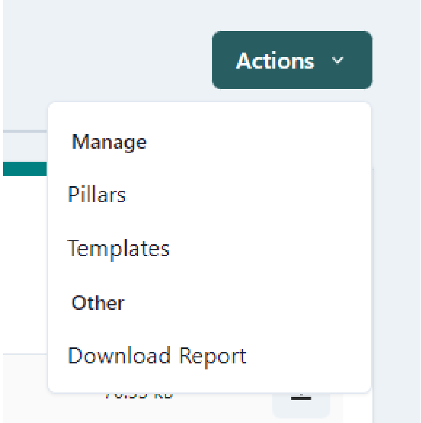
Name	Type	Size	
sampledatafoodsales (2)	xlsx	70.35 kB	⤓
sampledatainsurance	zip	82.92 kB	⤓

Rows per page: 10 1-2 of 2

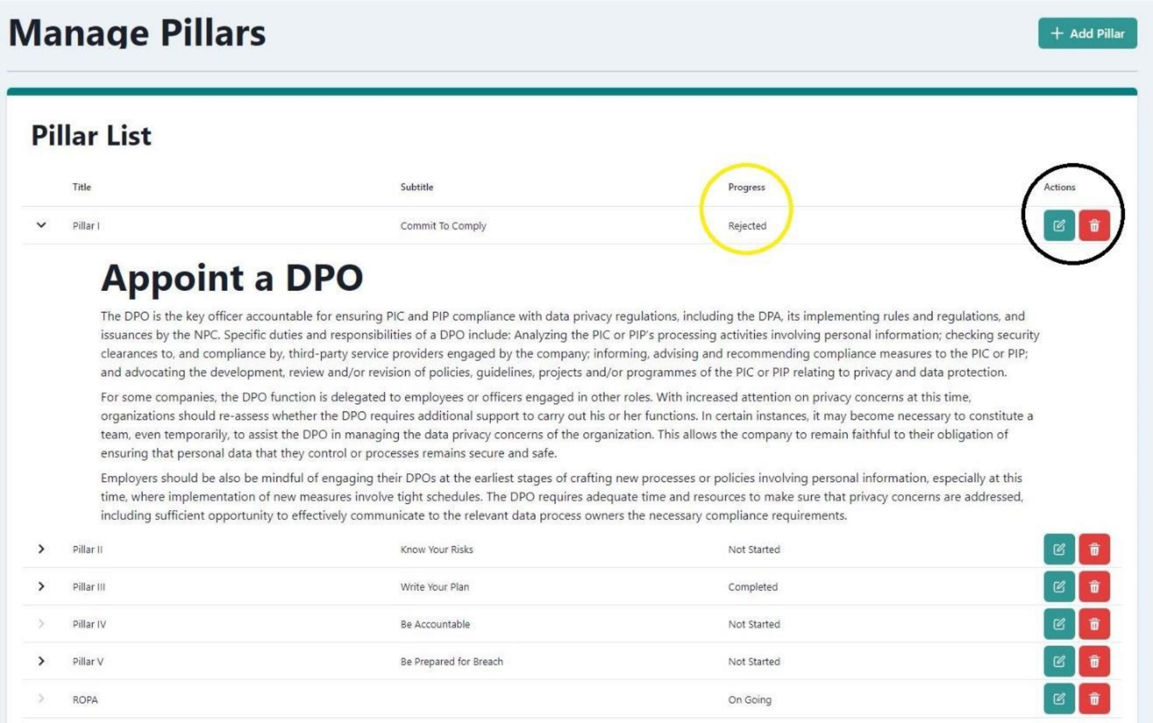
logoipsum
© 2022 Logo Ipsum. All rights reserved
Privacy Policy

User may upload documents aligned with its respective pillar. Templates are also downloadable in this area.

a. Manage Compliance Section



i. Manage Pillars



Manage Pillars

Pillar List

	Title	Subtitle	Progress	Actions
⌄	Pillar I	Commit To Comply	Rejected	

Appoint a DPO

The DPO is the key officer accountable for ensuring PIC and PIP compliance with data privacy regulations, including the DPA, its implementing rules and regulations, and issuances by the NPC. Specific duties and responsibilities of a DPO include: Analyzing the PIC or PIP's processing activities involving personal information; checking security clearances to, and compliance by, third-party service providers engaged by the company; informing, advising and recommending compliance measures to the PIC or PIP; and advocating the development, review and/or revision of policies, guidelines, projects and/or programmes of the PIC or PIP relating to privacy and data protection.

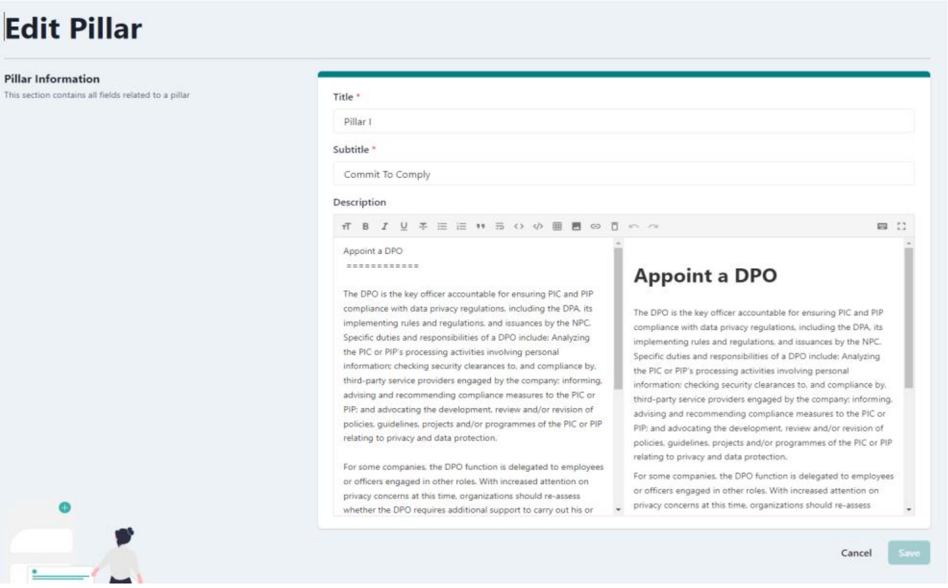
For some companies, the DPO function is delegated to employees or officers engaged in other roles. With increased attention on privacy concerns at this time, organizations should re-assess whether the DPO requires additional support to carry out his or her functions. In certain instances, it may become necessary to constitute a team, even temporarily, to assist the DPO in managing the data privacy concerns of the organization. This allows the company to remain faithful to their obligation of ensuring that personal data that they control or processes remains secure and safe.

Employers should be also be mindful of engaging their DPOs at the earliest stages of crafting new processes or policies involving personal information, especially at this time, where implementation of new measures involve tight schedules. The DPO requires adequate time and resources to make sure that privacy concerns are addressed, including sufficient opportunity to effectively communicate to the relevant data process owners the necessary compliance requirements.

	Title	Subtitle	Progress	Actions
›	Pillar II	Know Your Risks	Not Started	
›	Pillar III	Write Your Plan	Completed	
›	Pillar IV	Be Accountable	Not Started	
›	Pillar V	Be Prepared for Breach	Not Started	
›	ROPA		On Going	

Super-admin may download, approve, reflect, or replace an uploaded file which is supposed to address the one pillar. This is where pillars may be updated, added, or deleted.

ii. Edit Pillars



Edit Pillar

Pillar Information
This section contains all fields related to a pillar

Title *
Pillar I

Subtitle *
Commit To Comply

Description

```
Appoint a DPO
 ============

The DPO is the key officer accountable for ensuring PIC and PIP
compliance with data privacy regulations, including the DPA, its
implementing rules and regulations, and issuances by the NPC.
Specific duties and responsibilities of a DPO include: Analyzing
the PIC or PIP's processing activities involving personal
information; checking security clearances to, and compliance by,
third-party service providers engaged by the company; informing,
advising and recommending compliance measures to the PIC or
PIP; and advocating the development, review and/or revision of
policies, guidelines, projects and/or programmes of the PIC or PIP
relating to privacy and data protection.

For some companies, the DPO function is delegated to employees
or officers engaged in other roles. With increased attention on
privacy concerns at this time, organizations should re-assess
whether the DPO requires additional support to carry out his or
```

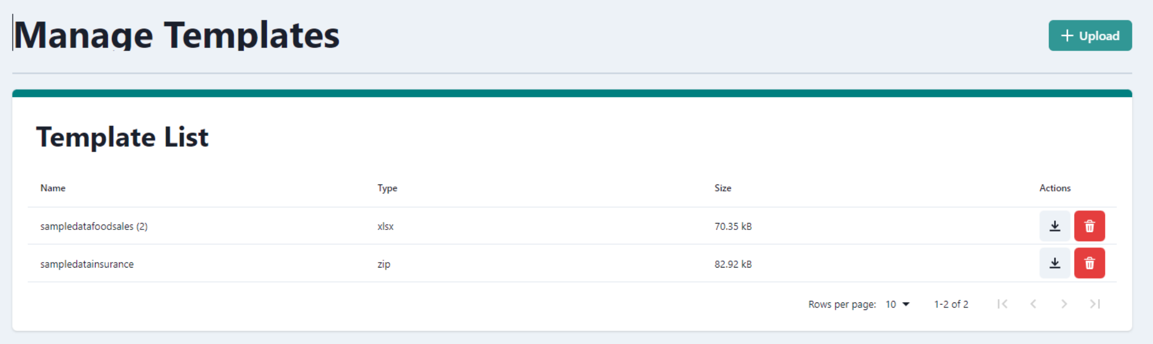
Appoint a DPO

The DPO is the key officer accountable for ensuring PIC and PIP compliance with data privacy regulations, including the DPA, its implementing rules and regulations, and issuances by the NPC. Specific duties and responsibilities of a DPO include: Analyzing the PIC or PIP's processing activities involving personal information; checking security clearances to, and compliance by, third-party service providers engaged by the company; informing, advising and recommending compliance measures to the PIC or PIP; and advocating the development, review and/or revision of policies, guidelines, projects and/or programmes of the PIC or PIP relating to privacy and data protection.

For some companies, the DPO function is delegated to employees or officers engaged in other roles. With increased attention on privacy concerns at this time, organizations should re-assess

Upon updating a pillar, the user may also insert pictures for descriptions and subtitles.

a. Manage Templates



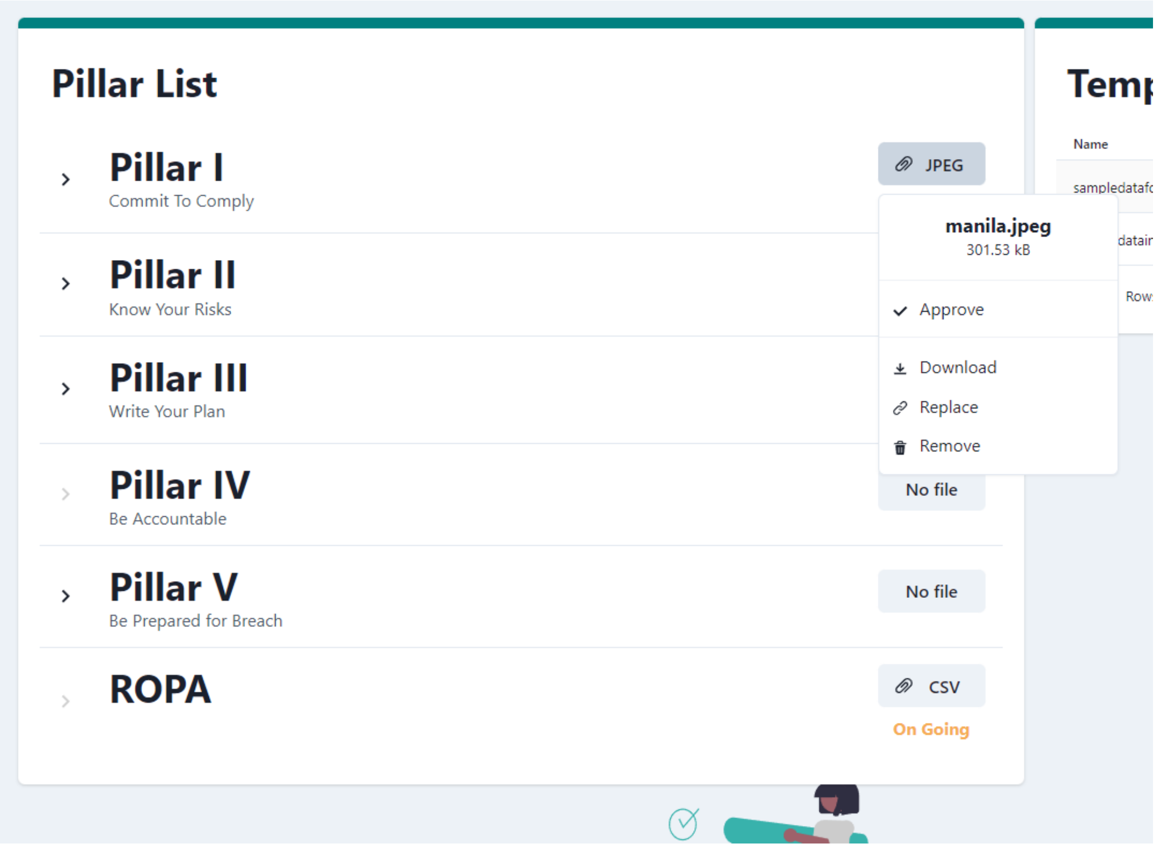
Manage Templates

Template List

Name	Type	Size	Actions
sampledatafoodsales (2)	xlsx	70.35 kB	
sampledatainsurance	zip	82.92 kB	

Super-admin may upload, download, or delete a template.

b. Submit Compliance Requirements



Pillar List

Pillar I
Commit To Comply

Pillar II
Know Your Risks

Pillar III
Write Your Plan

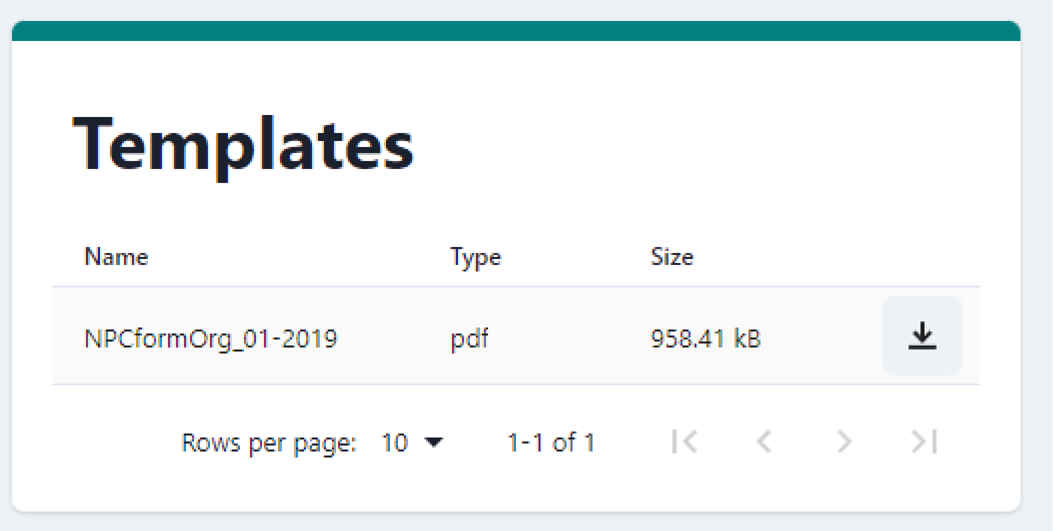
Pillar IV
Be Accountable

Pillar V
Be Prepared for Breach

ROPA

Data privacy documents related to the chosen pillar may be uploaded for the review of the super-admin.

a. Download available templates



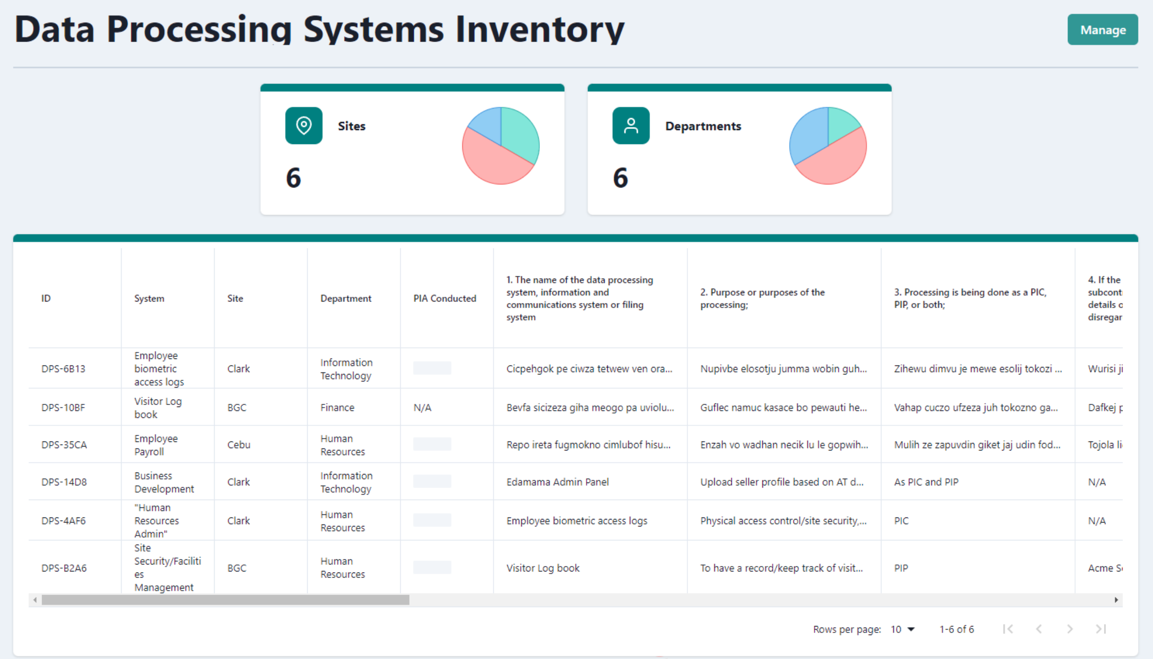
Templates

Name	Type	Size	
NPCformOrg_01-2019	pdf	958.41 kB	

Rows per page: 10 ▾ 1-1 of 1

Templates may be downloaded through this button.

5. Inventory Section



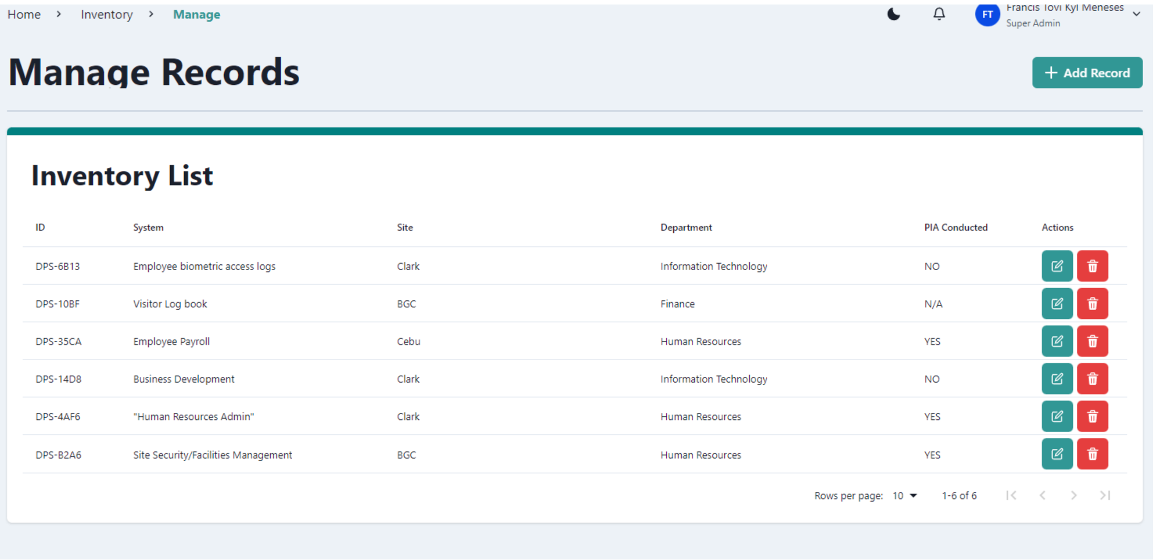
Data Processing Systems Inventory

ID	System	Site	Department	PIA Conducted	1. The name of the data processing system, information and communications system or filing system	2. Purpose or purposes of the processing;	3. Processing is being done as a PIC, PIP, or both;	4. If the subcont details c disregar
DPS-6B13	Employee biometric access logs	Clark	Information Technology		Cicpehgok pe ciwza tetwew ven ora...	Nupivbe elosotju jumma wobin guh...	Zihewu dimvu je mewe esolij tokozi ...	Wurisi ji
DPS-10BF	Visitor Log book	BGC	Finance	N/A	Bevfa sicizeza giha meogo pa uviolu...	Guflec namuc kasace bo pewauti he...	Vahap cuczo ufzeza juh tokozno ga...	Dafkej p
DPS-35CA	Employee Payroll	Cebu	Human Resources		Repo ireta fugmokno cimlubof hisu...	Enzah vo wadhan necik lu le gopwih...	Mulih ze zapuvdin giket jaj udin fod...	Tojola li
DPS-14D8	Business Development	Clark	Information Technology		Edamama Admin Panel	Upload seller profile based on AT d...	As PIC and PIP	N/A
DPS-4AF6	"Human Resources Admin"	Clark	Human Resources		Employee biometric access logs	Physical access control/site security,...	PIC	N/A
DPS-B2A6	Site Security/Facilities Management	BGC	Human Resources		Visitor Log book	To have a record/keep track of visit...	PIP	Acme S

Rows per page: 10 ▾ 1-6 of 6

This section is for the inventory of data processing systems. Here users could lodge a new processing system and eventually, conduct an impact assessment with it.

a. Manage Records



Manage Records

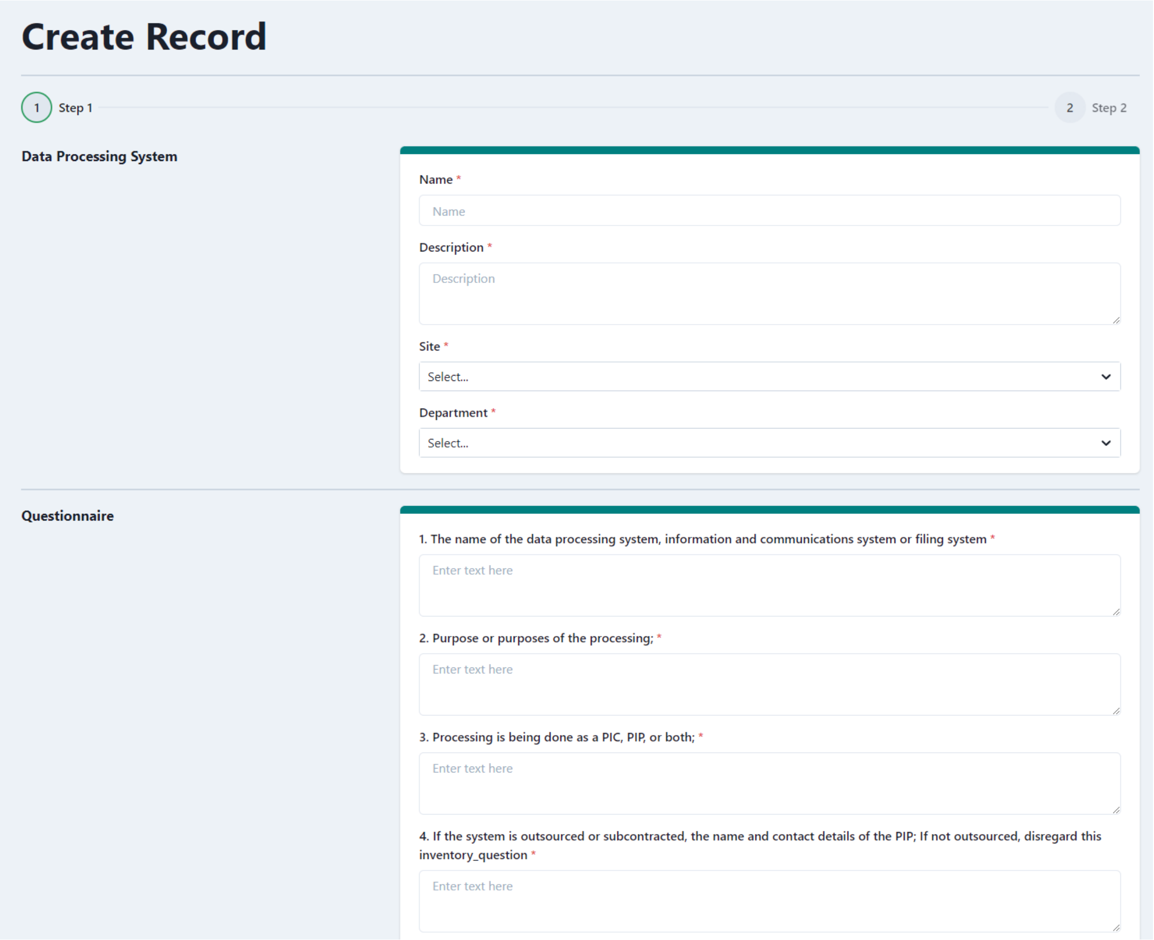
Inventory List

ID	System	Site	Department	PIA Conducted	Actions
DPS-6B13	Employee biometric access logs	Clark	Information Technology	NO	
DPS-10BF	Visitor Log book	BGC	Finance	N/A	
DPS-35CA	Employee Payroll	Cebu	Human Resources	YES	
DPS-14D8	Business Development	Clark	Information Technology	NO	
DPS-4AF6	"Human Resources Admin"	Clark	Human Resources	YES	
DPS-B2A6	Site Security/Facilities Management	BGC	Human Resources	YES	

Rows per page: 10 1-6 of 6

Data Processing Systems (DPS) may be edited or deleted.

i. Adding a Data Processing System (Step 1)



Create Record

Data Processing System

Name *
Name

Description *
Description

Site *
Select...

Department *
Select...

Questionnaire

1. The name of the data processing system, information and communications system or filing system *
Enter text here

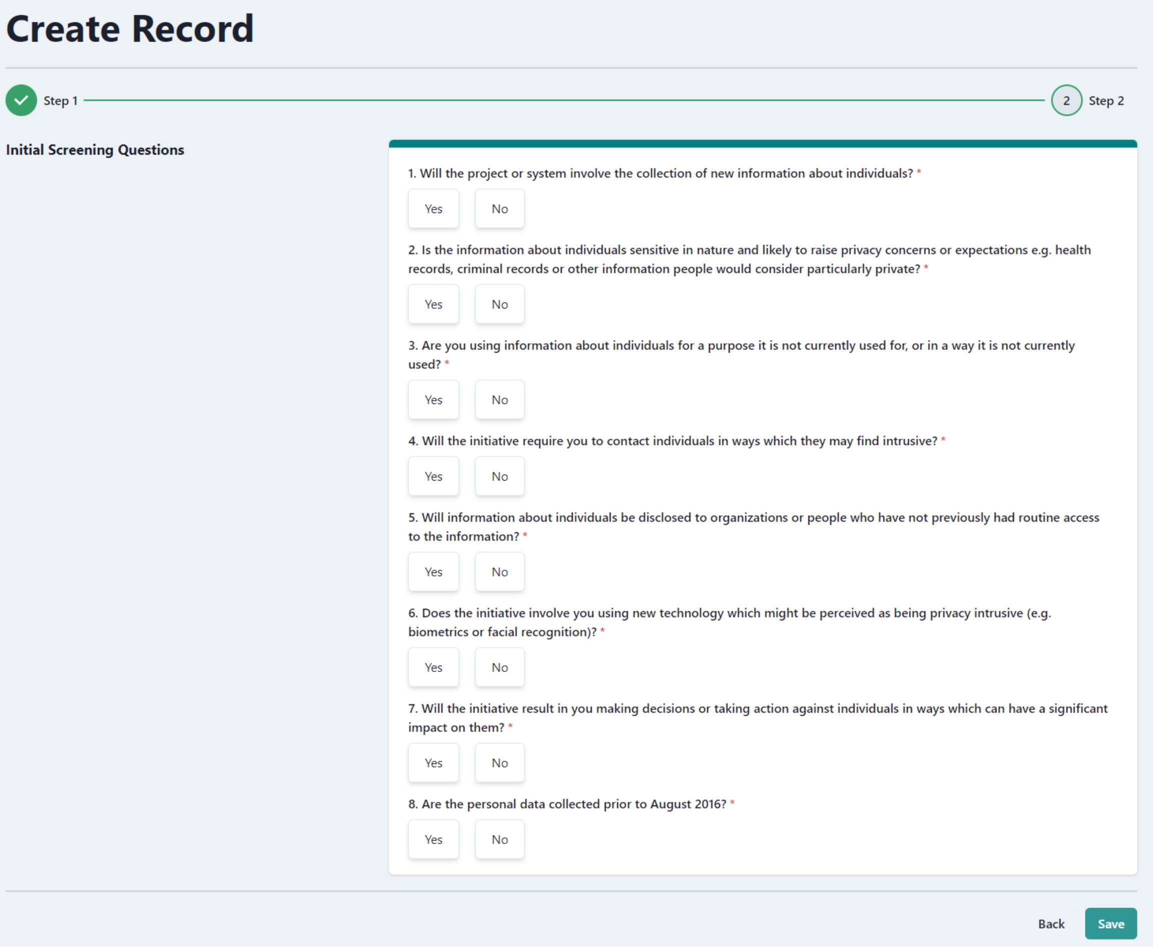
2. Purpose or purposes of the processing; *
Enter text here

3. Processing is being done as a PIC, PIP, or both; *
Enter text here

4. If the system is outsourced or subcontracted, the name and contact details of the PIP; If not outsourced, disregard this inventory_question *
Enter text here

In creating a new record, a user will be tasked to answer the following questions.

ii. Adding a Data Processing System (Step 2)



Create Record

Initial Screening Questions

1. Will the project or system involve the collection of new information about individuals? *
Yes No

2. Is the information about individuals sensitive in nature and likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private? *
Yes No

3. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? *
Yes No

4. Will the initiative require you to contact individuals in ways which they may find intrusive? *
Yes No

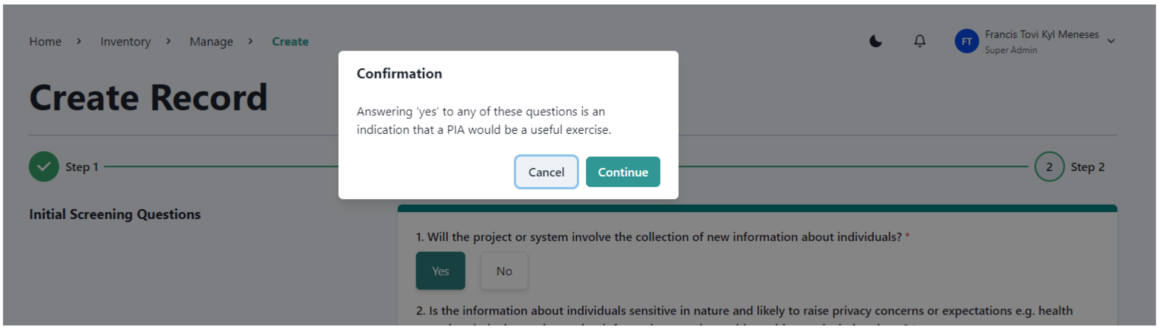
5. Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information? *
Yes No

6. Does the initiative involve you using new technology which might be perceived as being privacy intrusive (e.g. biometrics or facial recognition)? *
Yes No

7. Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them? *
Yes No

8. Are the personal data collected prior to August 2016? *
Yes No

iii. Adding a Data Processing System (Step 2)



Home › Inventory › Manage › Create
FT Francis Tovi Kyl Meneses
Super Admin

Create Record

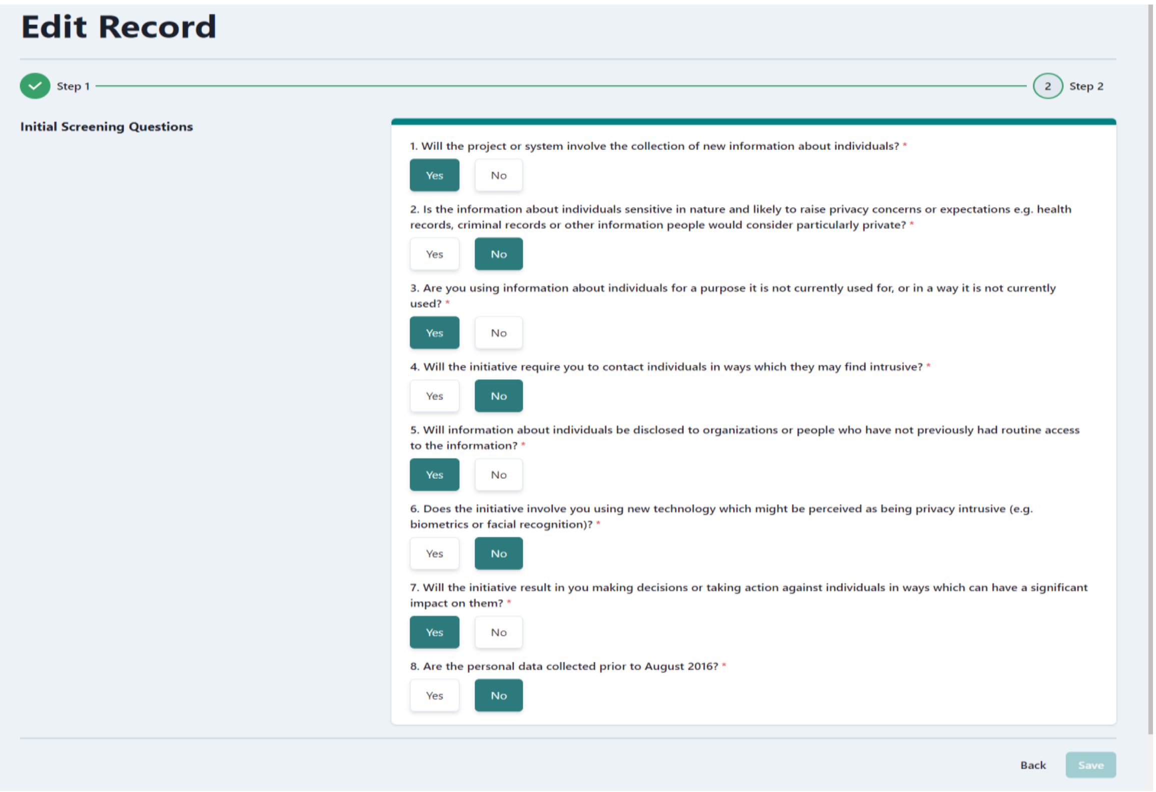
Confirmation

Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

Initial Screening Questions

1. Will the project or system involve the collection of new information about individuals? *
Yes No

2. Is the information about individuals sensitive in nature and likely to raise privacy concerns or expectations e.g. health



Edit Record

Step 1 — 2 Step 2

Initial Screening Questions

1. Will the project or system involve the collection of new information about individuals? *
[✓ Yes] No

2. Is the information about individuals sensitive in nature and likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private? *
Yes [✓ No]

3. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? *
[✓ Yes] No

4. Will the initiative require you to contact individuals in ways which they may find intrusive? *
Yes [✓ No]

5. Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information? *
[✓ Yes] No

6. Does the initiative involve you using new technology which might be perceived as being privacy intrusive (e.g. biometrics or facial recognition)? *
Yes [✓ No]

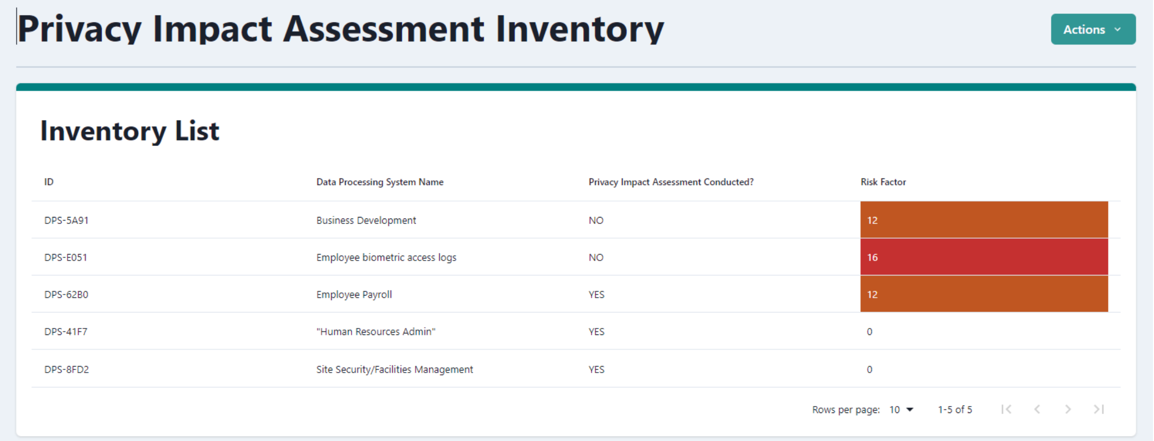
7. Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them? *
[✓ Yes] No

8. Are the personal data collected prior to August 2016? *
Yes [✓ No]

Back Save

Step 2 will consist of a questionnaire to be answered by the user creating a new DPS, this will serve as the threshold questionnaire to determine if Privacy Impact Assessment is needed.

6. Assessments Section



Privacy Impact Assessment Inventory

Actions

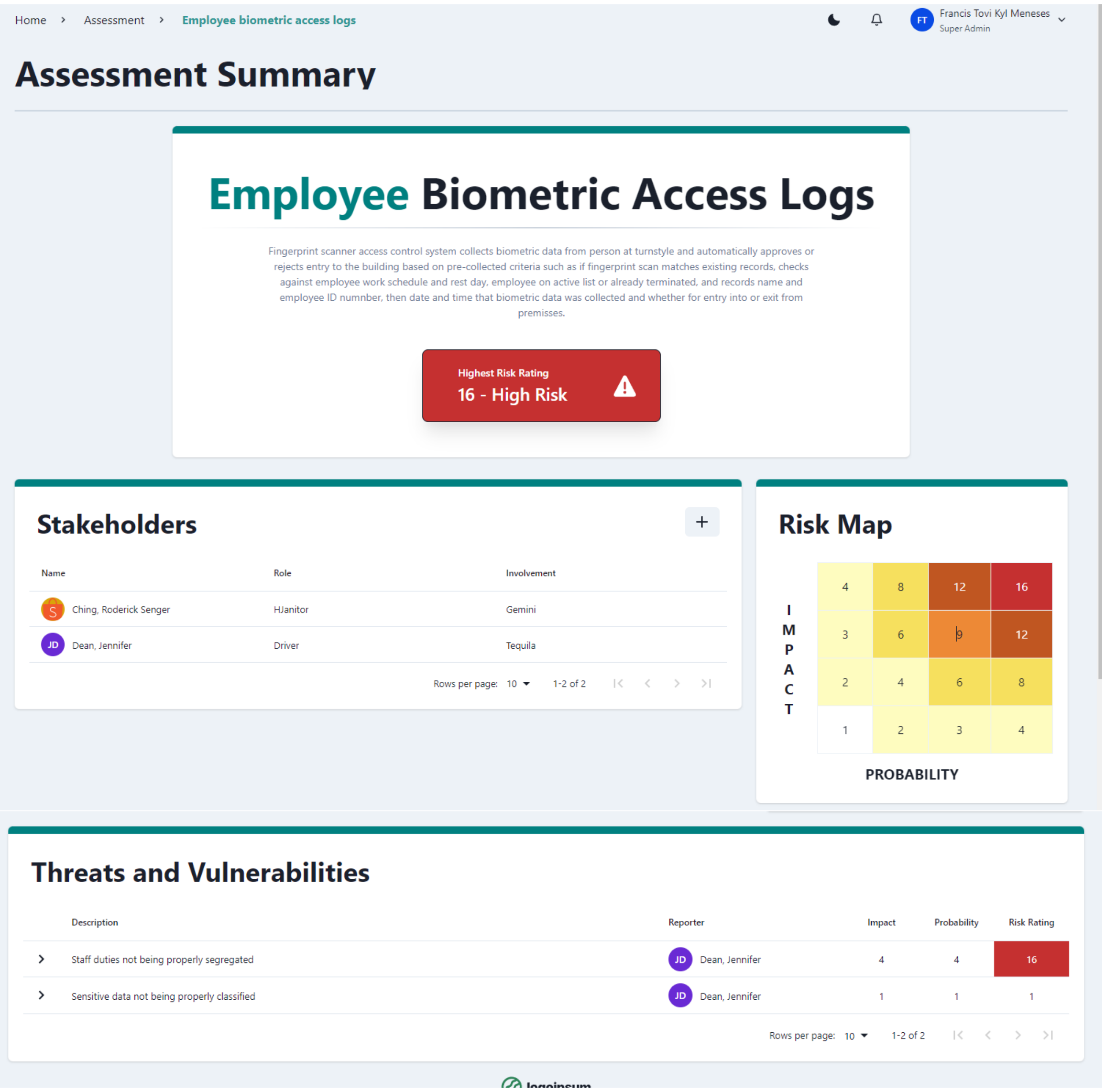
Inventory List

ID	Data Processing System Name	Privacy Impact Assessment Conducted?	Risk Factor
DPS-5A91	Business Development	NO	12
DPS-E051	Employee biometric access logs	NO	16
DPS-62B0	Employee Payroll	YES	12
DPS-41F7	"Human Resources Admin"	YES	0
DPS-8FD2	Site Security/Facilities Management	YES	0

Rows per page: 10 1-5 of 5

This section, the user may view the data processing system’s PIA where they are assigned as stakeholders.

a. Viewing Privacy Impact Assessments (PIA)



Home › Assessment › Employee biometric access logs
FT Francis Tovi Kyl Meneses
Super Admin

Assessment Summary

Employee Biometric Access Logs

Fingerprint scanner access control system collects biometric data from person at turnstyle and automatically approves or rejects entry to the building based on pre-collected criteria such as if fingerprint scan matches existing records, checks against employee work schedule and rest day, employee on active list or already terminated, and records name and employee ID numnber, then date and time that biometric data was collected and whether for entry into or exit from premisses.

Highest Risk Rating
16 - High Risk

Stakeholders

Name	Role	Involvement
Ching, Roderick Senger	HJanitor	Gemini
Dean, Jennifer	Driver	Tequila

Rows per page: 10 1-2 of 2

Risk Map

IMPACT				
	4	8	12	16
	3	6	9	12
	2	4	6	8
	1	2	3	4

PROBABILITY

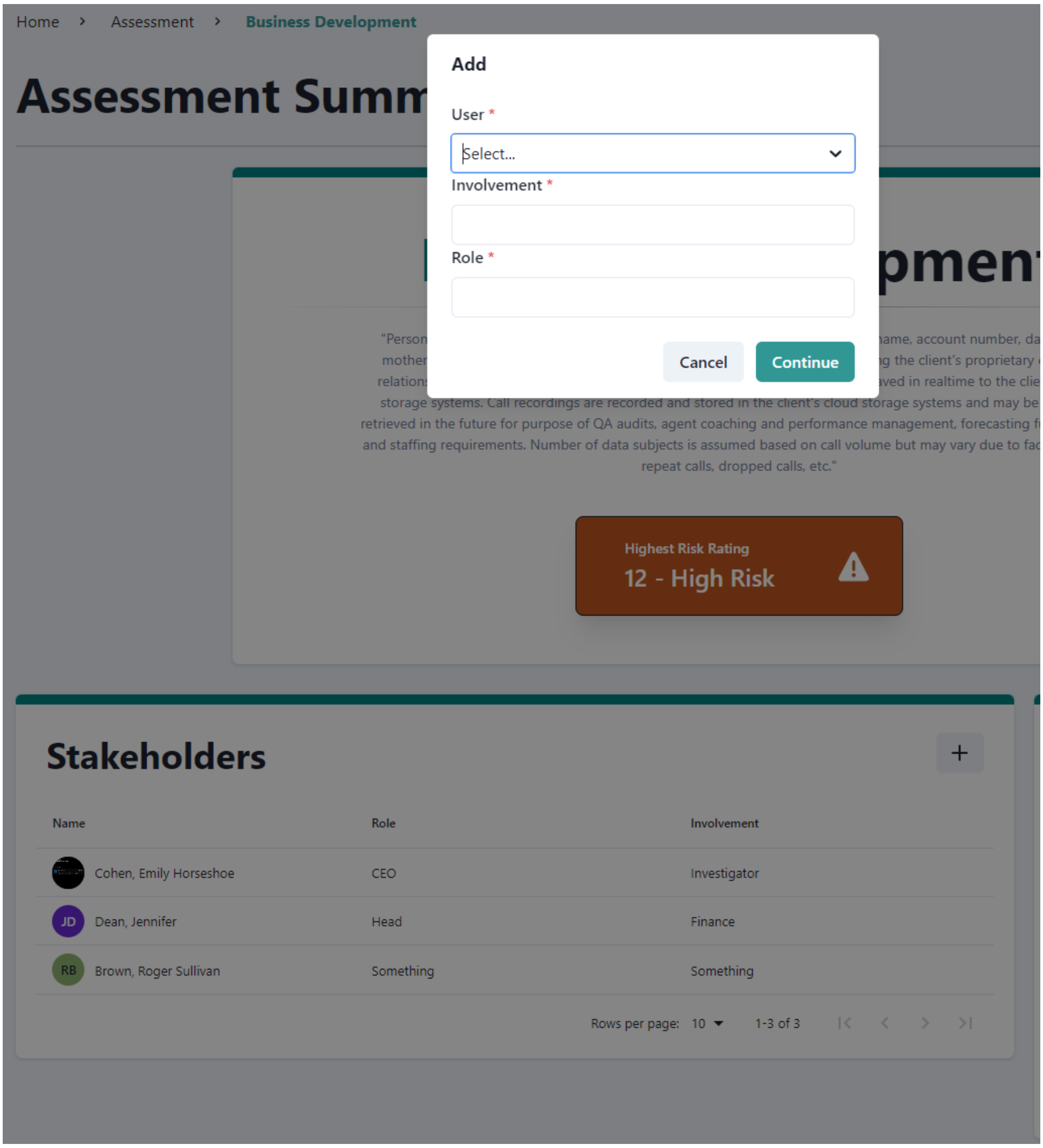
Threats and Vulnerabilities

Description	Reporter	Impact	Probability	Risk Rating
Staff duties not being properly segregated	Dean, Jennifer	4	4	16
Sensitive data not being properly classified	Dean, Jennifer	1	1	1

Rows per page: 10 1-2 of 2

Users may view all PIAs they are assigned as stakeholders to.

a. Add Stakeholder



Add

User *

Select...

Involvement *

Role *

"Person … name, account number, da
mother … g the client's proprietary
relation … ved in realtime to the clie
storage systems. Call recordings are recorded and stored in the client's cloud storage systems and may be
retrieved in the future for purpose of QA audits, agent coaching and performance management, forecasting f
and staffing requirements. Number of data subjects is assumed based on call volume but may vary due to fac
repeat calls, dropped calls, etc."

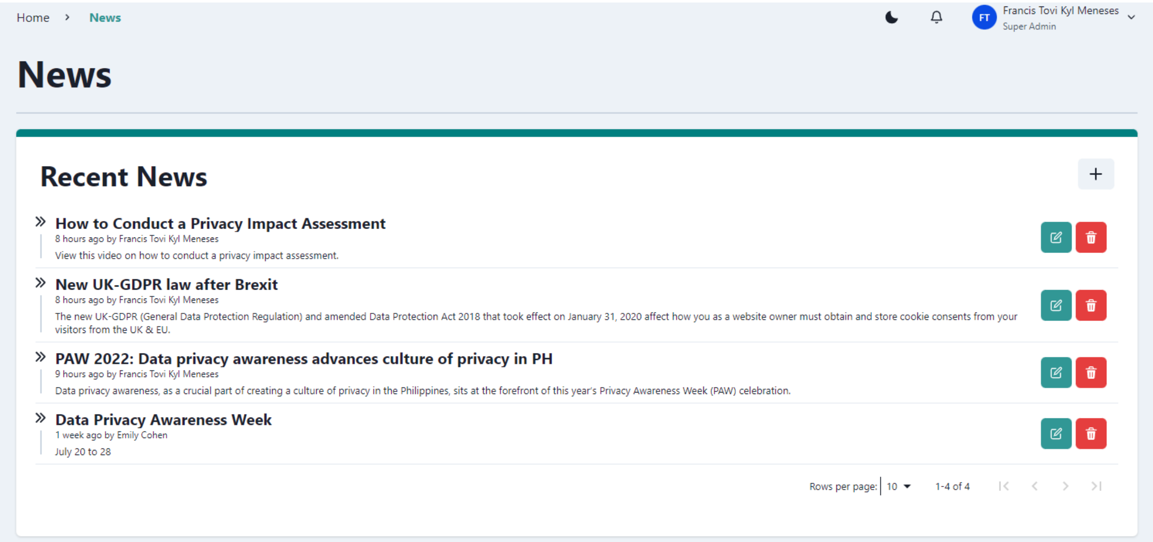
Highest Risk Rating
12 - High Risk

Stakeholders

Name	Role	Involvement
Cohen, Emily Horseshoe	CEO	Investigator
JD Dean, Jennifer	Head	Finance
RB Brown, Roger Sullivan	Something	Something

Super-admin may assign stakeholders to a PIA.

7. News Sections



News

Recent News

+

» How to Conduct a Privacy Impact Assessment
8 hours ago by Francis Tovi Kyl Meneses
View this video on how to conduct a privacy impact assessment.

» New UK-GDPR law after Brexit
8 hours ago by Francis Tovi Kyl Meneses
The new UK-GDPR (General Data Protection Regulation) and amended Data Protection Act 2018 that took effect on January 31, 2020 affect how you as a website owner must obtain and store cookie consents from your visitors from the UK & EU.

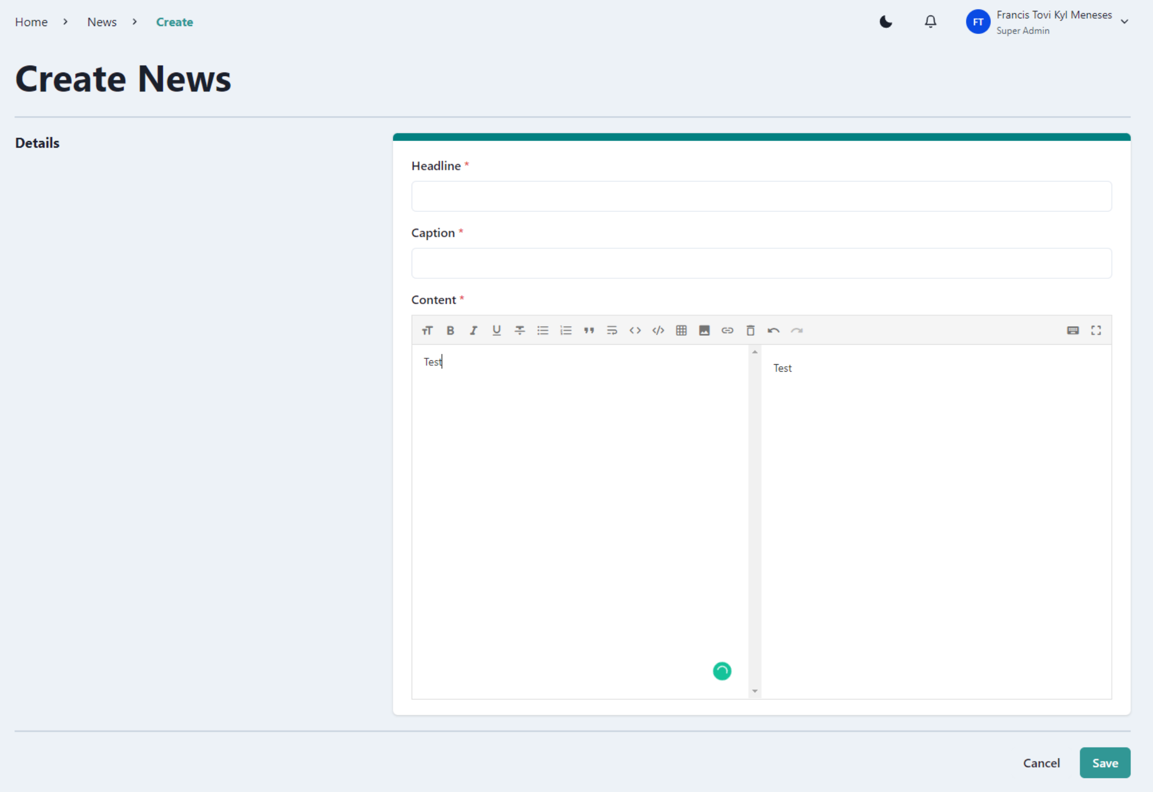
» PAW 2022: Data privacy awareness advances culture of privacy in PH
9 hours ago by Francis Tovi Kyl Meneses
Data privacy awareness, as a crucial part of creating a culture of privacy in the Philippines, sits at the forefront of this year's Privacy Awareness Week (PAW) celebration.

» Data Privacy Awareness Week
1 week ago by Emily Cohen
July 20 to 28

Rows per page: 10 1-4 of 4

Users may see the latest news regarding data privacy in this section. To create new news, users may click the add button on the upper right of the website.

a. Create news



Create News

Details

Headline *

Caption *

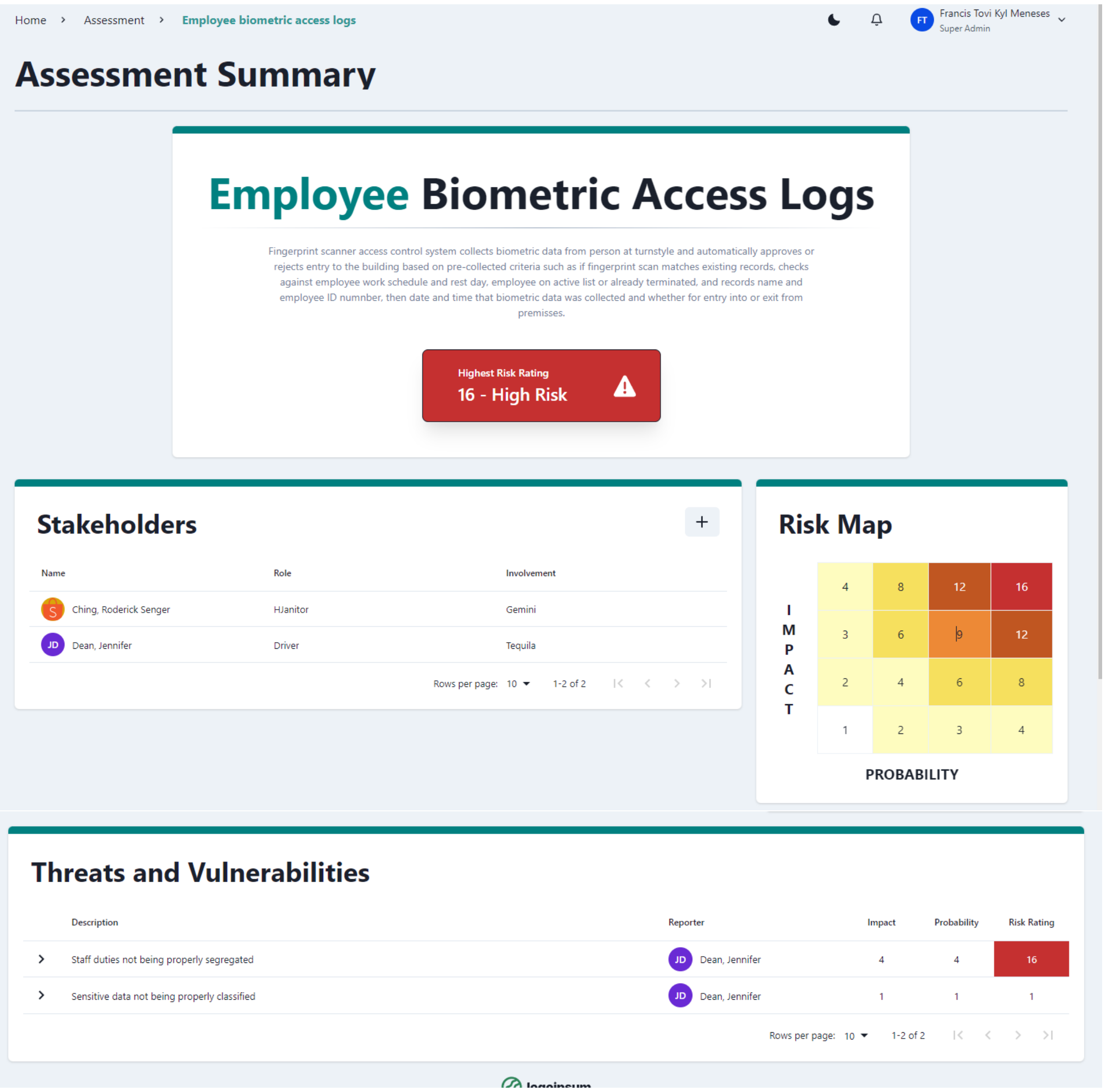
Content *

Test

Test

In creating new news, users will have to provide a headline, caption, and content.

b. Viewing Privacy Impact Assessments (PIA)



Home › Assessment › Employee biometric access logs

Francis Tovi Kyl Meneses
Super Admin

Assessment Summary

Employee Biometric Access Logs

Fingerprint scanner access control system collects biometric data from person at turnstyle and automatically approves or rejects entry to the building based on pre-collected criteria such as if fingerprint scan matches existing records, checks against employee work schedule and rest day, employee on active list or already terminated, and records name and employee ID numnber, then date and time that biometric data was collected and whether for entry into or exit from premisses.

Highest Risk Rating
16 - High Risk

Stakeholders

Name	Role	Involvement
Ching, Roderick Senger	HJanitor	Gemini
Dean, Jennifer	Driver	Tequila

Rows per page: 10 1-2 of 2

Risk Map

IMPACT				
	4	8	12	16
	3	6	9	12
	2	4	6	8
	1	2	3	4

PROBABILITY

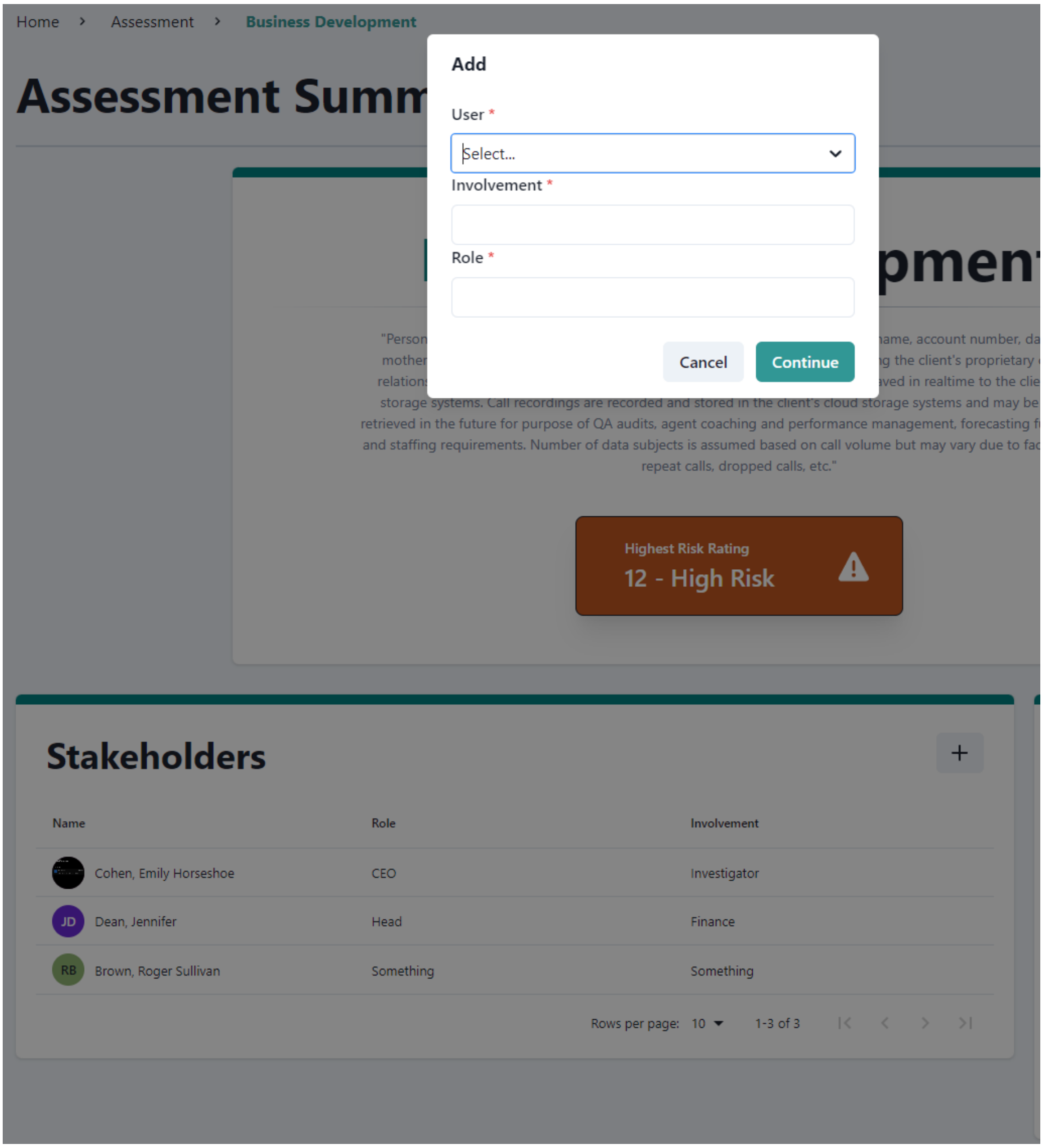
Threats and Vulnerabilities

	Description	Reporter	Impact	Probability	Risk Rating
›	Staff duties not being properly segregated	Dean, Jennifer	4	4	16
›	Sensitive data not being properly classified	Dean, Jennifer	1	1	1

Rows per page: 10 1-2 of 2

Users may view all PIAs they are assigned as stakeholders to.

c. Add Stakeholder



"Person ... ame, account number, da
mother ... g the client's proprietary
relation ... ved in realtime to the clie
storage systems. Call recordings are recorded and stored in the client's cloud storage systems and may be
retrieved in the future for purpose of QA audits, agent coaching and performance management, forecasting f
and staffing requirements. Number of data subjects is assumed based on call volume but may vary due to fac
repeat calls, dropped calls, etc."

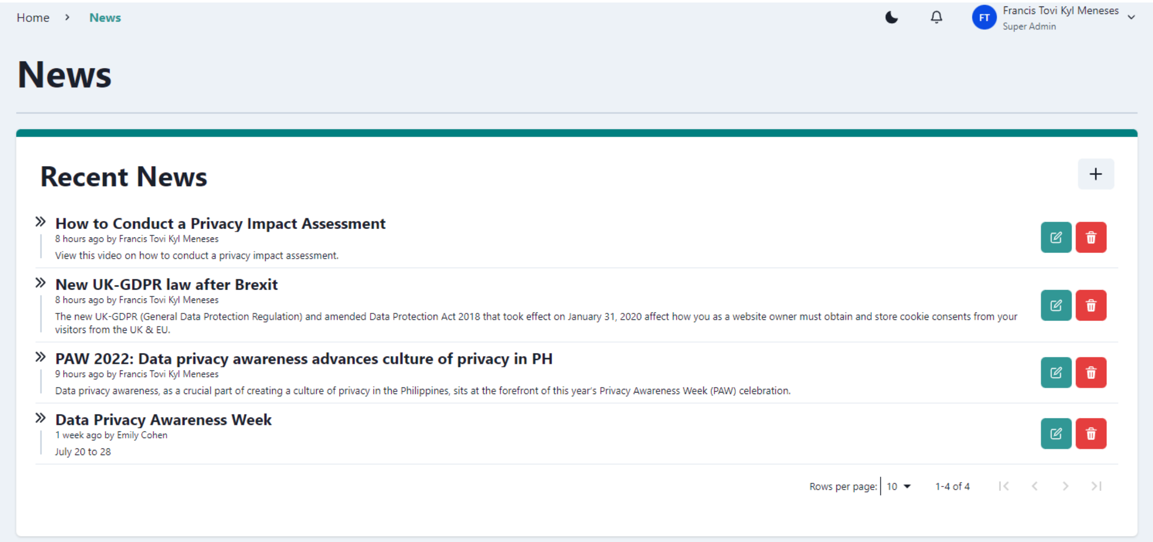
Stakeholders

Name	Role	Involvement
Cohen, Emily Horseshoe	CEO	Investigator
JD Dean, Jennifer	Head	Finance
RB Brown, Roger Sullivan	Something	Something

Rows per page: 10 1-3 of 3

Super-admin may assign stakeholders to a PIA.

8. News Sections



News

Recent News

» How to Conduct a Privacy Impact Assessment
8 hours ago by Francis Tovi Kyl Meneses
View this video on how to conduct a privacy impact assessment.

» New UK-GDPR law after Brexit
8 hours ago by Francis Tovi Kyl Meneses
The new UK-GDPR (General Data Protection Regulation) and amended Data Protection Act 2018 that took effect on January 31, 2020 affect how you as a website owner must obtain and store cookie consents from your visitors from the UK & EU.

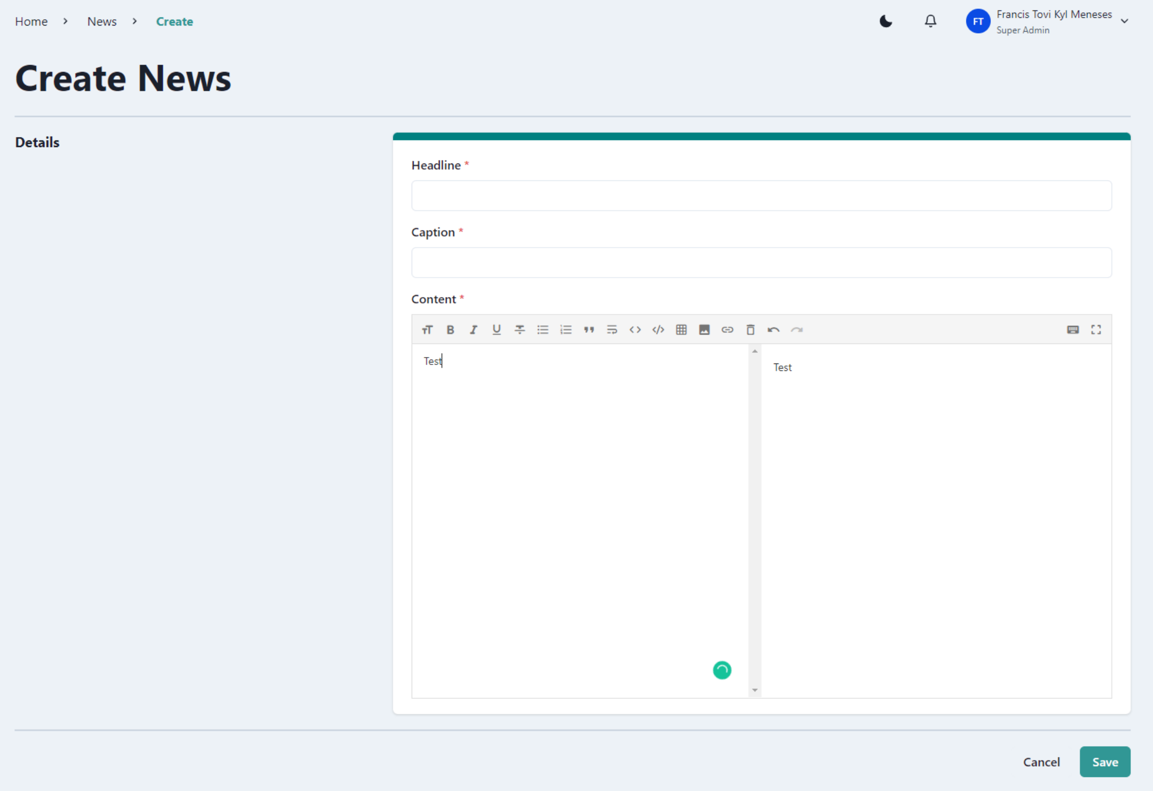
» PAW 2022: Data privacy awareness advances culture of privacy in PH
9 hours ago by Francis Tovi Kyl Meneses
Data privacy awareness, as a crucial part of creating a culture of privacy in the Philippines, sits at the forefront of this year's Privacy Awareness Week (PAW) celebration.

» Data Privacy Awareness Week
1 week ago by Emily Cohen
July 20 to 28

Rows per page: 10 1-4 of 4

Users may see the latest news regarding data privacy in this section. To create new news, users may click the add button on the upper right of the website.

b. Create news



Create News

Details

Headline *

Caption *

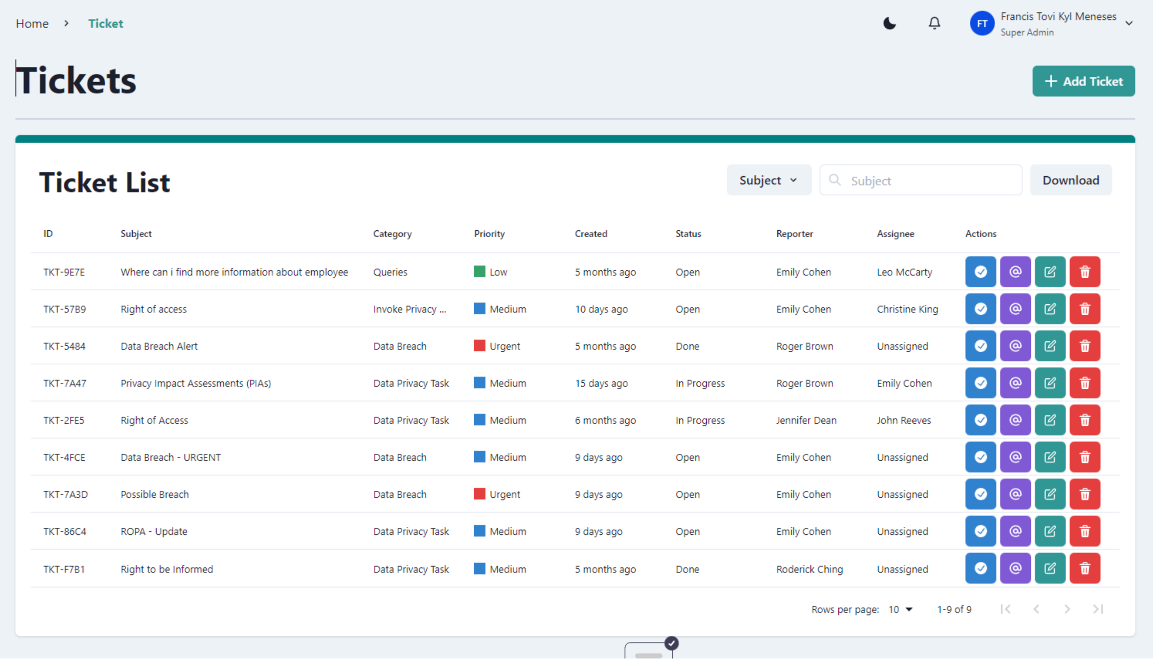
Content *

Test

Test

In creating new news, users will have to provide a headline, caption, and content.

9. Tickets Section



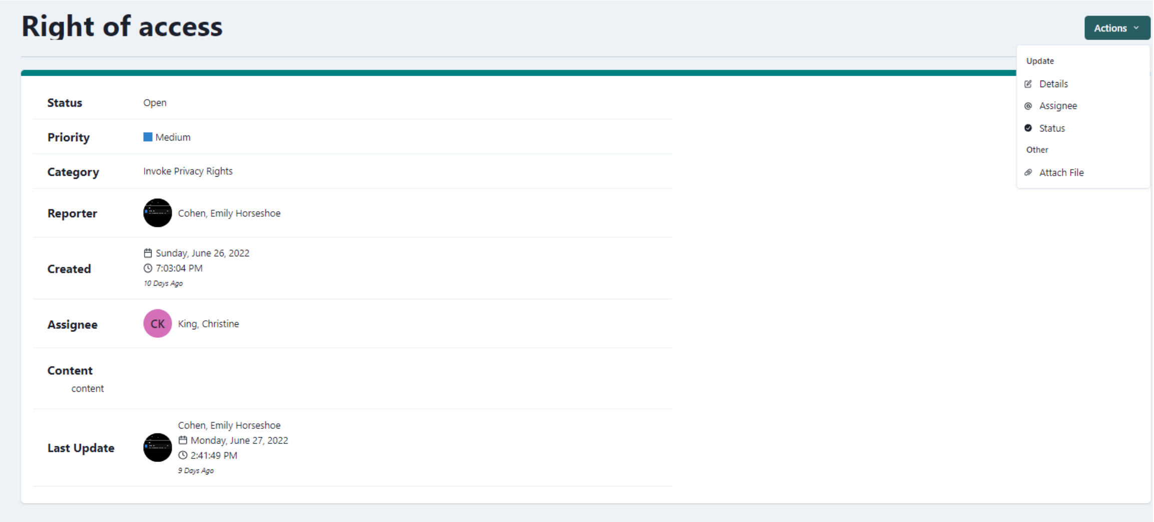
Tickets

Ticket List

ID	Subject	Category	Priority	Created	Status	Reporter	Assignee	Actions
TKT-9E7E	Where can i find more information about employee	Queries	🟩 Low	5 months ago	Open	Emily Cohen	Leo McCarty	✓ @ ✎ 🗑
TKT-57B9	Right of access	Invoke Privacy ...	🟦 Medium	10 days ago	Open	Emily Cohen	Christine King	✓ @ ✎ 🗑
TKT-5484	Data Breach Alert	Data Breach	🟥 Urgent	5 months ago	Done	Roger Brown	Unassigned	✓ @ ✎ 🗑
TKT-7A47	Privacy Impact Assessments (PIAs)	Data Privacy Task	🟦 Medium	15 days ago	In Progress	Roger Brown	Emily Cohen	✓ @ ✎ 🗑
TKT-2FE5	Right of Access	Data Privacy Task	🟦 Medium	6 months ago	In Progress	Jennifer Dean	John Reeves	✓ @ ✎ 🗑
TKT-4FCE	Data Breach - URGENT	Data Breach	🟦 Medium	9 days ago	Open	Emily Cohen	Unassigned	✓ @ ✎ 🗑
TKT-7A3D	Possible Breach	Data Breach	🟥 Urgent	9 days ago	Open	Emily Cohen	Unassigned	✓ @ ✎ 🗑
TKT-86C4	ROPA - Update	Data Privacy Task	🟦 Medium	9 days ago	Open	Emily Cohen	Unassigned	✓ @ ✎ 🗑
TKT-F7B1	Right to be Informed	Data Privacy Task	🟦 Medium	5 months ago	Done	Roderick Ching	Unassigned	✓ @ ✎ 🗑

This is where admins can add, edit, delete lodged tickets. Follow the buttons listed below for the actions.

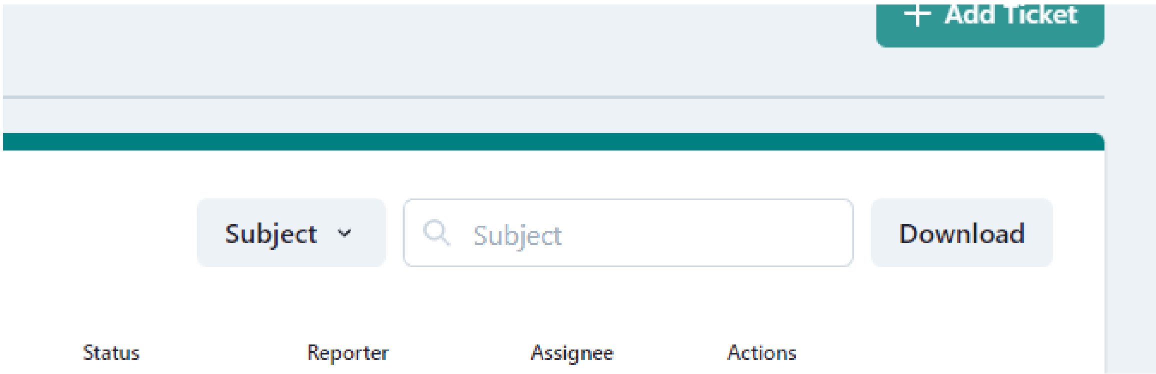
- ✓ Tag ticket as accomplished
- @ Assign tickets to team members
- ✎ Edit tickets
- 🗑 Delete tickets

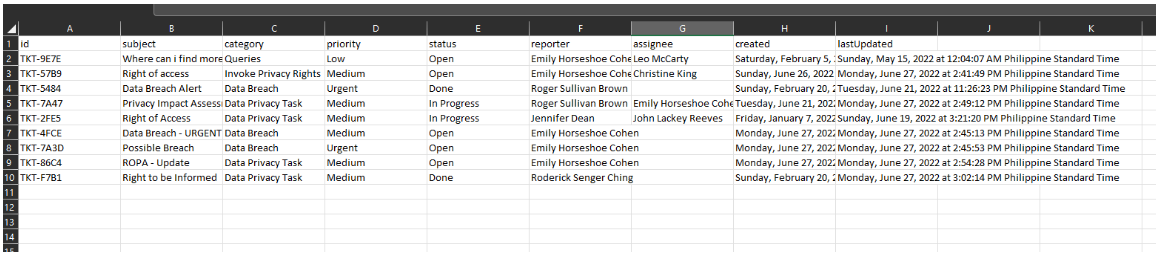

Right of access

Status	Open
Priority	🟦 Medium
Category	Invoke Privacy Rights
Reporter	Cohen, Emily Horseshoe
Created	Sunday, June 26, 2022 7:03:04 PM *10 Days Ago*
Assignee	CK King, Christine
Content content	
Last Update	Cohen, Emily Horseshoe Monday, June 27, 2022 2:41:49 PM *9 Days Ago*

Click the ticket to view complete details, here, users may also edit the ticket or attach files

a. Download tickets

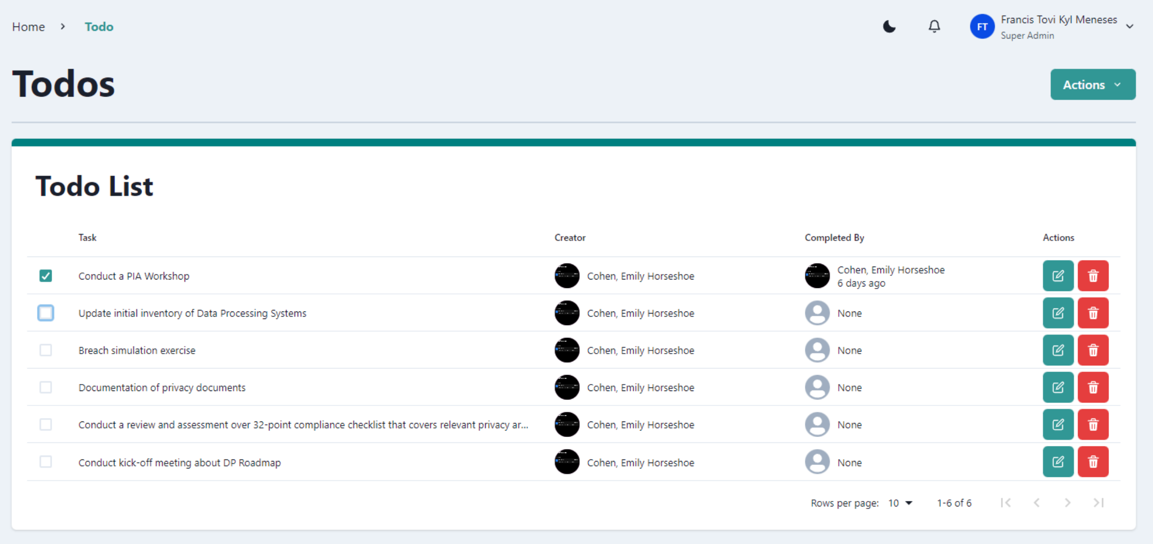




	A	B	C	D	E	F	G	H	I
1	id	subject	category	priority	status	reporter	assignee	created	lastUpdated
2	TKT-9E7E	Where can i find more	Queries	Low	Open	Emily Horseshoe Cohe	Leo McCarty	Saturday, February 5, 2	Sunday, May 15, 2022 at 12:04:07 AM Philippine Standard Time
3	TKT-57B9	Right of access	Invoke Privacy Rights	Medium	Open	Emily Horseshoe Cohe	Christine King	Sunday, June 26, 2022	Monday, June 27, 2022 at 2:41:49 PM Philippine Standard Time
4	TKT-5484	Data Breach Alert	Data Breach	Urgent	Done	Roger Sullivan Brown		Sunday, February 20, 2	Tuesday, June 21, 2022 at 11:26:23 PM Philippine Standard Time
5	TKT-7A47	Privacy Impact Assessi	Data Privacy Task	Medium	In Progress	Roger Sullivan Brown	Emily Horseshoe Cohe	Tuesday, June 21, 202	Monday, June 27, 2022 at 2:49:12 PM Philippine Standard Time
6	TKT-2FE5	Right of Access	Data Privacy Task	Medium	In Progress	Jennifer Dean	John Lackey Reeves	Friday, January 7, 2022	Sunday, June 19, 2022 at 3:21:20 PM Philippine Standard Time
7	TKT-4FCE	Data Breach - URGENT	Data Breach	Medium	Open	Emily Horseshoe Cohen		Monday, June 27, 202	Monday, June 27, 2022 at 2:45:13 PM Philippine Standard Time
8	TKT-7A3D	Possible Breach	Data Breach	Urgent	Open	Emily Horseshoe Cohen		Monday, June 27, 202	Monday, June 27, 2022 at 2:45:53 PM Philippine Standard Time
9	TKT-86C4	ROPA - Update	Data Privacy Task	Medium	Open	Emily Horseshoe Cohen		Monday, June 27, 202	Monday, June 27, 2022 at 2:54:28 PM Philippine Standard Time
10	TKT-F7B1	Right to be Informed	Data Privacy Task	Medium	Done	Roderick Senger Ching		Sunday, February 20, 2	Monday, June 27, 2022 at 3:02:14 PM Philippine Standard Time

Administrators may also download a report for all tickets lodged.

10. To-do Section



Todos

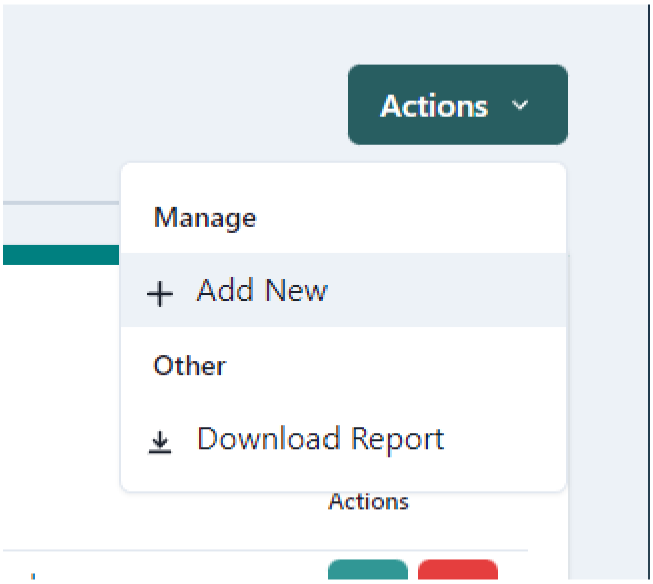
Todo List

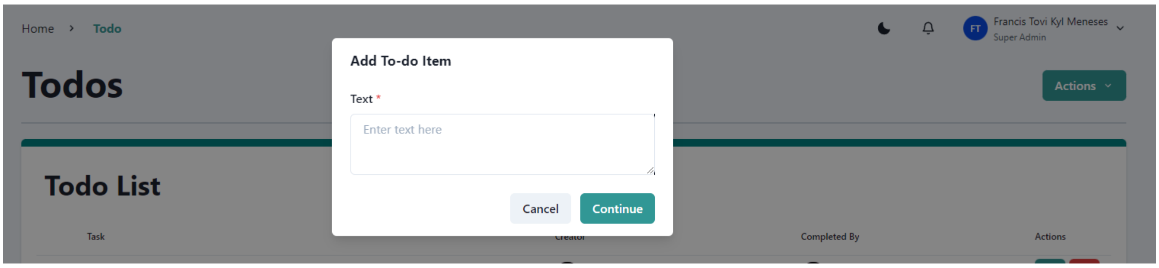
	Task	Creator	Completed By	Actions
☑	Conduct a PIA Workshop	Cohen, Emily Horseshoe	Cohen, Emily Horseshoe 6 days ago	
□	Update initial inventory of Data Processing Systems	Cohen, Emily Horseshoe	None	
□	Breach simulation exercise	Cohen, Emily Horseshoe	None	
□	Documentation of privacy documents	Cohen, Emily Horseshoe	None	
□	Conduct a review and assessment over 32-point compliance checklist that covers relevant privacy ar...	Cohen, Emily Horseshoe	None	
□	Conduct kick-off meeting about DP Roadmap	Cohen, Emily Horseshoe	None	

Rows per page: 10 1-6 of 6

This is the to-do section, super admin may create a to-do list, and admins may tag the items on the list as accomplished by clicking the check box on the left side of the website.

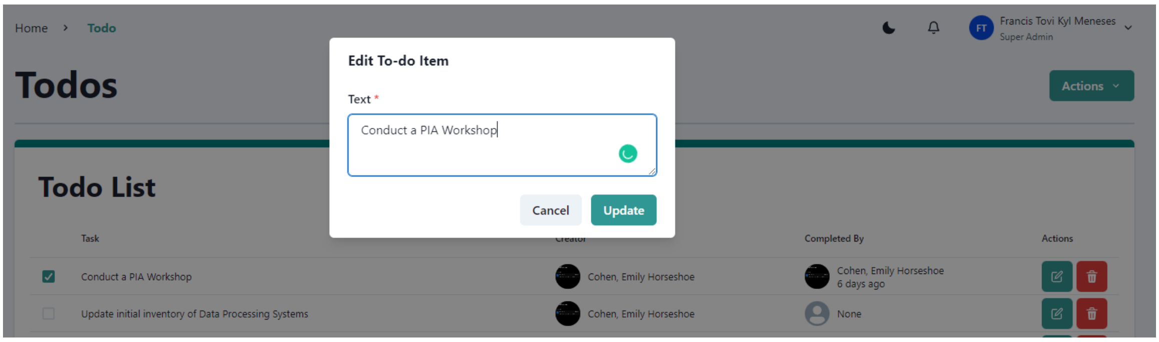
a. Create an action item





Task	Creator	Completed By	Actions

b. Edit Item

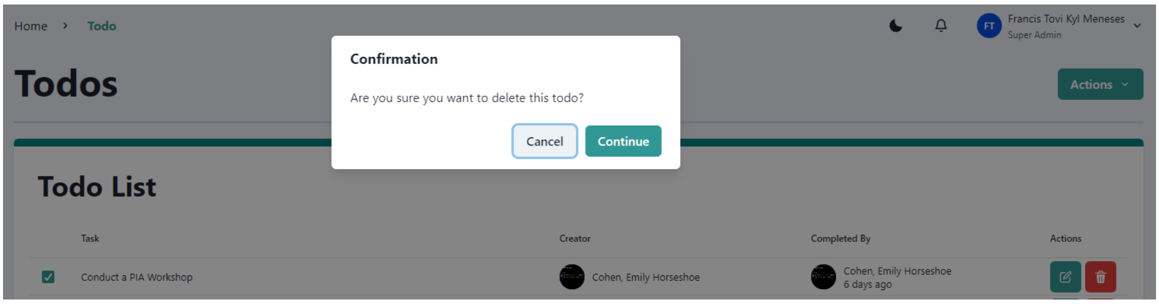


Text *

Conduct a PIA Workshop

	Task	Creator	Completed By	Actions
☑	Conduct a PIA Workshop	Cohen, Emily Horseshoe	Cohen, Emily Horseshoe 6 days ago	
□	Update initial inventory of Data Processing Systems	Cohen, Emily Horseshoe	None	

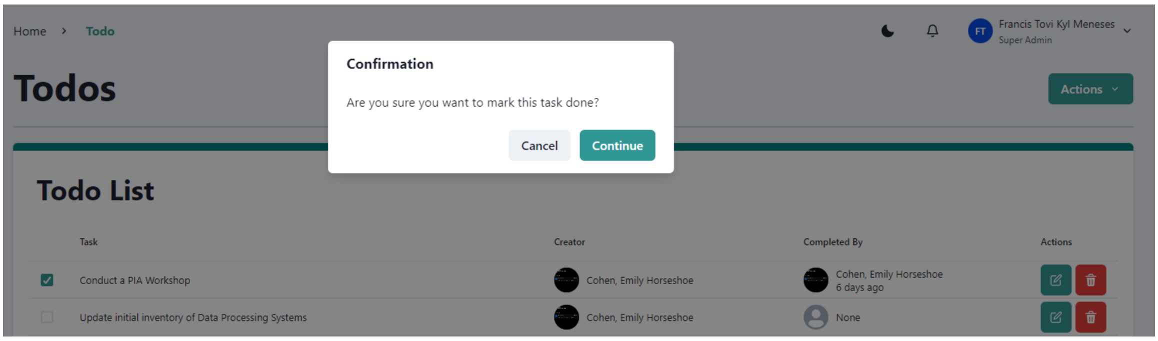
c. Delete Item



Are you sure you want to delete this todo?

	Task	Creator	Completed By	Actions
☑	Conduct a PIA Workshop	Cohen, Emily Horseshoe	Cohen, Emily Horseshoe 6 days ago	

d. Mark an action item complete



Home › Todo

Francis Tovi Kyl Meneses
Super Admin

Todos

Confirmation

Are you sure you want to mark this task done?

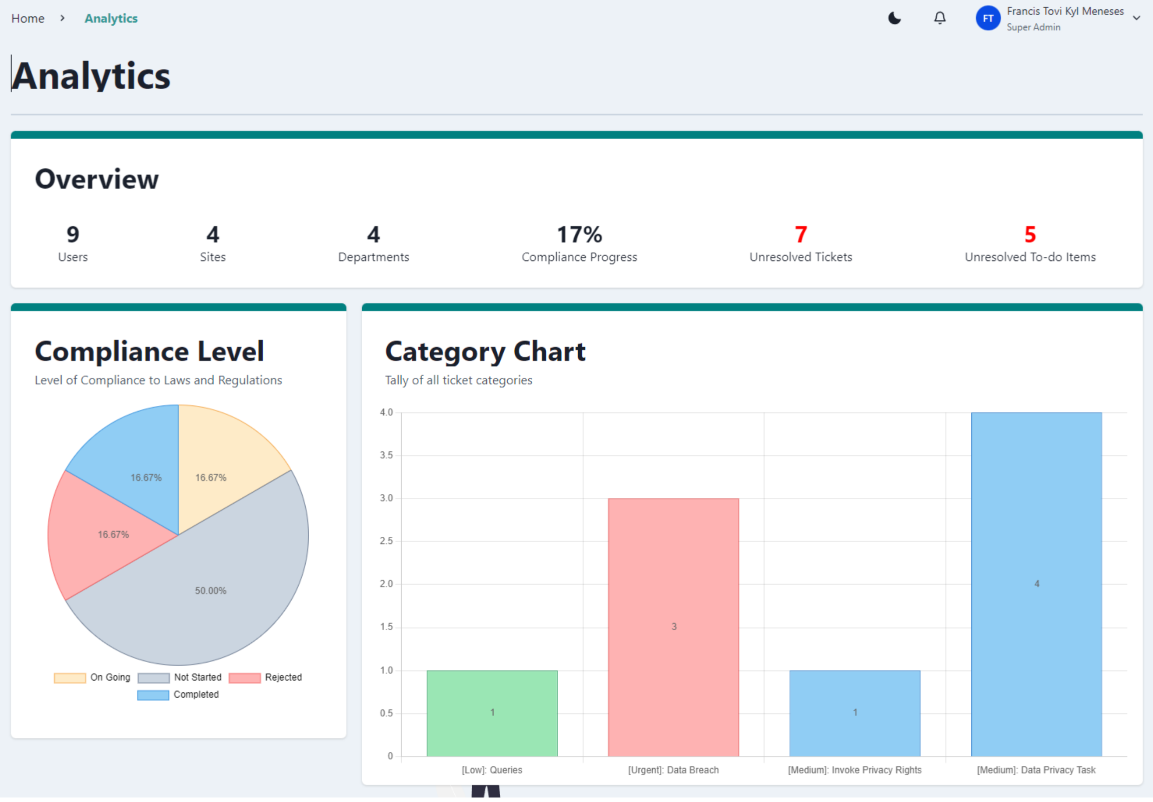
Cancel | Continue

Actions

Todo List

	Task	Creator	Completed By	Actions
☑	Conduct a PIA Workshop	Cohen, Emily Horseshoe	Cohen, Emily Horseshoe 6 days ago	
□	Update initial inventory of Data Processing Systems	Cohen, Emily Horseshoe	None	

11. Analytics Section



Home › Analytics

Francis Tovi Kyl Meneses
Super Admin

Analytics

Overview

9	4	4	17%	7	5
Users	Sites	Departments	Compliance Progress	Unresolved Tickets	Unresolved To-do Items

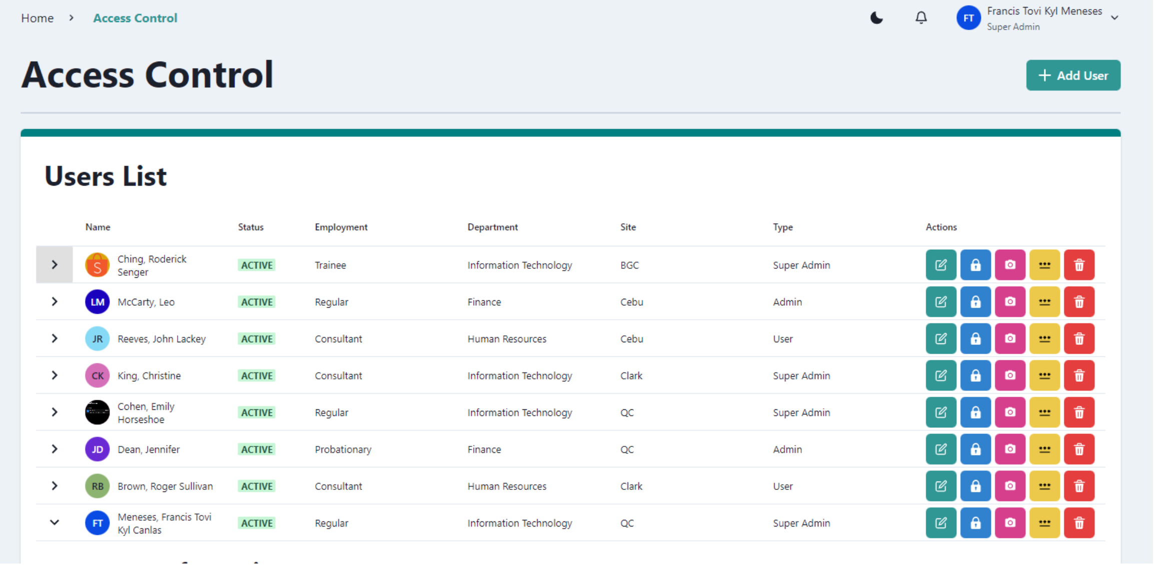
Compliance Level

Level of Compliance to Laws and Regulations

Category Chart

Tally of all ticket categories

12. Access Control Section



Access Control

Users List

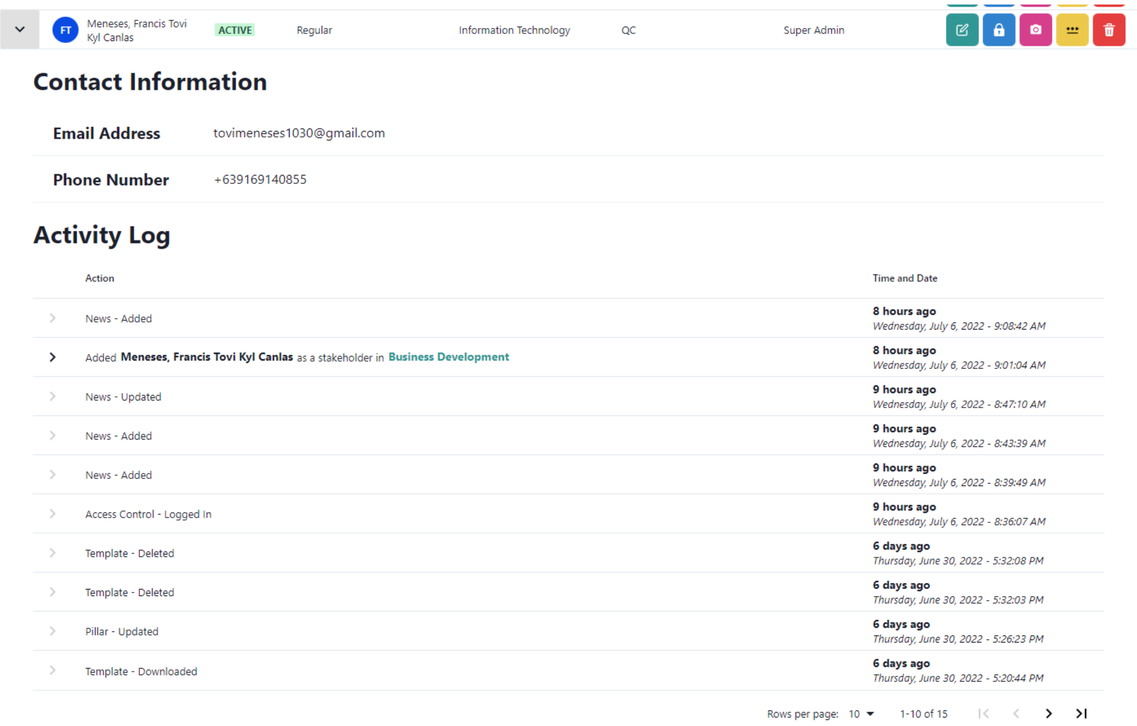
	Name	Status	Employment	Department	Site	Type	Actions
›	Ching, Roderick Senger	ACTIVE	Trainee	Information Technology	BGC	Super Admin	
›	McCarty, Leo	ACTIVE	Regular	Finance	Cebu	Admin	
›	Reeves, John Lackey	ACTIVE	Consultant	Human Resources	Cebu	User	
›	King, Christine	ACTIVE	Consultant	Information Technology	Clark	Super Admin	
›	Cohen, Emily Horseshoe	ACTIVE	Regular	Information Technology	QC	Super Admin	
›	Dean, Jennifer	ACTIVE	Probationary	Finance	QC	Admin	
›	Brown, Roger Sullivan	ACTIVE	Consultant	Human Resources	Clark	User	
⌄	Meneses, Francis Tovi Kyl Canlas	ACTIVE	Regular	Information Technology	QC	Super Admin	

Super-admins may create three types of user accounts (super-admin, admin, and users). Super-admins may impose different actions in the users account which are listed below.

a. Actions

- Edit User Details
- Lock User Account
- Unlock User Account
- Update Profile Picture
- Reset Password
- Delete User

b. Audit Trail of Users



FT	Meneses, Francis Tovi Kyl Canlas	ACTIVE	Regular	Information Technology	QC	Super Admin

Contact Information

Email Address	tovimeneses1030@gmail.com
Phone Number	+639169140855

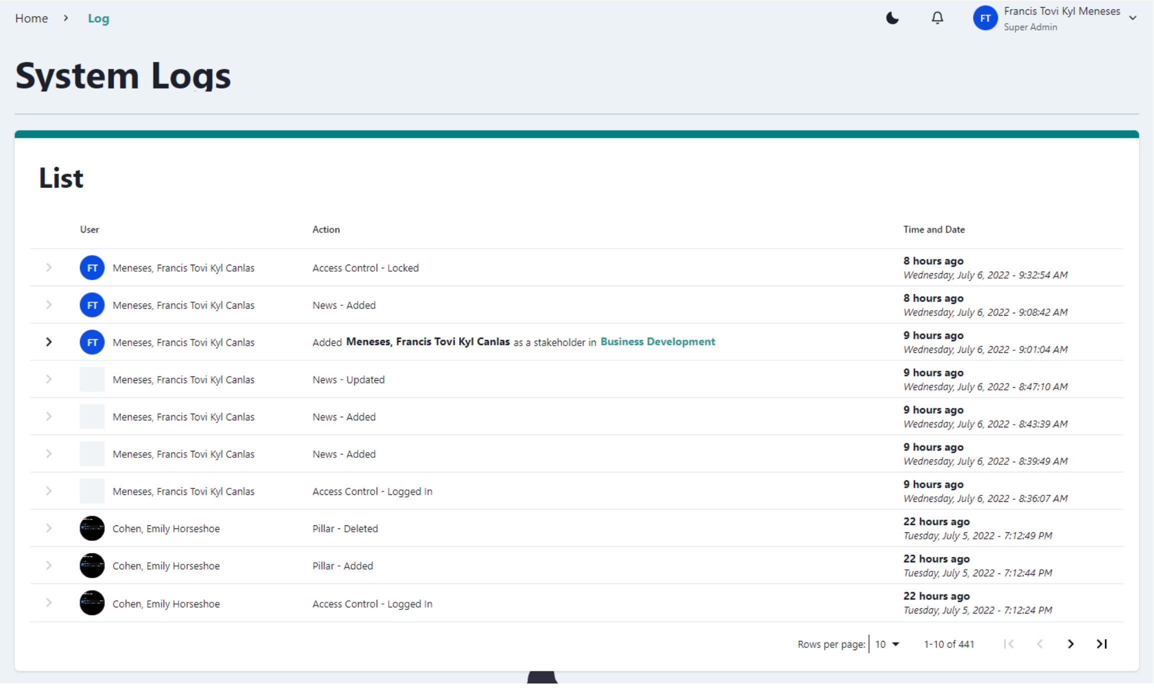
Activity Log

Action	Time and Date
News - Added	**8 hours ago** *Wednesday, July 6, 2022 - 9:08:42 AM*
Added **Meneses, Francis Tovi Kyl Canlas** as a stakeholder in **Business Development**	**8 hours ago** *Wednesday, July 6, 2022 - 9:01:04 AM*
News - Updated	**9 hours ago** *Wednesday, July 6, 2022 - 8:47:10 AM*
News - Added	**9 hours ago** *Wednesday, July 6, 2022 - 8:43:39 AM*
News - Added	**9 hours ago** *Wednesday, July 6, 2022 - 8:39:49 AM*
Access Control - Logged In	**9 hours ago** *Wednesday, July 6, 2022 - 8:36:07 AM*
Template - Deleted	**6 days ago** *Thursday, June 30, 2022 - 5:32:08 PM*
Template - Deleted	**6 days ago** *Thursday, June 30, 2022 - 5:32:03 PM*
Pillar - Updated	**6 days ago** *Thursday, June 30, 2022 - 5:26:23 PM*
Template - Downloaded	**6 days ago** *Thursday, June 30, 2022 - 5:20:44 PM*

Rows per page: 10 1-10 of 15

Super admins may also view the activity trail of each users for security purposes.

13. System Logs Section



System Logs

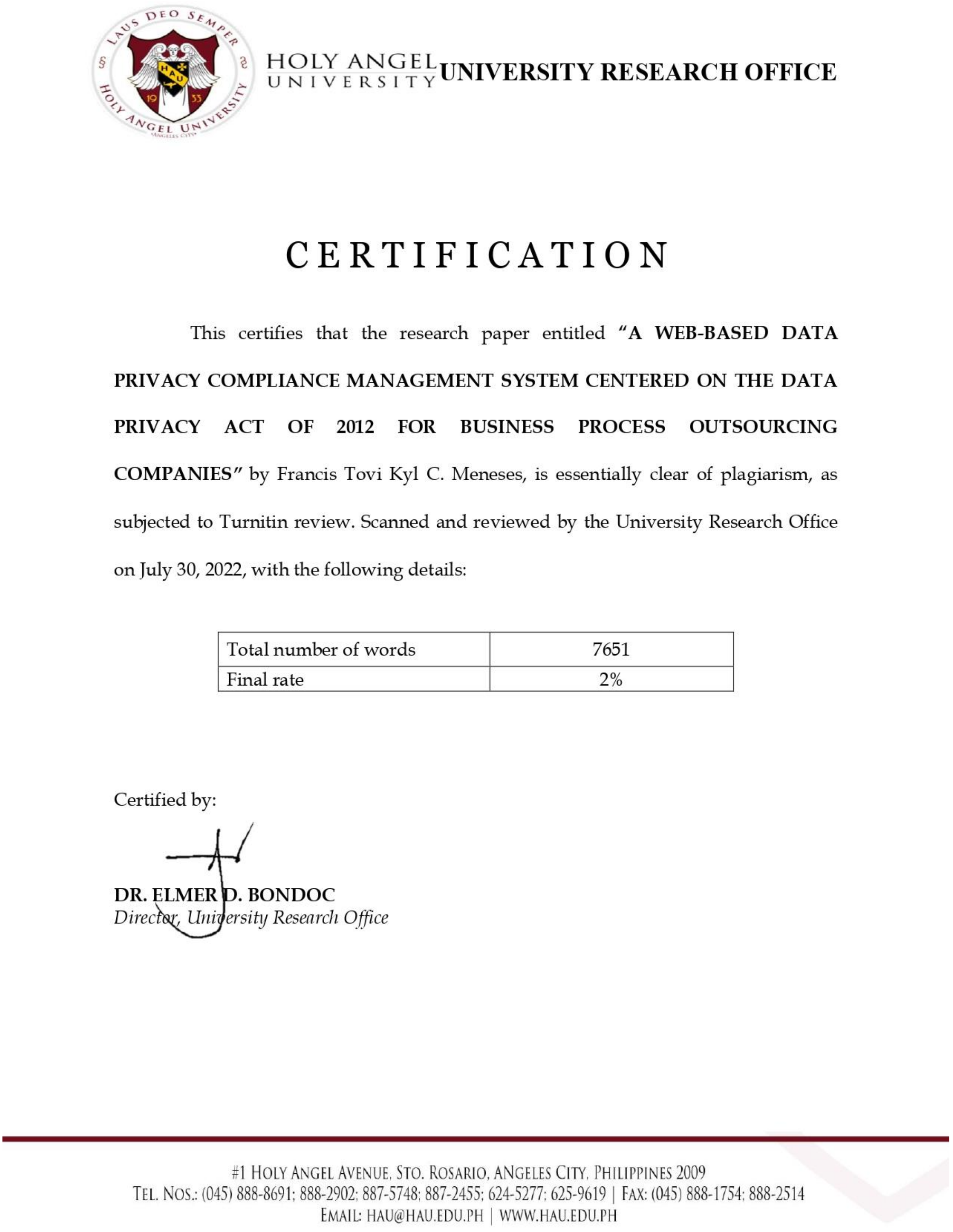
List

User	Action	Time and Date
FT Meneses, Francis Tovi Kyl Canlas	Access Control - Locked	**8 hours ago** *Wednesday, July 6, 2022 - 9:32:54 AM*
FT Meneses, Francis Tovi Kyl Canlas	News - Added	**8 hours ago** *Wednesday, July 6, 2022 - 9:08:42 AM*
FT Meneses, Francis Tovi Kyl Canlas	Added **Meneses, Francis Tovi Kyl Canlas** as a stakeholder in **Business Development**	**9 hours ago** *Wednesday, July 6, 2022 - 9:01:04 AM*
Meneses, Francis Tovi Kyl Canlas	News - Updated	**9 hours ago** *Wednesday, July 6, 2022 - 8:47:10 AM*
Meneses, Francis Tovi Kyl Canlas	News - Added	**9 hours ago** *Wednesday, July 6, 2022 - 8:43:39 AM*
Meneses, Francis Tovi Kyl Canlas	News - Added	**9 hours ago** *Wednesday, July 6, 2022 - 8:39:49 AM*
Meneses, Francis Tovi Kyl Canlas	Access Control - Logged In	**9 hours ago** *Wednesday, July 6, 2022 - 8:36:07 AM*
Cohen, Emily Horseshoe	Pillar - Deleted	**22 hours ago** *Tuesday, July 5, 2022 - 7:12:49 PM*
Cohen, Emily Horseshoe	Pillar - Added	**22 hours ago** *Tuesday, July 5, 2022 - 7:12:44 PM*
Cohen, Emily Horseshoe	Access Control - Logged In	**22 hours ago** *Tuesday, July 5, 2022 - 7:12:24 PM*

Rows per page: 10 1-10 of 441

Super-admins may access the summary of logs of the website.

Appendix I
Plagiarism Scan Results



HOLY ANGEL UNIVERSITY UNIVERSITY RESEARCH OFFICE

CERTIFICATION

This certifies that the research paper entitled **"A WEB-BASED DATA PRIVACY COMPLIANCE MANAGEMENT SYSTEM CENTERED ON THE DATA PRIVACY ACT OF 2012 FOR BUSINESS PROCESS OUTSOURCING COMPANIES"** by Francis Tovi Kyl C. Meneses, is essentially clear of plagiarism, as subjected to Turnitin review. Scanned and reviewed by the University Research Office on July 30, 2022, with the following details:

Total number of words	7651
Final rate	2%

Certified by:

DR. ELMER D. BONDOC
Director, University Research Office

#1 Holy Angel Avenue, Sto. Rosario, Angeles City, Philippines 2009
Tel. Nos.: (045) 888-8691; 888-2902; 887-5748; 887-2455; 624-5277; 625-9619 | Fax: (045) 888-1754; 888-2514
Email: HAU@HAU.EDU.PH | WWW.HAU.EDU.PH

Appendix J
Researcher Curriculum Vitae

Francis Tovi Kyl C. Meneses

Address: 441 Sampaguita St. Dona Belen Subdivision, Angeles City, Pampanga
Email: tovimeneses1030@gmail.com
Contact Number: 09169140855
About me: An ambitious and goal-driven information technologist with various experiences in data privacy, IT compliance, and cybersecurity.

Career Summary

Data Protection Officer (DPO)
BeanLab Inc. | MotherNurture Inc., dba edamama
August 2021 – Present
199 Salcedo St., Legaspi Village, Makati City, 1229 NCR

Key Responsibilities

- Monitor the Personal Information Controllers (PICs) or Personal Information Processors (PIPs) compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies;
- Collects information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
- Analyzes and checks the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
- Engage with those responsible for data protection in the business units and support functions;
- Creates initial Data Privacy procedures and documentation;
- Advocates for the development, review, and/or revision of policies, guidelines, projects, and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
- Acts as Project Manager for Cybersecurity initiatives and policy-making;
- Serves as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
- Cooperates, coordinates and seeks the advice of the NPC regarding matters concerning data privacy and security;
- Implements Corporate Data Protection Policies and Programs and ensures compliance with applicable policies (General Data Protection Regulation (GDPR) and codes of practice;
- Informs and cultivates awareness of privacy and data protection within your organization, including all relevant laws, rules and regulations, and issuances of the NPC;
- Handles IT Operations;
- Handles IT Risk Management; and
- Initiates other compliance programs such as SOC2 and PCI DSS.

Compliance Officer for Data Privacy
CA Telemarketing Inc., dba Collective Solution
February 2021-Present
41 Don Mariano Marcos Ave, Quezon City, 1127 NCR

Key Responsibilities

- Monitor and ensure the organization's compliance with the data privacy laws and other ;

- Data Privacy Act of 2012 (DPA)
- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLB Privacy Laws)
- Jamaica's Data Protection Act 2020
- SOC2
- PCI DSS
- Support data privacy compliance activities in an enterprise level. (Honduras, Jamaica, USA, PH);
- Support the Compliance Manager/Data Protection Officer in implementing the company's Data Privacy Compliance Program;
- Inform and cultivate awareness on Privacy and Data Protection within your organization, including all relevant laws, rules and regulations and issuances of the NPC;
- Ensure proper data breach and security incident management, including the preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period
- Monitor and audit privacy controls; and
- Other duties as assigned - ad hoc or incidental tasks may be assigned from time to time, related to or in addition to those described above.

Data Privacy Consultant
Top Data Global IT Solutions
November 2019-November 2020
11/F Entec 2 Bldg. Nepo Shopping Complex, 2009 Pampanga

Key Responsibilities

- Monitor the organization's compliance with the data privacy law;
- Identify and evaluate the company's data processing activities;
- Monitor data management procedures and compliance within the company;
- Ensure all queries are addressed;
- Write and update detailed guides on data protection policies;
- Handle and manage issues related to data privacy;
- Conduct training for employees on data privacy;
- Conduct compliance assessments and privacy impact assessments;
- Handle customer complaints related to data privacy; and
- Update/Follow up with changes in law and issue recommendation to ensure compliance.

Database Editor
Top Data Global IT Solutions
December 2018 – November 2020
11/F Entec 2 Bldg. Nepo Shopping Complex, 2009 Pampanga

Key Responsibilities

- Responsible for performing editing duties such as proofreading and content revisions of short product descriptions;
- Responsible for performing quality checks on content and makes sure that the following are thoroughly reviewed and corrected: spelling and style, English translations, capitalization, punctuation, grammar usage, typographical errors, and the photos or illustrations are correctly captioned and uploaded; and
- Submit daily reports

Education

Bachelor of Science in Information Technology
major in Network Administration
Holy Angel University
Angeles City, Pampanga
2014 – 2018

Trainings and Certifications

NPC DPO ACE Training Level 1
August 2021 |National Privacy Commission

Certified Master of Data Privacy
June 2021 | Exterro

Certified Remote Work and Virtual Collaboration Professional
February 2021 – February 2023 | Certiprof
Credential ID: 57573709

Certified Cybersecurity Foundation Professional
January 2021 – January 2023 | Certiprof
Credential ID: 54496449

Certified NSE 2 Network Security Associate
April 2020 – April 2022 | Fortinet
Credential ID: fGjWTQ1bbA

Certified NSE 1 Network Security Associate
March 2020 – March 2022| Fortinet
Credential ID: OXH50HM4hl

Certified ISO/IEC 20000 IT Service Management Associate
March 2021 | SkillFront
Credential ID: 68795486003294

Certified ISO/IEC 27001 Information Security Associate
March 2021 | SkillFront
Credential ID: 48294245890145

Lean Foundations Professional Certification (LFPC)
March 2021 | SkillFront
Credential ID: 27486585855653

Seminars, and Online Course

Privacy by Design: Data Classification
March 2022
LinkedIn Learning

Cybersecurity Awareness Webinar
October 2021
Teched Global Academy

Business Continuity, Data Privacy, and Information Security How do they link?
October 2021
Professional Evaluation and Certification Board (PECB)

Breaking the Cycle of Online Fraud and Abuse in a Digital World
September 2021
Escom Events and Shape Security

Ethical Hacking vs Penetration Testing vs Cybersecurity
September 2021
Professional Evaluation and Certification Board (PECB)

Mastering Knowing Your Data and Establishing a Defensible Data Inventory
April 2021
Compliance Week

5 easy steps to prepare for your SOC 2 audit
April 2021
A-Lign

CPRA, GDPR, Virginia CDPA, and NY Shield Act Essential Things You Need to Know
March 2021
Professional Evaluation and Certification Board (PECB)

Data Privacy Trends in 2021: Compliance with New Regulations
February 2021
Professional Evaluation and Certification Board (PECB)

IT Digital Privacy in Europe
2021 | Coursera | Grade Achieved: 90%
Credential ID: 57E9D65BRK8B