International Journal of Technology 15(1) 219-229 (2024)
Received Auguts 2022 / Revised October 2022 / Accepted June 2023

International Journal of Technology

Towards a Management System Framework for the Integration of Personal Data Protection and Data Governance: A Case Study of Thai Laws and Practices

Hathairat Ketmaneechairat[1*], Maleerat Maliyaem[2], Puttakul Puttawattanakul[2]

[1]*College of Industrial Technology, King Mongkut's University of Technology North Bangkok, Bangkok, 10800, Thailand*
[2]*Information Technology and Digital Innovation King Mongkut's University of Technology North Bangkok, Bangkok, 10800, Thailand*

Abstract. Thailand's Personal Data Protection Act, B.E. 2562 (2019), is now in effect. Moreover, the General Data Protection Regulation (GDPR) has been deemed fully operational. These two regulations have been mentioned in order to improve all Thai and international economic sectors as well as Thai public sectors. This study's objective is to establish a new management system framework for firms that wish to comply with standards while incorporating a data governance framework. This framework will be known as the Framework for Personal Data Protection Integrated Data Governance Management System (PDP-DGMS). Subject matter experts validate PDP-DGMS with the Index of Item Objective Congruence (IOC). The results demonstrate that the framework's components are acceptable. The PDP-DGMS implementation will serve as a consulting direction for low-cost adoption and process enhancement, both of which will largely benefit SMEs.

Keywords: Governance; Management system; Personal data protection; Thai laws

1. Introduction

The cumulative summary fines for GDPR (Voigt and Bussche, 2017) non-compliance have been assessed up to 1,050,587,602€, which is a frightening figure that companies should not take any chances with. In order to comply with regulations, organizations attempt to build a personal data protection framework as a guideline. However, effective implementation of personal data protection is incomplete without a robust data governance structure and framework. Engaging consulting firms could cost millions of Thai Baht, making it inappropriate for start-ups and small and medium-sized enterprises. In addition, achieving legal compliance is a continual process that necessitates organizations to perform duties to maintain their level of maturity and prevent nonconformities resulting from inefficient management practices. This statement introduces the research topic for the proposed process-oriented framework, which is referred to as "a Framework for Personal Data Protection Integrated Data Governance Management System (PDP-DGMS)", and aids in the implementation of a personal data protection structure that is integrated with data governance. PDP-DGMS is suitable for Thai-based organizations working in the Thai legal environment.

[*]Corresponding author's email: hathairat.k@cit.kmutnb.ac.th, Tel.: +66-65-6656-426
doi: 10.14716/ijtech.v15i1.5885

2. Related Works

The Personal Data Protection Act B.E. 2562 (PDPA) has been authorized and implemented in Thailand across a wide range of organizations and academic institutions.Similarities between the PDPA and the GDPR (Formichella *et al.,* 2021), severe penalties for non-compliance, the PDPA becomes a top worry and duty for businesses. In an effort to deconstruct and acquire a complete grasp of how a firm may plan for and handle a legal situation when personal data is still important for corporate expansion, the PDPA has attracted considerable attention (Dowpiset and Nuangjamnong, 2021; Naparat, 2020).

2.1. Thai Personal Data Protection Act. B.E. 2562 (2019)

Since 1998, personal data protection in Thailand has been the subject of academic and scientific inquiry (Methakunavudhi, 1998). When the data protection authority (Greenleaf and Suriyawongkul, 2019), the Personal Data Protection Committee, establishes the rules, the "Personal Data Protection Act B.E. 2562" might become one of the harshest data privacy laws in Asia (PDPC). The PDPA contains a total of 96 sections, which are organized into seven chapters and one transitional phrase. Several businesses are in the process of developing and adjusting their business processes to meet regulatory requirements and norms. The Thailand Data Protection Guidelines 3.0 (TDPG), as outlined by Bunaramrueang (2020), serve as a valuable resource for information related to implementation. The guidelines comprise 14 core chapters and encompass various industrial guidelines (from A to N).

2.2. Data Governance Framework

Data governance is an emerging topic in information management and is closely related to IT governance (Cheong and Chang, 2007). It refers to the decisions that must be made to enable the successful administration and utilization of IT (Khatri and Brown, 2010). Data Governance (DG) may refer to the exercise of authority and control over the management of data in support of a decision-making process for the efficient management and use of information technology (Abraham, Schneider, and Brocke, 2019). To support the national vision for digital transformation, the Thailand Digital Government Development Agency (Public Organization) (DGA) promotes the use of data governance in the public sector on a continual basis. The study highlights the significance of government data governance in connection to the expansion of digital government and identifies key considerations for the framework (Chullachakkawat *et al.,* 2020; Jairak, Praneetpolgrang, and Subsermsri, 2020). In accordance with Figure 1's depiction of the data management lifecycle, the Data Governance Framework (DGF) produced by DGA contains ten domains.

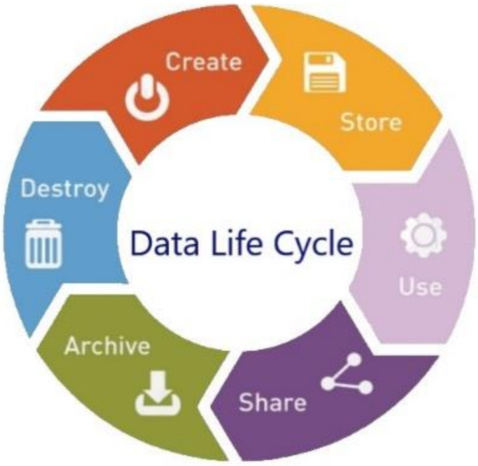

Figure 1 Data Life Cycle in Thai Data Governance Framework by DGA

The framework includes coverage for data security and privacy. Since personal data may be classified as private information, it is crucial to underline the importance of personal data protection within the context of data governance. indviduals responsible for collecting, processing, disseminating, and retaining personally identifiable information bear specific obligations and duties.

2.3. Management System and Standards

The objective of the integrated management system, which has been studied for decades (Heras-Saizarbitoria and Boiral, 2013; Wilkinson and Dale, 1999), is to identify the integration of many business-relevant areas, such as quality, environmental, and safety management. ISO Annex SL, as introduced by Tricker (2019), serves as the standard model for the Management System Structure (MSS), replacing ISO Guide 83. The Annex SL contains the following "High-Level Structure" clauses: Scope, Normative References, Terminology and Definitions, Organizational Context, Leadership, Planning, Support, Operation, Performance Assessment, and Improvement (Tančić, 2014).

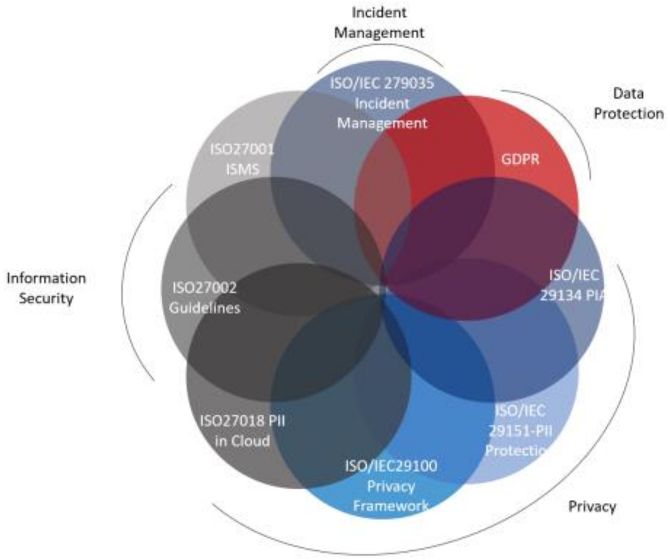

Figure 2 The Building Blocks of ISO/IEC 27701:2019 adapted from (Shaikh 2020).

Although paragraphs 1-3 aim to provide information in accordance with a certain international standard, clauses 4-10 will outline the real requirements and commence implementation. ISO/IEC 27701:2019 specifies the management system for managing personal data and protecting data subject privacy (Lachaud, 2020). The methodology for the integration of the GDPR and ISO27701 incorporates research and innovation (Anwar and Gill, 2020). Yet, without Data Governance, the security of personal data may not be adequately protected. The conceptual design of this study is studied and adopted from the works depicted in Figure 2. However, the MSS must be consistent with the requirements of PDPA and DGF integration; these requirements apply to DGF's unresolved components. Figure 1's advice does not cover the management framework or the protection of personal data throughout the lifecycle of the data. The layout of the management system and consideration of rules for the protection of personal data are crucial components of the PDP-DGMS implementation of this research.

3. Personal Data Protection Integration with Data Governance

PDP-DGMS is a process-oriented innovation and conceptual design for protecting personal data. It aims to decrease the risks identified in the area of personal data protection by providing the structure and selection of controls for the management system. It provides a framework for establishing PDPA compliance procedures and adapting to similar regulatory requirements. Due to the fact that PDP-DGMS is not meant to be the only choice, it cannot guarantee compliance with specific regulatory requirements. Organizations must modify PDP-DGMS to meet their needs and expectations. Figure 3 displays the conceptual design of the PDP-high DGMS. There are two primary design aspects, namely 1) Management system for the protection of personal data; and 2) controls for the protection of personal data.

3.1. Personal Data Protection Governance Management System (PDPG-MS)

The management system is described in the PDPG-MS, which also includes DGF's recommendations for establishing a data governance structure based on Annex SL and ISO27701. The separate section of this paper covers the description that is being made.

3.2. Personal Data Protection Governance Controls (PDPG-C)

PDPG-C extracts the governance controls, which include a few control domains, control domain objectives, and controls, based on recommendations from DGF and TDPG. However, the characteristics of each control will be presented in a separate study report as part of future work. This isolated section addresses the PDPG-C outline described in this paper.

3.3. Verification of PDP-DGMS

The PDP-DGMS verification considers both the PDPG-MS and PDPG-C verification results, along with the judgments from statistical expert reviews. The results will be listed in a separate section.

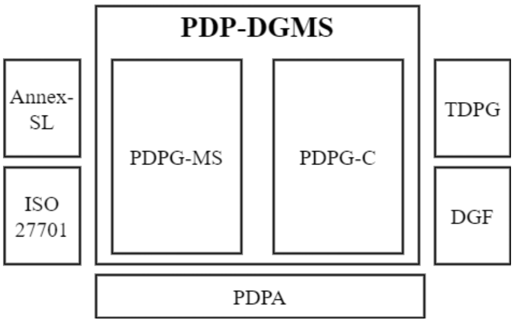

Figure 3 High-Level Structure Design of PDP-DGMS

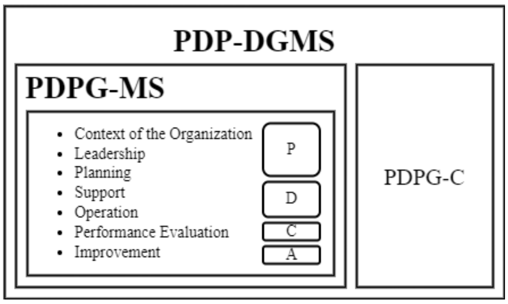

Figure 4 Design of PDP-DGMS

4. Personal Data Protection Governance Management System

4.1. Context of the Organization

Organizations should have a clear understanding of the expectations of various stakeholders. Stakeholders in the context of the PDPG-MS may include data subjects (the owners of personal data), data protection officers (DPOs), PDPC (Personal Data Protection Commission), staff members, shareholders, suppliers, outsourcers, business partners, and data processors, among others. It will be determined what these interested parties' needs and expectations are in terms of personal data protection and governance. Organizations should also take into account internal and external factors like GDPR and pertinent laws that may affect implementation and governance. However, to extract expectations and requirements, it is essential to implement a set of controls, which are detailed in the PDPG-C section, in accordance with the PDPG-MS. The identified interested parties imply the extent of personal data protection governance, and different company services and procedures may involve various specified interest groups. The scope of the governance for personal data protection should be made known to the public and suitably shared with the necessary parties. Organizations will be able to resolve the problem of who is concerned with whose personal data and how once they have this knowledge and insight.

Figure 4 illustrates how the PDPG-MS is formally constructed using the Annex SL as the high-level structure and expressed using the PDCA method. Clauses can be interpreted in a variety of ways; hence, the PDPG-MS does not consciously imply orderly execution.

4.2. Leadership

In Figure 5. The specialized steering group and PDPG-MS team are assigned by top management. The Data Governance Steering Committee (DGSC) is made up of executives and senior managers from several departments or business units who are concerned with data security. This steering group is responsible for the PDPG-MS enforcement, PDPG-MS improvement, and other leadership-related initiatives. The Data Governance Working Team (DGWT) is assigned by and established by the authority of DGSC, which is in charge of managing, directing, and controlling PDPG-MS. DGWT transforms policies into practices by integrating PDPG-MS into business operations. This team will also report on the effectiveness of PDPG-MS for potential future improvement. Data Custodian Teams (DCT) are business divisions and departments that use corporate data assets, regardless of the type of data. DCT is in charge of monitoring day-to-day activities and ensuring that procedures and policies are consistent. The "Data Protection Officer Team" (DPOT) is the collective of DPOs responsible for safeguarding personal data, primarily for legal compliance, which is understood to be the organization's context. The DGSC may assign to DPOT any extra responsibilities that are lawfully appropriated, in addition to the standards and expectations outlined in regulations. Although DPOT may include executive-level employees, it should directly report to the DGSC or senior management. The Data Protection Internal Auditor (DPIA), who is responsible for any significant nonconformities to internal and external regulations, conducts the PDPG-MS audit.

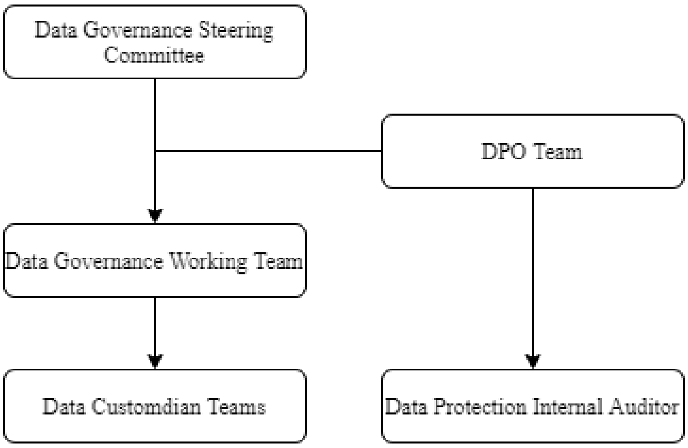
Data Governance Steering Committee
DPO Team
Data Governance Working Team
Data Customdian Teams
Data Protection Internal Auditor

Figure 5 PDPG-MS Basic Structure

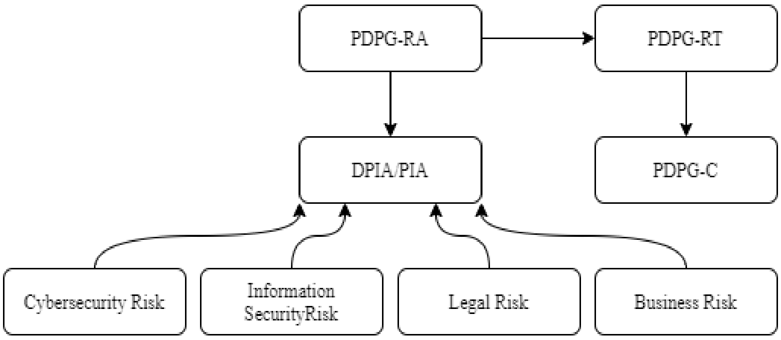

Figure 6 The relationship between PDPG-RA, PDPG-RT, PDPG-C, and PIA

4.3. Planning

Planning entails a series of activities and procedures that must be scheduled at the appropriate intervals. These include risk assessment for personal data protection governance (PDPG-RA), risk treatment for personal data protection governance (PDPG-RT), and personal data protection governance objectives. Unlike Privacy Impact Assessment (PIA), PDPG-RA aims to capture the high-level risks that affect the effectiveness of the PDPG-MS; these risks may lead to the causes of identified risks to personal data, which may involve PIA. PDPG-RA can be viewed as enterprise risk management, which incorporates multiple risk perspectives and domains, including legal, operation, finance, cybersecurity, information security, and privacy. The PDPG-RA results should be considered in the PIA process because an ineffective PDPG-MS may cause severe risks to personal privacy in an overall manner; this means that the PDPG-RA results will not point to each individual privacy or a personal dataset, but the results may cause the breach broadly. PDPG-RT is the subsequent procedure and handling of PDPG-RA results; it unveils an unacceptable level of risk to the treatment strategies and control selection of PDPG-C. PDPG-RT necessitates DGSC approval before DGWT can take action to mitigate risks. Both PDPG-RA and PDPG-RT must be aligned with the international risk management standard (International Organization Standardization, 2009). The personal data protection governance objectives serve as performance indicators for the PDPG-MS. DGSC should assign measures that are pertinent to the organization's context. The Goal-Question-Metric Plus (GQM+) (Basili *et al.*, 2007) technique is generally advised for establishing measurements and analyses that ensure alignment with organization strategies. Figure 6 graphically depicts this relationship.

4.4. Support

Clause 7, the Support Clause, is the core of the proposed management system framework. According to the PDCA model, support requirements are necessary not only in the "do" phase but also in the "plan," "check," and "act" phases. PDPG-MS subsequently adopts the support clause for the majority of its components. According to Annex-SL, support encompasses multiple facets, including resources, competence, awareness, communication, and documented information. Nevertheless, this paper modifies the support clause from a different perspective. PDPG-MS makes use of the iron triangle (Caccamese and Bragantini, 2012), time, cost, quality, scope, and the people-process-technology triangle (Javaid and Iqbal, 2017). Figure 7 displays this integration.

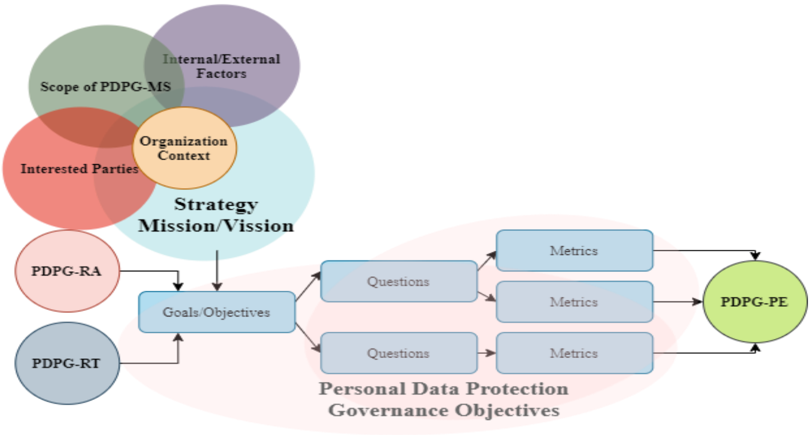

Figure 7 The relationship between organization context, PDPG-RA, PDPG-RT, PDPG-Objective, and PDPG-PE

People, Processes, and Technology elicit Annex-SL requirements coverage. Process refers to the supporting processes that contribute to the PDPG-MG. People refer to the roles, responsibilities, skills, and knowledge of interested parties under the PDPG-MS. Technology is the collection of tools and technologies used to support PDPG-MS. Time-Budget-Scope Triangle is used as a contribution to the support clause in PDPG-MS. This model is interpreted as the constraint that senior management should monitor and provide support for PDPG-MS implementation. Scope refers to the clearly defined limits of the PDPG-MS as supporting information for the governance management system. Budget is one of the constraints that senior management must allocate to the PPT framework's support. Time refers to the milestones and planned intervals that top management may pre-determine to establish the intended timeframe. The integration between the Time-Budget-Scope Triangle and the PPT framework forms the support clause in PDPG-MS shown in Figure 8.

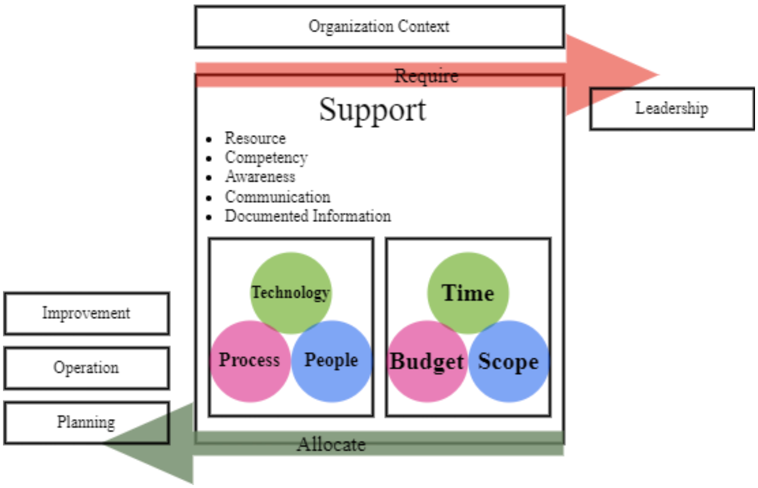

Figure 8 The integration between Time-Budget-Scope Triangle and PPT framework

4.5. Operation

This includes the execution of PDPG-RA, PDPG-RT, and selected PDPF-C controls.

4.6. Performance Evaluation

The objective of Performance Evaluation (PDPG-PE) is to ensure the efficacy of PDPG-MS. This activity may include audit, objective measurement and analysis, and management review as sub-activities. Audit refers to independent process adherence; it is used to determine if PDPG-MS has been implemented in accordance with its defined policies and procedures. Objective measurement and analysis entails measuring the defined objectives against criteria and thresholds and analyzing the results to extract useful information and knowledge from the PDPG-MS implementation. Lastly, DGSC and top management are responsible for reviewing the results of implementation and decision-making and directing continuous improvement through management review.

4.7. Improvement

The outcome of PDPG-PE is used to enhance PDPG-MS. There is a connection between the PDPG-PE, Support, and Improvement clauses, as improvement always necessitates allocated resources and support, as shown in Figure 9.

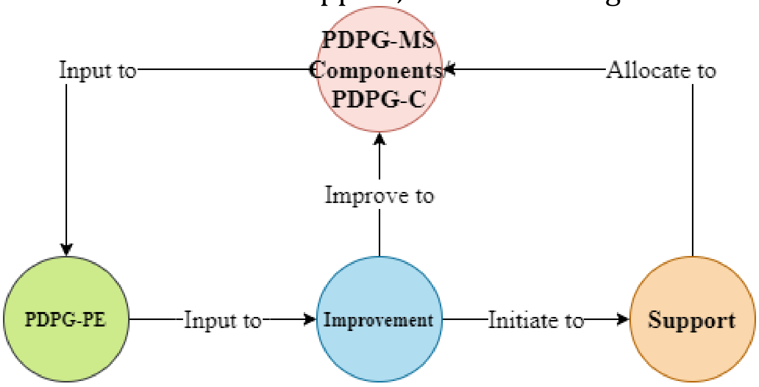

Figure 9 The relationships in continuous improvement.

5. Personal Data Protection Governance Controls

PDPG-C is a set of controls used in the governance of personal data; its purpose is to mitigate risks associated with the collection, use, processing, distribution, storage, and disposal of personal data. PDPG-C is designed utilizing the data lifecycle in DGF as its core domains and TDPG as its specific controls. Additionally, ISO27701 introduces additional controls to be considered for compliance with the international standard, whereas PDPA does not. The PDPG-C then incorporates the knowledge bodies from these three areas, ISO27701, DFG, and TDPG, into the domains and subdomains as in Table 1.

Table 1 Domain and sub-domains in PDPG-C.

Domain	Description	ISO	TDPG	DGF
C1	Personal Data Architecture			
C1.1	Understand Context of Personal Data Protection	X		
C1.2	Personal Data Flow/Journey		X	X
C1.3	Personal Data Classification		X	
C1.4	Lawful Basis for Processing		X	
C1.5	Data Processor Management	X	X	
C1.6	Personal Data Migration Plan			X
C2	Leadership			
C2.1	Assignment for Personal Data Protection and Governance	X	X	X
C2.2	Personal Data Protection Policy and Framework	X	X	X
C3	Personal Data Protection and Governance Risk Management			
C3.1	Data Protection Impact Assessment	X	X	
C3.2	Management of Information Security and Cybersecurity Risk	X		
C4	Support of Personal Data Protection and Governance			
C4.1	Human Resource	X		X
C4.2	Budget Allocation	X		

Table 1 Domain and sub-domains in PDPG-C (Cont.)

Domain	Description	ISO	TDPG	DGF
C4.3	Technologies for Personal Data Protection and Governance		X	
C4.4	Processes for Personal Data Protection and Governance	X		X
C5	Operation of Personal Data Protection and Governance			
C5.1	Personal Data Protection Technical Peer Review	X		
C5.2	Incident and Breach Notification Management	X	X	
C5.3	Personal Data Modelling			X
C5.4	Personal Data Storing	X	X	X
C5.5	Personal Data Integration and Transfer	X	X	X
C5.6	Personal Data Documentation and Content Management			X
C5.7	Personal Data Analytic		X	X
C5.8	Personal Meta Data			X
C5.9	Security and Privacy in Operation	X	X	X
C5.10	Personal Data Quality			X
C6	Performance Evaluation			
C6.1	Objective Measurement and Analysis	X		
C6.2	Executive Review	X		
C6.3	Personal Data Protection Independent Audit	X		
C7	Improvement			
C7.1	Improvement Planning	X		

6. Methodology

The verification procedure consists of four stages as follows:

- *Initializing Stage*

Five experts with experience implementing PDPA, DG, and ISO27701 or related topics have been selected.

- *Verification Stage*

The selection of five experts with criteria 1) Years of experience, 2) educational background, and 3) academic foundation.

- *Validation Stage*

The results of the IOC are examined by specialists, who then engage in an open discussion over the conclusion.

- *Finalizing Stage*

The finalized proposed framework is announced and distributed along with survey questionnaires to public seminars in order to validate the confidence level of the survey target regarding the potential applications of the PDPG-MS.

7. Result and Discussion

Table 2 s IOCs that meet the criteria (0.5) without major disagreement.

Table 2 IOC result

Component	E1	E2	E3	E4	E5	IOC
		PDPG-MS				
Context of the Organization	1	0	1	1	1	0.8
Leadership	1	1	1	1	1	1
Planning	1	1	1	1	1	1
Support	1	0	1	1	0	0.6
Operation	1	1	1	1	1	1

Table 2 IOC result (Cont.)

Component	E1	E2	E3	E4	E5	IOC
Performance Evaluation	1	1	1	1	1	1
Improvement	1	1	1	1	1	1
PDPG-C						
C1	1	1	1	1	1	1
C2	1	0	1	1	0	0.6
C3	1	-1	1	1	1	0.6
C4	1	0	1	1	1	0.8
C5	1	0	1	1	1	0.8
C6	1	-1	1	1	1	0.6
C7	1	1	1	1	1	1

The survey result in Table 3 indicates a significant acceptance of the proposed framework from 1,375 respondents ($\bar{X} = 4.48, N = 1{,}375$), which a sampling size of 400.

Table 3 The survey result on PDPG-C controls

PDPG-C	Domain	Number of Controls	Average score	percentage
C1	Personal Data Architecture	6	4.59	93.79
C2	Leadership	2	4.59	93.55
C3	Personal Data Protection and Governance Risk Management	2	4.52	90.99
C4	Support of Personal Data Protection and Governance	4	4.58	93.20
C5	Operation of Personal Data Protection and Governance	10	4.22	77.84
C6	Performance Evaluation	3	4.50	90.86
C7	Improvement	1	4.39	84.96

8. Conclusions

IOC and survey findings indicate that PDPG-MS is the most important component of PDP-DGMS. The validation by the expert panel verifies the adequacy of the proposed framework as the foundational concept for small to medium-sized businesses. The proposed approach is further validated through a quantitative survey involving individuals from both the public and private sectors with IT-related backgrounds. Regrettably, the recommended controls are not yet fully linked with the objective, as the operation controls may necessitate an investment in technology and resources. In future work, the implementation of PDP-DGMS will serve as a guiding resource for cost-effective adoption and process enhancement. These aspects are expected to significantly benefit SMEs.

References

Abraham, R., Schneider, J., Brocke, J.V., 2019. Data Governance: A Conceptual Framework, Structured Review, and Research Agenda. *International Journal of Information Management,* Volume 49, pp. 424–438

Anwar, M.J., Gill, A.Q., 2020. Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model. *In:* Australasian Conference on Information Systems

Basili, V., Heidrich, J., Lindvall, M., Munch, J., Regardie, M., Rombach D., Trendowicz, A., 2007. GQM+Strategies: A comprehensive Methodology for Aligning Business Strategies with

Software Measurement. *In:* First International Symposium on Empirical Software Engineering And Measurement, pp. 488–490

Bunaramrueang, P., 2020. Thailand Data Protection Guidelines 3.0. Faculty of Law, Chulalongkorn University, pp. 1–666

Caccamese, A., Bragantini, D., 2012. Beyond the Iron Triangle: Year Zero. Paper presented at PMI® Global Congress 2012—EMEA, Marsailles, France. Newtown Square, PA: Project Management Institute

Cheong, L. K., Chang, V., 2007. The Need for Data Governance: A Case Study. *In:* 18th Australasian Conference on Information System, pp. 999–1008

Chullachakkawat, C., 2020. Data Governance and Digital Government Development. *School of Administrative Studies Academic Journal,* Volume 3(2), pp. 123–135

Dowpiset, K., Nuangjamnong, C., 2021. An Investigation of Factors Affecting Intention to Comply Thailand PDPA with E-Services in Private University towards social media. *International Journal of Economics & Business Administration*, Volume 9(2), pp. 374–393

Formichella, J.P., Jamallsawat, N., McNair, B., Brikshasri, A., 2021. Thailand: Comparing privacy laws: GDPR v. Thai Personal Data Protection Act. OneTrust DataGuidanceTM, pp. 1–56

Greenleaf, G., Suriyawongkul, A., 2019. Thailand–Asia's Strong New Data Protection Law. Privacy Laws & Business International Report, pp. 1-7

Heras-Saizarbitoria, I., Boiral, O., 2013. ISO 9001 and ISO 14001: Towards A Research Agenda on Management System Standards. *International Journal of Management Reviews*, Volume 15(1), pp. 47–65

Jairak, K., Praneetpolgrang, P., Subsermsri, P., 2015. Information Technology Governance Practices Based on Sufficiency Economy Philosophy in the Thai University Sector. *Information Technology & People*, Volume 28(1), pp. 195–223

Javaid, M.I., Iqbal, M.M.W., 2017. A Comprehensive People, Process and Technology (PPT) Application Model for Information Systems (IS) Risk Management in Small/Medium Enterprises (SME). *In:* International Conference on Communication Technologies (ComTech), pp. 78–90

Khatri, V., Brown, C. V., 2010. Designing Data Governance. *Communications of the ACM,* Volume 53(1), pp. 148–152

Lachaud, E., 2020. ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification. *European Data Protection Law Review Journal,* Volume 6(2), pp. 194–210

Methakunavudhi, P., 1998. A Guideline for Data Protection Legislation in Thailand. *ACM SIGCAS Computers and Society,* Volume 28(3), pp. 28–30

Naparat, D., 2020. Exploring Thailand's PDPA Implementation Approaches and Challenges. *In:* ACIS 2020 Proceedings, pp. 1–8

Tančić, D., 2014. Harmonization of Management Systems According to the Requirements of Annex Sl. *In:* International Conference on Strategic Management - IMKSM2014, pp. 1–8

Tricker, R., 2019. What is Annex SL all about? In: *Quality Management Systems.* Routledge: London

Voigt, P., Bussche, A.V.D., 2017. *The EU General Data Protection Regulation (GDPR) : A Practical Guide.* Cham: Springer International Publishing

Wilkinson, G., Dale, B. G., 1999. Models of Management System Standards: A Review of the Integration Issues. *International Journal of Management Reviews*, Volume 1(3), pp. 279–298