International Journal of Instructional Cases
ISSN: 2399-830x

The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand

Chadsada Tungtrakul *
[1]Faculty of Business Administration, King Mongkut's University of Technology North Bangkok, Thailand.
ORCID: https://orcid.org/0009-0000-9594-9224
Email: c.tungtrakul@gmail.com

Thitirat Thawornsujaritkul
[2]Faculty of Business Administration, King Mongkut's University of Technology North Bangkok, Thailand.
ORCID: https://orcid.org/0009-0007-8887-9409
Email: thitiratth@kmutnb.ac.th

Thanin Silpcharu
[3]Faculty of Business Administration, King Mongkut's University of Technology North Bangkok, Thailand.
ORCID: https://orcid.org/0000-0001-9503-2379
Email: tanin.s@fba.kmutnb.ac.th

*Corresponding Author Email: c.tungtrakul@gmail.com

Received Date: 11-06-2024; Accepted Date: 30-11-2024; Publication Date: 27-12-2024

Abstract
The Personal Data Protection Act 2019 (PDPA) is a statute that governs the protection of personal data, making it crucial for the industrial business sector to adhere to the law and establish effective guidelines. This research aims to investigate the approaches for managing personal data protection in the industrial business sector through qualitative and quantitative research methods. The qualitative research included In-Depth Interviews with nine experts, as well as Focus Group Discussions with 11 qualified specialists. The quantitative study involved a survey of 500 executives within the industrial business sector, with the data analysed using descriptive, inferential, and multivariate statistics. The findings revealed that the Guidelines for Information

How to cite (APA):
Tungtrakul, C., Thawornsujaritkul, T., Silpcharu, T. (2024). The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand. *International Journal of Instructional Cases*, *8*(2), 196-210.
International Journal of Instructional Cases

International Journal of Instructional Cases
ISSN: 2399-830x

Technology Management concerning Personal Data Protection in the Industrial Business Sector in Thailand comprise four key aspects, ranked according to their mean levels of importance as follows: 1) Laws and Governance ($\bar{X}$ = 4.20), 2) Audit and Evaluation ($\bar{X}$ = 4.19), 3) Internal Control ($\bar{X}$ = 4.16), and 4) Organisational Support ($\bar{X}$ = 4.15). The most significant aspects identified within each category were: understanding the legal standards associated with the Personal Data Protection Act, establishing regular audits and monitoring of personal data storage in accordance with legal standards, developing guidelines for managing personal data security systems, and collaborating with leading external technology organisations such as Microsoft to assess the security of information systems. The hypothesis test results indicated that executives from different industrial business sectors, including Manufacturing and Services, consistently recognised a statistically significant level at 0.05. The analysis of the Structural Equation Model (SEM) demonstrated that the model met the assessment criteria and aligned with the empirical data. The assessed values for the chi-square probability, relative chi-square, goodness-of-fit index, and root mean square error of approximation were 0.188, 1.096, 0.965, and 0.014, respectively.

Keywords: Students Learning Satisfaction, Perseverance, Flow Experience, Learning Motivation, Vocational Education.

Introduction

In the contemporary era, technology and vast amounts of data drive both the economy and society. Data serves as a critical resource, underpinning business operations in the "Digital Age." Personal data, in particular, has become increasingly valuable and essential for the functioning of modern businesses.

Technological advancements have facilitated the rapid dissemination of personal data, However, the misuse of personal data—whether through negligence or insufficient control measures—can lead to significant issues for data owners, including inconvenience, distress, and financial or reputational damage. These issues may result in lawsuits, compensation claims, and broader harm to the organisation. Consequently, the prioritisation of privacy rights and the protection of personal data is imperative. To address these concerns, Thailand has enacted the PDPA, which serves as a comprehensive framework for safeguarding personal data. The average total cost of a personal data breach, as illustrated in Figure 1, underscores the critical need for robust measures to ensure data protection compliance and mitigate potential risks.

Figure 1 illustrates that the average total cost of a personal data breach increased from \$3.62 million in 2017 to a record high of \$4.45 million in 2022. Thailand began enforcing the PDPA on 1st June 2022. Between 2022 and 2023, the average total cost of leaked personal data in the industrial business sector exhibited a consistently rising trend. Consequently, the industrial business sector must prioritise strict compliance

International Journal of Instructional Cases
ISSN: 2399-830x

with the PDPA 2019, aligning with the Strategic Plan for the Promotion and Protection of Personal Data of Thailand 2024–2027. This strategic initiative aims to drive Thailand towards achieving the law's highest objectives and intent. In 2024, the government will commence the development of policy guidelines to assist business operators in handling personal data in accordance with appropriate and legally compliant standards. This initiative provides an opportunity to establish robust personal data management practices, enhancing organisational credibility and fostering a positive corporate image grounded in good governance. Building trust in this manner encourages customer loyalty, thereby offering a competitive advantage and strengthening the industrial business sector's capacity in the market.

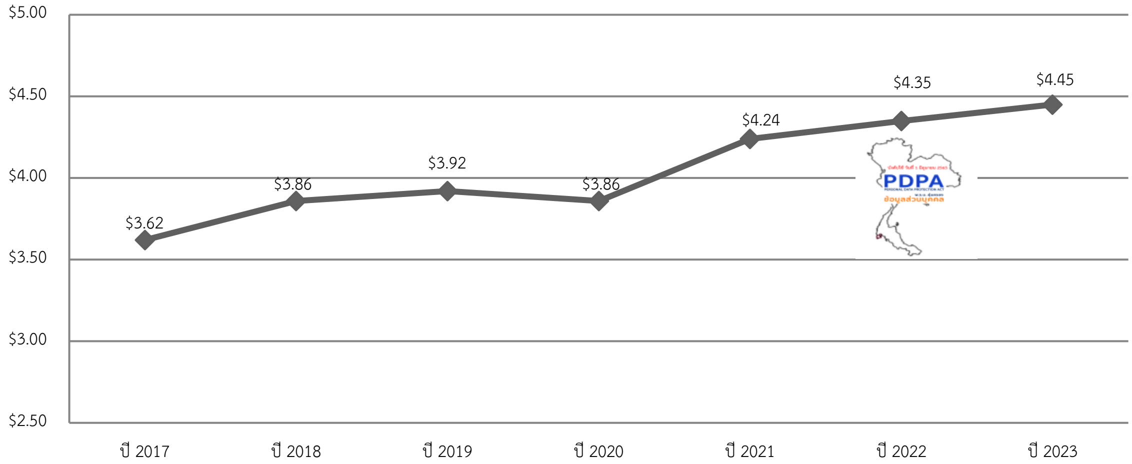

Figure 1: The Average Total Cost of Personal Data Breaches in the Industrial Business Sector
Source: The Cost of Data Breach Report 2023.

Objectives

1. To study the components of the management approach to The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand.
2. To develop a structural equation model to The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand

Literature Review

In contemporary corporate management, information technology is utilised to enhance efficiency. Data plays a pivotal role in digital businesses, and its effective management contributes significantly to organisational growth and success. Industrial business operators are required to manage critical data comprehensively, encompassing its collection, storage, processing, analysis, and appropriate disclosure, tailored to the nature of the business (Taherdoost, 2022). Furthermore, these operators

International Journal of Instructional Cases
ISSN: 2399-830x

must understand their legal "status" in data operations, which includes:

1. Personal Data Controller: Individuals or legal entities authorised to make decisions regarding the collection, use, or disclosure of personal data.
2. Personal Data Processor: Individuals or legal entities that collect, use, or disclose personal data based on the instructions of, or on behalf of, the Personal Data Controller.

If the aforementioned activities are performed independently of instructions or without acting on behalf of a Personal Data Controller, the entity assumes dual roles as both a Personal Data Controller and a Personal Data Processor. Effective personal data management necessitates a well-defined operational policy, with leadership fostering and supporting principles of Diversity, Equity, and Inclusion (DEI) to generate positive organisational outcomes. Emphasis should be placed on effective organisational management, grounded in Management Concepts and Organisation Theory. This involves setting objectives, defining clear structures and responsibilities, organising personnel, making decisions and issuing directives aligned with designated roles, controlling processes and evaluations, fostering collaboration, preparing comprehensive reports, and allocating budgets to establish and sustain standards and practices. These foundational elements enable the analysis of organisational structures and the identification of essential components necessary for creating an effective framework for Information Technology Management in Personal Data Protection within Thailand's industrial business sector. The resulting guidelines can serve as a replicable model for future entrepreneurial success. These elements can be synthesised into four key aspects as follows:

1. Laws and Governance: This encompasses a system of rules enforced by an authoritative entity, such as the government, to regulate behaviour, ensure order, and facilitate administration in alignment with principles of good governance (Cogan, 2023). It represents the interplay of civil society, as well as private and public sectors, necessitating a balance of roles among these entities to foster effective coexistence and execution of responsibilities. For businesses, adherence to proper practices is critical to mitigating the risk of fines and maintaining customer trust (Machado et al., 2023). Strict measures, including mandatory reporting, inspections, and penalties for legal violations, have been implemented in various domains (Kuner et al., 2021). Furthermore, fostering morality, ethics, and honesty, alongside respecting rights and avoiding infringements in business operations and social responsibilities, is essential for achieving broad acceptance and legitimacy (Alkhafaji, 2011).
2. Organisational Support: This refers to the organisational framework, including decision-making authority, systems, personnel development, performance evaluation, rewards, and systematic work processes. It encompasses strategic

International Journal of Instructional Cases
ISSN: 2399-830x

goal setting, dissemination of policy information throughout the organisation, and the creation of a conducive work environment, including the provision of tools, equipment, and software to enhance communication and social skills development. Organisational culture is equally important, with an emphasis on supervisor and employee behaviours, and the establishment of shared goals to support teamwork.

Aligned with Eisenberger et al. (2001) and the principles of Organisational Support Theory (OST), retaining valuable human resources requires fostering sentiments, beliefs, and attitudes that align with organisational benefits. This approach encourages employee commitment and behaviours that contribute to organisational success. Support from the organisation must span various dimensions, including financial rewards, opportunities for promotion, quality-of-life improvements, recognition of opinions, participation, and skill development. This support can be evaluated through four key areas: 1) Performance, 2) Opportunities for growth and development within the organisation, 3) The organisation's concern for employee well-being, and 4) Recognition and appreciation of employee contributions. Effective resource sharing and allocation strengthen organisational resilience, simplify operational complexities, and promote sustainable business practices (Gordon et al., 1993).

3. Internal Control: This refers to organisational processes designed to ensure that operations align with established goals and objectives. It involves fostering a culture of honesty and ethics, as well as developing a robust organisational structure and governance system. Key elements include identifying and assessing operational risks and formulating strategies to mitigate them. Policies and procedures are implemented to guide operations towards achieving objectives, such as approval mechanisms, inspections, segregation of duties, information collection and dissemination, and the creation of channels for addressing personnel misconduct. Additionally, the use of banking applications to facilitate payment inspections and ensure transparent financial transactions is critical. Corruption prevention measures, alongside leadership that exemplifies morality and ethics, further enhance the effectiveness of internal controls (Alkhafaji, 2011).
4. Audit and Evaluation: This involves systematic methods to examine and analyse organisational or project operations to ensure compliance with goals and effectiveness. Auditing assesses the accuracy, completeness, and reliability of data and operations, conducted by either internal units or external agencies. The primary aim is to enhance internal processes or provide impartial, independent opinions. This process requires independent auditors and evaluators, free from conflicts of interest, to measure and analyse outcomes. Transparency, participation from relevant stakeholders, and adherence to

International Journal of Instructional Cases
ISSN: 2399-830x

ethical practices are crucial throughout the audit and evaluation process.

Auditing and evaluation provide assurance and independent recommendations that add value and enhance operational effectiveness. Internal auditing specifically improves organisational risk management, control, and governance processes, ensuring they remain relevant in contemporary contexts. Future auditing and evaluation should incorporate advanced technologies, such as Artificial Intelligence (AI) and Big Data Analytics, to enhance accuracy and enable continuous, real-time assessments (Byrnes et al., 2018).

Conceptual Framework of the Research

The conceptual framework of the research is presented in Figure 2.

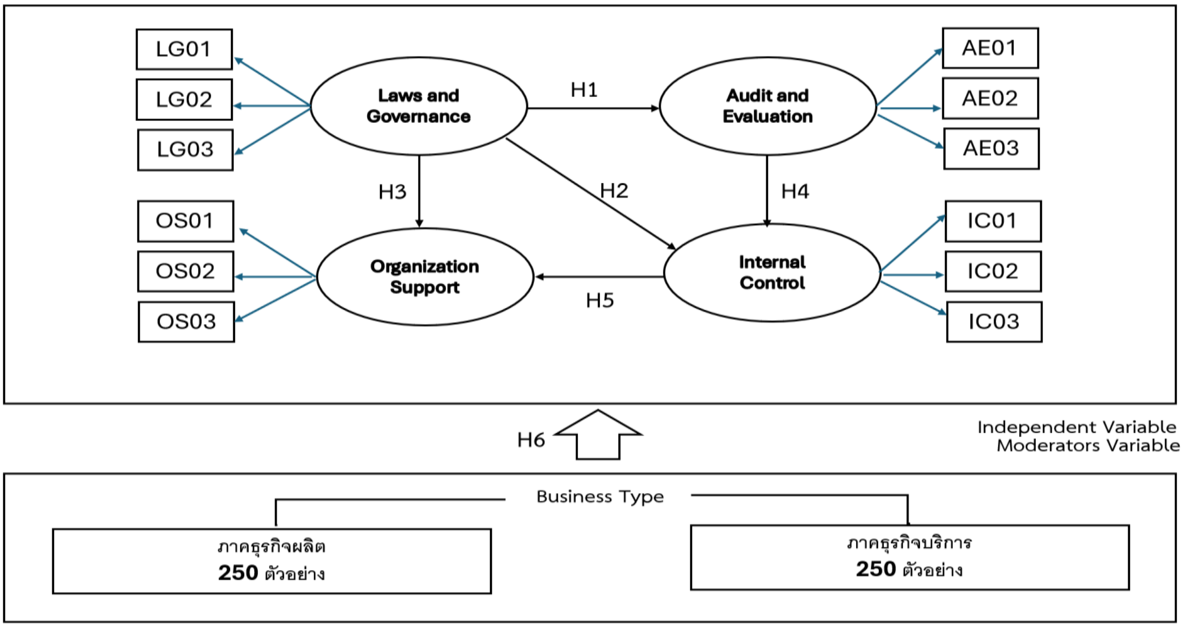

Figure 2: Conceptual Framework of the Research on The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand.

Methodology

This research employs an inductive approach using a mixed-methodology technique, as endorsed by the Doctor of Business Administration Programme in Industrial Business Administration, Faculty of Business Administration, King Mongkut's University of Technology North Bangkok, Thailand. The study comprises the following three steps:

Step 1: Qualitative Research

This phase involved in-depth interviews with a purposive sample of nine experts, divided into three groups:

International Journal of Instructional Cases
ISSN: 2399-830x

1. Three executives or entrepreneurs from industrial business organisations.
2. Three representatives from the government sector or related organisations.
3. Three academics with relevant expertise.

Step 2: Quantitative Research

A survey was conducted among executives from organisations complying with the Personal Data Protection Committee Announcement under Section 41(2) of the PDPA 2019, comprising a population of 1,156 entities. A sample size of 500 respondents was determined using multi-stage sampling, as follows:

- Cluster Sampling divided the businesses into two categories:
  1. 250 manufacturing businesses.
  2. 250 service businesses.
- The Probability Sampling method was employed using the Lottery Method technique.

Research instruments included questionnaires with checklist and scale questions based on a 5-point Likert scale.

- The Index of Item-Objective Congruence (IOC) for the 100 questions related to research objectives ranged from 0.60 to 1.00.
- The standard deviation values for checklist questions ranged between 0.407 and 2.638, and for rating-scale questions, the corrected item-total correlation values were between 0.312 and 0.832.
- The reliability of the questionnaire, analysed using Cronbach's Alpha Coefficient, was 0.982.

Step 3: Qualitative Research

Focus group discussions were conducted to validate the research model. The sample consisted of 11 qualified experts from the industrial business sector, selected using the purposive sampling method. These experts provided recommendations and validated the structural equation model, titled "The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand." The structural equation model was cooperatively approved during this phase.

Results

The research findings indicate that the overall importance of the components of the approach to information technology management for personal data security in the industrial business sector in Thailand is high, with an average value of 4.18. When examining each component individually, all were found to have a high level of importance. The Laws and Governance component was deemed the most important,

International Journal of Instructional Cases
ISSN: 2399-830x

with an average value of 4.20. The Audit and Evaluation component followed closely with an average value of 4.19, while the Internal Control component scored an average value of 4.16, and the Organizational Support component had an average value of 4.15. Further analysis of each item within these components revealed the following:

Laws and Governance: The most important item was creating an understanding of the legal standards related to the PDPA 2019 for personnel, which received an average score of 4.49. This was followed by the strict enforcement of the PDPA 2019, with an average score of 4.41, and ensuring that personal data collected, used, or disclosed receives consent from the data owner, either in writing or via an electronic system, with an average value of 4.35.

Audit and Evaluation: Establishing regular audits and monitoring of personal data stored in the organisation according to legal standards received an average score of 4.29. This was followed by promoting good governance processes and adherence to principles of honesty and ethics (average score: 4.27, SD = 0.50), and regularly reporting evaluation results and proposing measures to address issues and obstacles to the working group (average score: 4.27, SD = 0.51).

Internal Control: Establishing guidelines for implementing personal data security control systems scored an average value of 4.22. This was followed by prioritising the achievement and dividing workloads across departments (average score: 4.21, SD = 0.44), and establishing a regular business continuity plan and reviewing the business continuity plan (BCP) (average score: 4.21, SD = 0.49).

Organisational Support: Supporting the assessment of personal data security information systems by leading external technology organisations, such as Microsoft, received an average score of 4.23. This was followed by creating a manual with step-by-step instructions for personal data security operations for personnel (average score: 4.22), and regularly testing the knowledge and understanding of personal data security for all personnel (average score: 4.21).

The research findings on the importance of the components of information technology management guidelines for personal data security in the industrial business sector in Thailand, categorised by the type of industrial business organisation, revealed that the service business sector places the highest importance on the Audit and Evaluation component, with an average value of 4.25. This was followed by the Laws and Governance component (average value of 4.23) and the Internal Control component (average value of 4.22). In contrast, the manufacturing business sector places the highest importance on the Laws and Governance component, with an average value of 4.17, followed by the Audit and Evaluation component (average value of 4.14) and the Organisational Support component (average value of 4.10). To compare the importance level of the components of personal data security management guidelines across the industrial business sector, categorised by the type of business organisation,

International Journal of Instructional Cases
ISSN: 2399-830x

a "t-test" was conducted to compare the means of the two independent population groups. The results were statistically significant at the 0.05 level, both overall and within each component, as presented in Table 1.

Table 1: Mean and Standard Deviation of Personal Data Security Management Importance, Categorized by Business Organization Type

Components of The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand.	Manufacturing Business Sector		Service Business Sector		T-Value	P-Value
	$\bar{X}$	S.D.	$\bar{X}$	S.D.		
Overall	4.13	0.20	4.22	0.34	-3.90	0.00*
1. Laws and Governance	4.17	0.24	4.23	0.35	-2.19	0.03*
2. Audit and Evaluation	4.14	0.23	4.25	0.38	-3.79	0.00*
3. Internal Control	4.10	0.22	4.22	0.38	-4.26	0.00*
4. Organization Support	4.10	0.21	4.19	0.34	-3.96	0.00*

* Significantly different at the 0.05 level

This study utilised a structural equation model to examine the causal factors leading to Information Technology Management regarding Personal Data Protection in the Industrial Business Sector in Thailand. The objective was to analyse and develop a structural equation model for the Guide to Information Technology Management regarding Personal Data Protection in the Industrial Business Sector in Thailand. The model was refined using the Modification Index method, which involved reviewing the program's output values alongside theoretical principles to systematically remove inappropriate observational variables, one at a time. The new model was then processed, and this iterative process continued until the final structural equation model was developed, as presented in Table 2. The structural equation model is depicted in Figure 3, with the variable definitions provided in Table 3.

Table 2: Statistical Values Assessing the Consistency of the Structural Equation Model Before and After Improvement.

Statistics	Consideration Criteria	Before Improvement	After Improvement
1. CMIN- ρ (Chi-Square Probability Level)	ρ > 0.05	0.000	0.188
2. CMIN/df (Relative Chi-Square)	< 2.00	2.826	1. 096
3. GIF (Goodness of Fit Index)	> 0.90	0.630	0.965
4. RMSEA (Root Mean Square Error of Approximation)	< 0.08	0.060	0.014

International Journal of Instructional Cases
ISSN: 2399-830x

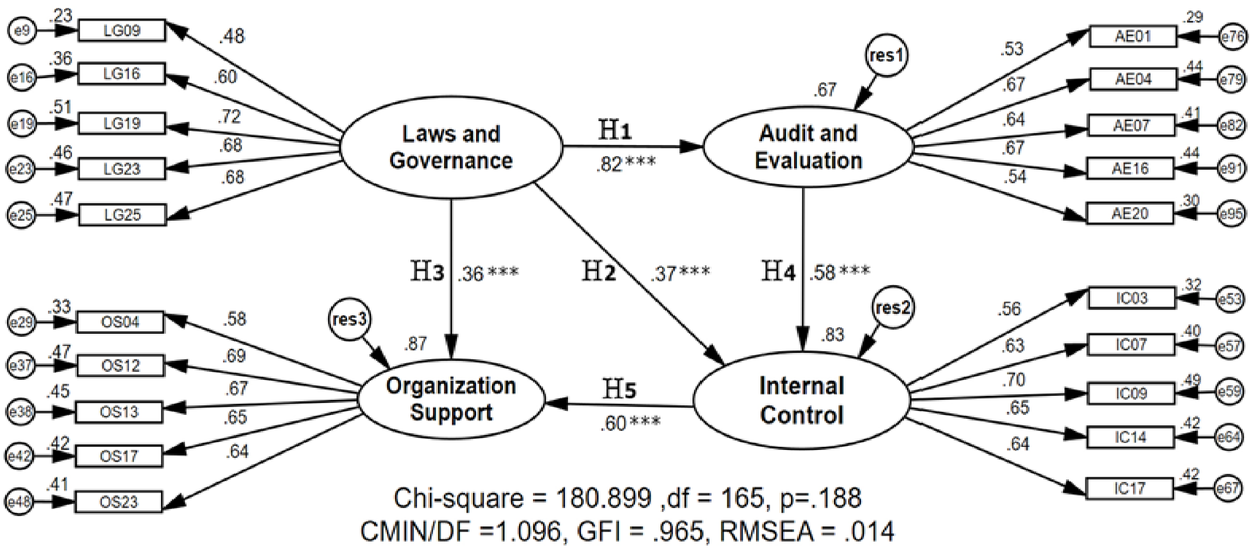

Figure 3: Equation Model of the Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand, Standardized Estimate Mode After the Model Improvement.

Table 3: Definitions of Variables in Analysing Factors Influencing the Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand

Variable	Meaning	Variable	Meaning
LG09	Establish a method for compensating data subjects who have been harmed by a breach if a court determines that the data controller must compensate the data subject.	AE01	Promote Good Governance processes that are strict to the principles of honesty and ethics.
LG16	Define the duties of those involved in the organization's data, such as data protection officers, data controllers, and personal data users.	AE04	Use Checks and Balances to create equilibrium in the audit results from both internal and external auditors.
LG19	Define the scope or types of personal data protection, such as personnel data, customer data, and data on suppliers of goods and services, among others.	AE07	Establish severity and chance standards for the organization to use in assessing the occurrence of a data breach.
LG23	The PDPA 2019 requires the deletion or destruction of personal data after the expiration of the data retention period as stipulated by law.	AE16	Assess the knowledge and skills of individuals within the organization (Internal Auditor) in the area of personal data security.

International Journal of Instructional Cases
ISSN: 2399-830x

Variable	Meaning	Variable	Meaning
LG25	Communicate the Data Protection Policy and Privacy Policy to relevant individuals.	AE20	Regularly report evaluation results and propose measures to address problems and obstacles to the working group.
OS04	Establish a systematic linkage for personal data storage throughout the organization.	IC03	Establish guidelines for implementing the personal data security control system.
OS12	Establish a communication format that allows executives to convey information to operational personnel directly, quickly, and clearly.	IC07	Create a PDPA Check List for the organization.
OS13	Set salary increases according to the position and duties related to enhanced personal data security work.	IC09	Ensure that the organization's website has a channel to inform users and obtain their consent for the use of Cookies in cases where personal information is collected from users.
OS17	Support the Data Loss Prevention technology system with Soft File documents to prevent data leakage.	IC14	Prepare the Data Record of Processing (RoP) thoroughly according to the Sub Business Process.
OS23	Support the development of the skills and knowledge of Data Protection Officers (DPOs) to meet international certification standards.	IC17	Establish a Data Subject Rights and Data Subject Rights Request system, which serves as a channel for receiving requests from personal data owners to exercise their rights.

Discussion and Conclusion

The research findings indicate that the component with the highest average value was the Laws and Governance component, with an average score of 4.20. This aligns with previous studies highlighting the importance of laws as rules and regulations established by the government for collective enforcement, which play a significant role in business operations. Businesses must comprehend, understand, and comply with these laws in an accurate and appropriate manner (Bradford et al., 2020). Incorporating principles of morality, ethics, and honesty is essential, as businesses must respect rights, avoid violations, and refrain from imitating others in business practices to gain social acceptance (Alkhafaji, 2011).

International Journal of Instructional Cases
ISSN: 2399-830x

This approach helps to mitigate the risk of legal infractions and builds customer trust (Machado et al., 2023). Non-compliance with the law can lead to penalties as prescribed by law (Kuner et al., 2021). Businesses must adapt to regulatory changes, such as the PDPA 2019, by developing staff competencies to support the expanded responsibilities regarding personal data, implementing system controls, ensuring operational independence, and assisting personnel in carrying out their duties as mandated by law (Yuniarti, 2022). The type of business organization affects its specific needs and practices for managing cybersecurity. Industry operators must adhere to appropriate standards and frameworks to protect their data and systems effectively (Taherdoost, 2022).

The research results indicate that the most important item in the information technology management strategy for personal data security in the industrial business sector in Thailand was creating an understanding of the legal standards related to the PDPA 2019 for personnel, with an average score of 4.49. This is crucial because, in any work environment, all members must have a clear understanding of the objectives and goals of their tasks. It is important for everyone to comprehend their roles, collaborate as a team, and communicate effectively to share knowledge. This openness fosters the expression of opinions and facilitates learning from the experiences of others. Providing decision-making and management authority leads to greater efficiency and effectiveness in achieving common goals (Bradford et al., 2020). This approach minimizes the risk of errors and strengthens customer confidence (Machado et al., 2023). Focusing on improving communication and problem-solving methods enhances decision-making, streamlining the work process and increasing efficiency (Černevičiūtė et al., 2019; Marques, 2008).

The results from the hypothesis testing of the established influence lines for five out of six items are as follows: 1) The Laws and Governance component directly influences the Audit and Evaluation component, showing statistical significance at the .001 level. 2) The Laws and Governance component directly influences the Internal Control component, with statistical significance at the .001 level. 3) The Laws and Governance component directly influences the Organizational Support component, with statistical significance at the .001 level. 4) The Audit and Evaluation component directly influences the Internal Control component, with statistical significance at the .001 level. 5) The Internal Control component directly influences the Organizational Support component, with statistical significance at the .001 level. The overall analysis of both the direct and indirect influences of the structural equation model for managing personal data security in the business sector, conducted in the standardized estimate mode after model improvement, shows the highest overall influence on the Laws and Governance component.

This significant impact on the Organizational Support component, with a Standardized Regression Weight of 0.86 (0.36 + 0.22 + 0.28), is derived from: 1) The

International Journal of Instructional Cases
ISSN: 2399-830x

direct influence of the Laws and Governance component on the Organizational Support component, which has a Standardized Regression Weight of 0.36. 2) The indirect influence of the Laws and Governance component on the Internal Control component, with a Standardized Regression Weight of 0.37, which subsequently affects the Organizational Support component with a Standardized Regression Weight of 0.60, resulting in a combined weight of 0.22 (0.37 x 0.60 = 0.22). 3) The indirect influence of the Laws and Governance component on the Audit and Evaluation component, characterized by a Standardized Regression Weight of 0.82, which extends to the Internal Control component (Standardized Regression Weight of 0.58) and subsequently affects the Organizational Support component (Standardized Regression Weight of 0.60), promoting a combined weight of 0.28 (0.82 x 0.58 x 0.60 = 0.28). This indicates that the ability to conduct business sustainably and gain acceptance stems from operating in compliance with the law, maintaining transparency and openness, and supporting strong corporate governance.

These practices must be developed with effective internal business controls to ensure organizational efficiency (Alkhafaji, 2011). The law is key in business support, resulting in a positive and significant relationship between organizational support and personnel performance. Organizational support is important for employee behaviour, as it makes employees feel valued and recognized by the organization (Tamimi & Tamam, 2023). For example, compliance with labour laws significantly influences employees and their perceptions, feelings, and behaviours, increasing organizational justice, positively impacting organizational citizenship behaviour (OCB), organizational commitment, and reducing resignation intentions (Red & Teng-Calleja, 2021). These results are consistent with research by Ahmed et al. (2015), which states that Perceived Organizational Support (POS) significantly and positively affects employee engagement, job satisfaction, and organizational commitment. In addition, POS has a moderate impact on resignation behaviour and intentions.

Recommendations

The study recommends that, at the policy level, the Master Plan for Personal Data Promotion and Protection (2024-2027) should be prioritised. This includes raising awareness of the PDPA 2019, encouraging data-sharing between the public and private sectors, and tracking personal data breaches to guide national security efforts. The Ministry of Industry and the Ministry of Digital Economy and Society should offer tax incentives to SMEs and promote ISO/IEC 27001:2013 standards to enhance customer trust. Policies should also focus on developing skilled Personal Data Protection Officers (DPOs). At the operational level, businesses are advised to ensure PDPA compliance through clear legal processes, regular audits, and robust governance practices. Additionally, internal controls should be developed, organisational support strengthened, and breach analyses conducted to improve data protection skills. DPOs should be supported by responsible personnel, IT systems, and

International Journal of Instructional Cases
ISSN: 2399-830x

individual development plans to ensure compliance with the PDPA 2019.

References

Ahmed, I., Nawaz, M. M., Ali, G., & Islam, T. (2015). Perceived organizational support and its outcomes: A meta-analysis of latest available literature. *Management Research Review*, *38*(6), 627-639. https://doi.org/10.1108/MRR-09-2013-0220

Alkhafaji, A. F. (2011). Strategic Management: Formulation, Implementation, and Control in a Dynamic Environment. *Development and Learning in Organizations: An International Journal*, *25*(2). https://doi.org/10.1108/dlo.2011.08125bae.001

Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, *7*(1), lsaa034. https://doi.org/10.1093/jlb/lsaa034

Byrnes, P. E., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren Jr, J. D., & Vasarhelyi, M. (2018). Evolution of auditing: From the traditional approach to the future audit. In *Continuous auditing: Theory and application* (pp. 285-297). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78743-413-420181014

Černevičiūtė, J., Strazdas, R., Kregždaitė, R., & Tvaronavičienė, M. (2019). Cultural and creative industries for sustainable postindustrial regional development: The case of Lithuania. *Journal of International Studies (2071-8330)*, *12*(2). https://doi.org/10.14254/2071-8330.2019/12-2/18

Cogan, M. S. (2023). Thai Politics in Translation: Monarchy, Democracy and the Supra-constitution: Michael K. Connors & Ukrist Pathmanand (eds). NIAS Press. Copenhagen, 2021. pp. 248. £62. ISBN 978 87 7694 285 4. *Asian Affairs*, *54*(2), 390–392. https://doi.org/10.1080/03068374.2023.2217057

Eisenberger, R., Armeli, S., Rexwinkel, B., Lynch, P., & Rhoades, L. (2001). Reciprocation of perceived organizational support. *The Journal of applied psychology*, *86*(1), 42-51. https://doi.org/10.1037/0021-9010.86.1.42

Gordon, G. L., Calantone, R. J., & Di Benedetto, C. A. (1993). Business-to-business Service Marketing: How Does it Differfrom Business-to-Business Product Marketing? *Journal of Business & Industrial Marketing*, *8*(1), 45-57. https://doi.org/10.1108/08858629310027605

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU general data protection regulation: A commentary/update of selected articles. *Update of Selected Articles (May 4, 2021)*. https://doi.org/10.2139/ssrn.3839645

Machado, P., Vilela, J., Peixoto, M., & Silva, C. (2023). A systematic study on the impact of GDPR compliance on Organizations. Proceedings of the XIX Brazilian Symposium on Information Systems(435-442). https://doi.org/10.1145/3592813.3592935

Marques, J. (2008). Workplace diversity: developing a win-win-win strategy. *Development and Learning in Organizations: An International Journal*, *22*(5), 5-8. https://doi.org/10.1108/14777280810896372

International Journal of Instructional Cases
ISSN: 2399-830x

Red, C. L., & Teng-Calleja, M. (2021). Examining the relationship between labor law compliance and employee perceptions, attitudes and behaviors. *Employee Responsibilities and Rights Journal*, *33*(4), 337-357. https://doi.org/10.1007/s10672-021-09369-z

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), 2181. https://doi.org/10.3390/electronics11142181

Tamimi, M., & Tamam, M. B. (2023). The effect of organizational support on employee performance: A systematic literature review. https://doi.org/10.53402/ajebm.v2i2.337

Yuniarti, S. (2022). Protection of Indonesia's Personal Data After Ratification of Personal Data Protection Act. *Progressive Law Review*, *4*(2). https://doi.org/10.36448/plr.v4i02.85