An Integrated Cybersecurity Framework for Personal Data Protection: A Case Study on Thai Personal Data Protection Act B.E. 2562

Puttakul Sakul-Ung* Amornvit Vatcharaphrueksadee** Songtam Vanijkachorn***
Chartphat Klaymanee**** Sanya Vasoppakarn***** Korakod Pumkrachan******
Prachyapol Vaidyakula******* Nawhath Aeksirinithipon******** and Maleerat Maliyaem*

Received : November 19, 2020
Revised : December 16, 2020
Accepted : December 22, 2020

Abstract

Cybersecurity is a worldwide topic, yet, personal data draw attention to cyber-attacks. This combination of two challenges is addressed for an integrated solution. This paper introduces the integrated cybersecurity framework which intentionally considers personal data protection from cyber threats. A case study is performed in the context of Thai Personal Data Protection Act B.E. 2562 (PDPA). The proposed framework is evaluated and assessed objective adherences. The results identify significant acceptance from cybersecurity experts that the proposed framework incorporates personal data protection according to PDPA.

Keywords: Cybersecurity, Personal Data Protection, PDPA, Privacy, Security Framework.

1. Introduction

In February 2013, the National Institute of Standards and Technology (NIST) had an Executive Order (13636) for initiating the voluntary framework to reduce cybersecurity risks. This framework aims to identify, assess and manage cybersecurity-related risks, individual privacy protection, and civil liberties, it is called the NIST cybersecurity framework (CSF) [1, 2]. Afterwards, the NIST CSF is studied and evolved to address higher capability and applicability to serve multiple dimensions in the security paradigms. This paper introduces a conceptual design of the cybersecurity framework where privacy and personal data protection are highlighted. Herewith, the proposed framework contains multiple categories, the first category and its functions are presented in this work; it is Identify.

In 2019, Thai Personal Data Protection Act B.E. 2562 (PDPA) was released. It serves as the general laws for the protection of personal data along with organizations' obligations and responsibilities over privacy and rights of the data subject. Many organizations have adopted a variety of general guidelines and practices to ensure compliance with PDPA; NIST CSF is one of the approaches.

This paper, then, studies and introduces how the compliance alignment between NIST CSF and PDPA can be considered, established and implemented using a case study of Thai IT and PDPA consulting company.

* *Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok.*
** *Faculty of Information Technology and Digital Innovation, North Bangkok University Bangkok, Thailand.*
*** *Thailand Institute of Scientific and Technological Research, Pathum thani, Thailand.*
**** *Information Technology and Blood Donor Registration Department.National Blood Center, Thai Red Cross Society.*
***** *National Health Security Office, Thailand.*
****** *Worldvision foundation of Thailand, Bangkok, Thailand.*
******* *V89 technology Co. Ltd., Bangkok, Thailand.*
******** *N.C.C.Management & Development Co. Ltd., Bangkok, Thailand.*

Table 1. *Review Criteria for Related-Work.*

Criteria	Value
Keywords	Cybersecurity Framework / Privacy Framework / Personal Data Protection
Publication Year	2014 – 2020
Title	Cybersecurity Framework / Privacy Framework / Personal Data Protection
Database	Any
No. of Citation	Any
Include Patents	Yes
Include Citations	Yes

2. Related Works

A systematic review is performed by using criteria, keywords, publication year, and title; these criteria are limited by the scope of work. The related works are grouped into categories, cybersecurity frameworks, and personal data protection act.

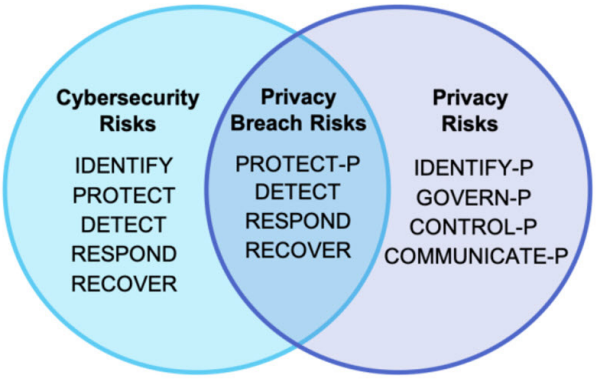
2.1 Cybersecurity Frameworks

The review explores NIST CSF and its related-works. This review aims to capture the evolution and the studied use-case of NIST CSF.

Firstly, NIST CSF contains five categories including Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). Identity refers to a group of functions which aim to establish the understanding of context, risks and opportunity. Protect implicates protective security controls that prevent cyber-threats. Detect is a group of functions that help in cyber-threats detection. Respond enables process-oriented management to handle cybersecurity incidents. Last, Recover refers to a set of functions for resilience and continuity management.

The gap and drawback of NIST CSF have been reported as lack of MEA03 (Monitor, Evaluate and Assess Compliance with External Requirements). It is not a part of NIST CSF. Since this work aims to correlate between NIST CSF and PDPA compliance, the MEA03 then is a crucial factor. However, throughout the review on NIST 800 series, the work in [3] innovates compliance assessment process as a part of NIST CSF; the process contains the following as subcategories, Legal and Regulatory Compliance, Information Privacy, Intellectual Property, and Compliance with Security Policies and Standards. These subcategories are grouped into category, it is called as Compliance Assessment.

Figure 1. *NIST CSF Core Categories.*



(1) *The cybersecurity and privacy overlapping area.*

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PP-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Management Policies, Processes, and Procedures
		CT.DM-P	Data Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PP-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.DP-P	Data Protection Policies, Processes, and Procedures
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

(2) *The categories presented in NIST PF.*

Figure 2. *The perspective and detail of NIST PF.*

In this work, the existing privacy frameworks are reviewed. There are several works which extend the NIST CSF framework.

The work in [4], [5] addresses the privacy crisis that brings out term under the NIST framework, which is called the NIST privacy framework (NIST PF). This framework provides five core functions, which are Identify (ID-P), Govern (GV-P), Control (CT-P), Communicate (CM-P), and Protect (PR-P).

This framework projects the cybersecurity and privacy perspectives in the overlapped areas as shown in Figure 2(1). Where the privacy perspective concerns privacy protection, the privacy breach is then managed through the NIST CSF. This implies the ultimate solution for privacy protection requires the combination of both frameworks. Hence, this work introduces an integrated work by combining these two frameworks.

2.2 Personal Data Protection Act

The Personal Data Protection Act (PDPA) is one of the areas in both IT and Law fields. This review is based on the technical and information technology related to PDPA. Many works examine how organizations react and frame their obligations to country's PDPA, for example, works in [6], [7] explores the PDPA compliance in the context of Malaysia, work in [8] for the Indian context, and work in [9], [10] for Thai financial institutes and cloud in government organizations.

In the context of Thailand, several works have been carried out to provide guidelines and proposals for amending of Thai laws to protect personal data [11], [12]. Surprisingly, Thailand's Personal Data Protection Act of 2019 is also claimed as one of the strongest data privacy laws in Asia [13].

Eventually, this work studies the details of PDPA where the applicable chapters are linked to the proposed cybersecurity framework. The Thai PDPA chapters are presented in Table 2.

Table 2. *Chapters in Thai PDPA.*

Chapter	Description
I	Personal Data Protection Committee
II	Personal Data Protection • Part 1 General Provision • Part 2 Personal Data Collection • Part 3 Use or Disclosure of Personal Data
III	Rights of the Data Subject
IV	Office of the Personal Data Protection Committee
V	Complaints
VI	Civil Liability
VII	Penalties • Part 1: Criminal Liability • Part 2: Administrative Liability

This review also inspects into Sections presented in the Thai PDPA to find the correlation between personal data protection and cybersecurity. It is found that under Section 37(1) and 40(2) identifies the security measure used in the protection of personal data as the following statements:

"Section 37 The Data Controller shall have the following duties:

(1) provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of Personal Data, and such measures must be reviewed when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate security and safety. It shall also be in accordance with the minimum standard specified and announced by the Committee;" and

"Section 40 The Personal Data Processor shall have the following duties:

(2) provide appropriate security measures for preventing unauthorized or unlawful loss, access to, use, alteration, correction or disclosure, of Personal Data, and notify the Data Controller of the Personal Data breach that occurred;"

These obligations require The Personal Data Controller as well as The Personal Data Processor to ensure the security controls and measures are in place in order to protect the personal data. These obligations are not represented in Figure 2(2) because the security measures are part of NIST CSF not in NIST PF.

3. Research Methodology

In this section, the research methodology used in this work is described as the following: Review of the related-works, Limit the scope of work, Introduce the proposed framework, Validate the proposed framework, and Conclusion.

3.1 Review of The Related-works

This work deploys the systematic review based on search criteria; the summarized related works are presented in section 2 (Related Works).

3.2 Limit The Scope of Work

The scope of work is divided into two-dimension, cybersecurity framework scope, and personal data protection act scope. These two scopes are limited to suit the presentation of works on different channels. This determination is done by the consensus of researchers and interviewers who are involved in this project.

3.2.1 Cybersecurity Framework Scope, the core categories of NIST CSF are studied and reviewed against the regulatory requirements of Thai PDPA. However, this paper presents the full conceptual design of the proposed cybersecurity framework along with a specific case study on the Identify category. The details of the case study in other categories will be presented in future works.

3.2.2 Personal Data Protection Act, this work examines personal data protection based on Thai Personal Data Protection Act B.E. 2562. Yet, the scope of chapters and sections of the Act is limited to only related obligations under Data Controller, Data Processor and Data Subject; that means the chapters on Personal Data Protection Committee, Office of the Personal Data Protection Committee, Complaints, Civil Liability, and Penalties are excluded.

3.3 Introduce The Proposed Framework

This work forms the proposed framework based on the related works; it is done by documentary analysis and exploratory analysis. The formation of the proposed framework is reviewed by researchers to finalize the conceptual design of the framework. The detail of the proposed framework is presented in the next section of this paper.

3.4 Validate The Proposed Framework

To ensure the proposed framework validity, two validating methods are deployed as the following

3.4.1 Quantitative validation is determined by using Index of Item Objective Congruence (IOC), this value is an acceptable threshold in the proposed framework components which are designed to serve the Thai PDPA as regulatory requirements in the scope of consideration.

3.4.2 Qualitative validation is determined by using the interview method; the result of quantitative validation is again qualitatively validated. This validation is achieved by the reviewing and commending from the IT and security consultants who are currently working in Innovative Information Technology Consulting Co. Ltd. (IITC), the consulting company registered in Thailand.

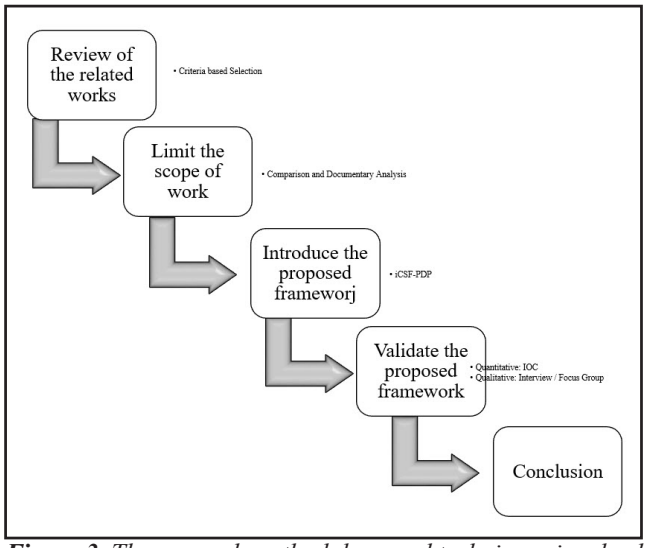


Figure 3. *The research methodology and techniques involved in this work.*

3.5 Conclusion

In sum, the conclusion over presenting the scope of work is summarized and presented in this paper.

The overall research methodology and techniques deployed in this work is represented in Figure 3.

4. An Integrated Cybersecurity Framework for Personal Data Protection

An Integrated Cybersecurity Framework for Personal Data Protection (iCSF-PDP) is conceptually designed to mitigate cybersecurity risks related to personal data and to draw guidelines for organizations that are practicing PDPA compliance.

The integration of NIST CSF and NIST PF is done by the comparison among core categories and subcategories. It is found that the protection of personal data requires both security and privacy perspectives. Besides, compliance assessment is also a critical factor to be considered. Based on the relationship, this work enhances and contributes to the comparison as shown in Table 3.

Table 3. *Comparison of Frameworks.*

iCSF-PDP	NIST CSF	NIST PF	Almuhammadi, et al.
ID	ID	ID-P	Asset Management
			Business Environment
			Risk Assessment
			Data Processing Ecosystem Risk Management
			Data Mapping
	ID	GV-P	Governance
			Risk Management Strategy
			Compliance Assessment
CM	PR	GV-P	Awareness and Training
			Monitoring and Review
		CM-P	Communication Policies, Processes, and Procedures
			Data Processing Awareness
CT		CT-P	Data Management Policies, Processes, and Procedures
			Data Management
			Disassociated Processing
	PR	PR-P	Access Control
			Data Security
			Information Protection Processes and Procedures
			Maintenance
			Protective Technology
	DE		Anomalies and Events
			Security Continuous Monitoring
			Detection Processes
RS	RS		Response Planning
			Response Communications
			Response Analysis
			Response Mitigation
			Response Improvement
RC	RC		Recovery Planning
			Recovery Improvement
			Recovery Communication
Missing categories/subcategories are highlighted by grey color			

Table 3 shows that NIST CSF does not contain data concerning such as data management policies, data processing, where NIST PF reuses cybersecurity components from NIST CSF (DE, RS, and RC) as optional implementation. The perspective of NIST seems to be a clear separation between privacy and cybersecurity with a few overlapping areas.

The work in [3] captures an area in NIST CSF and contributes compliance assessment as one of the subcategories in the Identify category, this work is loosely related to NIST PF since it does not intentionally cover privacy.

4.1 High Level Structure of iCSF-PDP

Unlike NIST's perspective, iCSF-PDP integrated cybersecurity and privacy into a single structure. But this integration is proposed to ensure legal compliance to PDPA.

The high-level conceptual design of iCSF-PDP is integration between cybersecurity frameworks and privacy framework based on NIST original works and related works. iCSF-PDP contains five core categories described in Figure 4.

Figure 4. *iCSF-PDP Core Categories.*

4.1.1 Identify, this category aims to create context awareness and understanding of cybersecurity and personal data protection aspects to the organization and its stakeholders. In this category, it proposes 5 functions as the following:

1) Understanding the Context of the Organization, the organization shall determine interested parties and their expectations, internal and external issues related to PDPA compliance.

2) Risk Strategy and Assessment, risk strategy shall be defined under the organization's context. Risk Assessment shall be performed to identify risks related to PDPA compliance; this is including but not limited to cybersecurity risks, information security risks, and privacy impact analysis.

3) Asset Management and Data Mapping, information and data is one type of asset; the difference is that data assets cannot exist without media or other assets which are holding it. Data Mapping refers to a Data Inventory which identifies

essential information regarding particular data such as classification, owner, related business processes and technologies, storage, and lawful basis.

4) Governance, this refers to high-level governance and leadership demonstration in the organization such as policy statements, role and responsibility assignments, management communications, and so on.

5) Compliance Assessment, the organization shall assess the applicable regulatory and law requirements which are related to the context, this is including but not limited to general laws, specific laws, ordinance, Ministry Announcement, and so on.

4.1.2 Control, this category refers to a group of controls used to mitigate and manage risks which are associated with the context of the organization and identified risks. The core concept of this category is "controls selection and implementation"; these controls are divided into groups as the following:

1) Detective Controls, a group of technologies used for anomalies and events detection, security monitoring, etc.

2) Preventive Controls, a group of technologies used for Access Control, Preventive Maintenance, Protective Technology, Data Security, etc.

3) Corrective Controls, a group of technologies used for correction of abnormalities and malfunctioning, for example, Corrective Maintenance.

4) Policies, Processes and Procedures, a group of documented information that governs the business processes along with related technological controls. It also refers to organizational controls.

5) Disciplinary Controls, a group of defined disciplinary actions for an intentional or unintentional violation of organizational controls.

4.1.3 Communicate, this category subjects to internal and external communications; this includes the following practices.

1) Information Security and Cybersecurity Awareness is the method or combination of methods to ensure stakeholders are obtaining the knowledge and awareness to prevent information security breaches and cyber-attacks.

2) Data Processing Awareness is the method or combination of methods to ensure stakeholders are having knowledge and awareness to process personal data based on a lawful basis.

3) Competence Training aims to build knowledge and competence in related subject matters such as best practices, international standards, and laws.

4) Communication of policies, processes, and procedures refers to the internal and external communication of defined and enforced policies, processes and procedures within the context of the organization. Also, this refers to the communication of identified risks to relevant stakeholders.

5) Public Communication, communication to external parties such as regulators, business partners, customers, and mass media.

4.1.4 Respond, it refers to the ability of the organization to manage and respond to the incidents and breaches. This category contains the following steps.

1) Response Planning, the defined plans to handle weaknesses, events, and incidents that affect the business operations, and controls or introduce risks to personal data protection.

2) Response Analysis, the defined criteria to assess, evaluate, and prioritize the triggering events.

3) Response Resolution, the taken methods to close the incidents as soon as practicable. This resolution also refers to mitigation, acceptance, avoidance, and transferring of the consequences of incidents.

4) Response Communication and Escalation, the essential communication which takes place in every step to stakeholders of particular weaknesses, events, and incidents.

5) Response Improvement; it refers to the post-incident assessment to collect the knowledge and lesson learned. The improvement is possibly concerning technology, people, and process.

4.1.5 Recover, the final category which refers to

resiliency and recovery of business operations and controls during disaster or crisis. Moreover, this category can be integrated into business continuity management practices in such a way that privacy and personal data is fully and continuously protected regardless of the continuity of the organization. It contains the following functions.

1) Recovery Planning, it refers to the privacy continuity plan; this implies that the continuity of personal data protection shall be planned against possible risks of disruption and crisis. For example, the safeguards of personal data related databases won't be disabled and affected by network intrusion or failures.

2) Recovery Exercise, it refers to the testing of recovery plans to ensure that the plans are up-to-date and practicable during disruption or crisis.

3) Recover Analysis, this function provides assessment and analysis of associated criteria to business operation perspectives such as the recovery of personal data within the service level agreement (SLA) or operational level agreement (OLA). The maximum tolerable disruption threshold that will not affect the personal data protection mechanism or related applicable regulatory requirements.

4) Recovery Communication, it ensures the communications to stakeholders during disruption or crisis are appropriately managed, communicated, and monitored. This also includes the communication to regulators according to laws.

5) Recovery Improvement, similarly to response improvement, but the recovery improvement focuses on the improvement of planning, exercise, and communication to facilitate the faster and better recovery of business operations and controls in order to reduce and prevent consequences to personal data.

The above functions 25 areas presented in iCSF-PDP framework; the detail of each function will be presented in future works. The mapping between iCSF-PDP high-level structure and PDPA is shown in Table 4.

Table 4. *Mapping between iCSF-PDP and PDPA.*

ICSF-PDP	PDPA	Related Description
Identify (ID)	Chapter 2 and 3	• Understand organization context, stakeholders and expectations • Assess the compliance • Assess privacy risks and impact analysis • Identify personal data, data inventory and mapping • Establish Data Privacy Policy • Assign Data Protection Officer (DPO)
Control (CT)	Chapter 2 and 3	• Define the policies on personal data collection • Define the policies on use or disclosure of personal data • Define the policies for data subject rights • Establish the appropriate security measures • Maintain the record of processing
Communicate (CM)	Chapter 3	• Communicate the data subjects' rights and privacy notices
Respond (RS)	Chapter 3	• Notify for personal data breach
Recover (RC)	-	• Handle the recovery process to achieve the regulatory requirements and prevent compliance breach

4.2 A Case Study of iCSF-PDP: Identify Element for PDPA

In this section, a case study of iCSF-PDP in "Identify" against PDPA is examined and presented in accordance with Table 4.

4.2.1 Understand organization context, stakeholders and expectations: organization shall understand what, why, how, when, and who in accordance with personal data protection.

1) What are the business processes and services that concern personal data protection? This the question that enables overseeing the sources and scopes of personal data within the organization. The results of this function could be a business architecture that has linkages to personal data; this is called a defined scope.

2) Why does the personal data exist in the defined scope? The lawful basis is an important factor for the data processing activities; addressing this question is to identify the applicable basis that determines how personal data is collected and managed.

3) How does the organization handle personal data? This question addresses the following architecture in enterprise architecture, information system and application architecture, infrastructure architecture, and security architecture. These architectures identify the related technologies

and security measures used to handle personal data. Moreover, the rights of Data Subjects should be addressed in relation to the particular personal data.

4) When are personal data collected and distributed? And How long will personal data be stored? These questions identify the starting and ending point of holding personal data within the context. This also involves the determination of lawful basis and applicable laws which define the reason for data collection and period of storing.

5) Who is responsible for personal data protection? DPO is the first answer, but other people may involve as stakeholders to particular personal data such as Data Subjects, business owners, and Data Processors.

Understanding of the organization context mainly contributes to the compliance of Section 39 of PDPA.

4.2.2 Assess the compliance, the compliance assessment mainly focuses on putting applicable laws and regulatory requirements on the table. These requirements shall be assessed as a compliance checklist to stakeholders. If any nonconformity is found during the assessment process, then the organization shall take the serious actions for closure, otherwise, report to regulators for further actions. The compliance assessment evaluates the requirements under the Section 19, 20, and 21 of PDPA.

4.2.3 Assess privacy risks and impact analysis, this function aims to generally assess the criticality and sensitivity of personal data. Especially the personal data under Section 26 of PDPA. The personal data impact analysis guides the actions to be taken under Section 37 (4).

4.2.4 Identify personal data, data inventory, and data mapping. This function aims to create the source of information regarding personal data within the defined scope. Recalling 4.2.1, the data mapping is the results of contribution from understanding the context of the organization, and it is a part of data inventory. Identified personal data along with the mapping will sorely contribute as documented information for the compliance under Section 39 of PDPA.

4.2.5 Establish data privacy policy, this is the high-level statements which govern the entire defined scope. The data privacy policy contains the high-level statement for the compliance of PDPA, where possible, the several processes and procedures should be defined and documented to serve as organizational controls. This set of policies, processes, and procedures contribute to the compliance of Chapter 2, and Chapter 3 of PDPA. The example of processes is including but not limited to the following:

1) Data Security and Classification Policy

2) Procedure for Managing Data Subjects' Rights

3) Procedure for Personal Data Processing and Disclosure

4) Procedure for Secured Transfer of Personal Data

5) Procedure for Handling Personal Data Breach

The number of policies, processes and procedures established within the defined scope depends on the documentation cultures of the organization. Importantly, the compliance checklist shall determine the coverage of PDPA and ensure that no significant Section of PDPA is left without attention.

4.2.6 Assign the DPO, who is in charge of personal data protection under the defined scope. This function strongly links to Section 41 of PDPA.

The completed body of knowledge of iCSF-PDP is still undergoing. This paper aims to provide the fundamental conceptual design of the framework and the example of the case study. The evaluation of the proposed framework is validated in the next section.

5. Validation of The Proposed Framework

The validation takes place by using both quantitative validation and qualitative validation.

5.1 Quantitative Validation

Index of Item Objective Congruence (IOC) is used to validate the content of the iCSF-PDP. This validation is done by five professionals who are working in the cybersecurity and personal data protection field, these evaluators have more than 5 years of experience in cybersecurity.

The IOC Index is used as the basis for screening the quality

and adherence of the proposed categories and functions under iCSF-PDP. In each function, the experts are asked to determine the content validity score:

The score = 1, if the experts certainly agree that the function meets its objectives.

The score = -1, if the experts disagree that the function meets its objectives.

The score = 0, if the experts are not sure that the function meets its objectives.

The qualified functions should have the IOC equal to or greater than 0.5.

Table 5. *IOC results.*

Category	ID	Function	IOC
ID	ID-UN	Understanding the Context of the Organization	1
	ID-RS	Risk Strategy and Assessment	1
	ID-AS	Asset Management and Data Mapping	1
	ID-GV	Governance	1
	ID-CA	Compliance Assessment	1
CT	CT-DC	Detective Controls	1
	CT-PC	Preventive Controls	1
	CT-CC	Corrective Controls	1
	CT-PO	Policies, Processes and Procedures	1
	CT-DP	Disciplinary Controls	0.6
CM	CM-IC	Information Security and Cybersecurity Awareness	0.8
	CM-DP	Data Processing Awareness	0.8
	CM-CT	Competence Trainings	0.8
	CM-CP	Communication of policies, processes, and procedures	0.8
	CM-PC	Public Communication	0.8
RS	RS-PL	Response Planning	0.8
	RS-AN	Response Analysis	0.6
	RS-RE	Response Resolution	0.8
	RS-CM	Response Communication and Escalation	0.8
	RS-IM	Response Improvement	0.8
RC	RC-PL	Recovery Planning	0.6
	RC-EX	Recovery Exercise	0.6
	RC-AN	Recovery Analysis	0.4
	RC-CM	Recovery Communication	0.6
	RC-IM	Recovery Improvement	0.6

From the IOC value, the only rejected component is Recovery Analysis (RC-AN). The high degree of acceptance shows in the areas of Identify (ID) and Control (CT). Compliance Assessment (ID-CA) which is contributed by the reviewed work is confirmed as a necessary component by IOC result. The overall specific IOC for each category is shown in Figure 5.

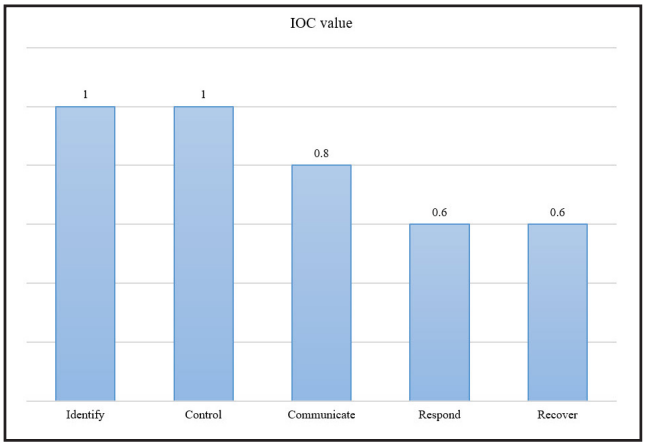


Figure 5. *iCSF-PDP IOC value.*

After the interpretation of the quantitative result, the study is brought to the next validation method, a qualitative validation.

5.2 Qualitative Validation

Senior IT consultant, who is currently working as a security consulting company, Innovative Information Technology Consulting Co. Ltd., is invited for the interview. The agenda of this interview aims to gather information and comment on the interpretation of the quantitative validation result of iCSF-PDP.

"The quantitative validation result is not surprising, because the NIST cybersecurity and privacy frameworks trends to be linked but not the same. This may be a reason why RS and RC are not fully accepted as core components in iCSF-PDP. Still, it is accepted even though IOC is not quite a high degree" - said the interviewee. Since the development of iCSF-PDP contains two NIST's frameworks. The result identifies the Recover (RC) is not directly linked to privacy concerns, on the other hand, it is about the security aspects. "I disagreed with the concept of separation between cybersecurity and privacy because the majority of privacy breaches also violate one of the attributes in information security, confidentiality, integrity or availability, or the combination of attributes" - the interviewee said. This

dialogue may pursue a different perspective against the quantitative result. The interviewee supports the integration of cybersecurity and privacy frameworks because the result of privacy breach trends to be linked to an information security breach as well.

6. Conclusion

iCSF-PDP is accepted through the content validity method, IOC. The qualitative validation supports the integration between cybersecurity and privacy framework to form the personal data protection. Further work will be determined and enhanced based on the validation result, for example, examining RS and RC components to form a stronger linkage between cybersecurity, privacy and personal data protection is one of the interesting areas.

7. References

[1] K. Stine, K. Quill, and G. Witte. "Framework for improving critical infrastructure cybersecurity." *National Institute of Standards and Technology*, DOI:10.1002/https://dx.doi.org/10.6028/nist.cswp.02122014, 2014.

[2] S. J. Shackelford, A. A. Proia, B. Martell, and A. N. J. T. I. l. L. Craig. "Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices." Vol. 50, pp. 305, 2015.

[3] S. Almuhammadi, M. J. C. S. Alsaleh, and I. Technology. "Information security maturity model for NIST cyber security framework." DOI: 10.5121/csit.2017.70305, Vol. 7, No. 3, pp. 51-62, 2017.

[4] J. S. Hiller, R. S. J. J. o. C. Russell, and C. Management. "Privacy in crises: The NIST privacy framework." https://doi.org/10.1111/1468-5973.12143, Vol. 25, No. 1, pp. 31-38, 2017.

[5] D. Siderius. "NIST Standard Reference Simulation Website - SRD 173." *National Institute of Standards and Technology*, 2017.

[6] H. N. Chua, A. Herbland, S. F. Wong, Y. J. T. Chang, and Informatics. "Compliance to personal data protection principles: A study of how organizations frame privacy policy notices." *Telematics and Informatics*, Vol. 34, No. 4, pp. 157-170, 2017.

[7] N. A. Basarudin, A. L. Yeon, Z. Mohamed Yusoff, N. H. Md Dahlan, and N. J. M. C. R. J. Mahdzir. "Smart Home Users'information In Cloud System: A Comparison Between Malaysian Personal Data Protection Act 2010 And Eu General Data Protection Regulation." *Malaysian Construction Research Journal*, Vol. 2, No. 2, pp. 209-222, 2017.

[8] L. Determann and C. J. U. B. P. L. R. P. Gupta. *Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law*. 2018.

[9] T. Sairahu. "Factors Influencing Electronic Personal Data Protection Management and Development of Financial Institutes in Thai Banking Association." *In International Academic Multidisciplinary Research Conference in Los Angeles 2019*, pp. 36-40, 2019.

[10] A. Chaipunyathat, N. Porrawatpreyakorn, S. Nuchitprasitchai, and K. Viriyapant. "A Conceptual Model of Requirement Engineering in Cloud Project Delivery for Thai Government Organizations." *In 2019 Research, Invention, and Innovation Congress (RI2C)*, IEEE, Bangkok, Thailand, pp. 1-7, 2019.

[11] K. J. S. S. A. Thongraweewong. "The legal protection of personal data in the case of "Google street view": A comparative study of US, EU, and Thai laws." *Social Science Asia*, Vol. 3, No. 1, pp. 41-52, 2017.

[12] P. Sakul-Ung and S. Smanchat. "Towards Privacy Framework in Software Development Projects and Applications: An Integrated Framework." *In 2019 Research, Invention, and Innovation Congress (RI2C)*, IEEE, Bangkok, Thailand, pp. 1-6, 2019.

[13] G. Greenleaf and A. J. A. a. S. Suriyawongkul. *Thailand–Asia's strong new data protection law*, 2019.