Data Science and Engineering (DSE) Record, Volume 4, issue 1.

Comparative Study on Privacy Impact Assessment Metrics on Multi-domain Transactional Processing: Case Study of Registration Office, Chiang Mai University

Supaporn Thankham [1] and Pruet Boonma [2]

[1] Master's Degree Program in Data Science, Chiang Mai University, Chiang Mai, Thailand
[2] Department of Computer Engineering, Faculty of Engineering, Chiang Mai University, Chiang Mai, Thailand
supaporn_thankham@cmu.ac.th

Abstract. This independent study is a comparative study on privacy impact assessment metrics on multi-domain transactional processing: case study of Registration Office, Chiang Mai University. a privacy impact assessment should be conducted on which personal data, and what the high-risk data are, in order to guide other entities that have multi-domain linkage for doing a DPIA (Data Protection Impact Assessment) on high-risk data to ensure the security of personal infor-mation Including the storage and management of various personal info-mation appropriately. The researcher used the three tools, which include GS1 tool, iPIA tool, and SPIA tool, and conducted a DPIA using the ISO-IEC-27001-2013 Standard Framework and NIST Cybersecurity Framework to be guidelines for designing the specified DPIA.

Keywords: Privacy risk, Risk score privacy, Impact assessment, Privacy impact assessment

1 Introduction

1.1 Background and Significance of the Problem

The development of modern technology in Thailand is currently growing rapidly, which enable people to access the information of each other more comprehensively and quickly. As the number of channels to access personal data increases, the risk of data security breaches is also increasing. A Data Protection Impact Assessment (DPIA) [1] aims to systematically minimize the data protection risks arising from access to personal data. It also reduces the likelihood of any mistake or any action that is contrary to or inconsistent with the law in processing personal data made by data controllers and data processors. There are a variety of tools available to conduct a DPIA, such as GS1 tool [2], iPIA tool [3], SPIA tool [4], etc. As for Thailand, it specifies that data controllers both government entities and businesses are subject to the Personal Data Protection Act B.E. 2562 (2019) [5]. It is a law that grants rights of data subjects, establishing standards of keeping personal data safe and being used for the purpose according to the consent given by the data subject. The act was published in the Royal Gazette on May 27, 2019 and currently has been postponed to be fully enforced on June 1, 2022.

Chiang Mai University has continuously complied with the Personal Data Protection Act, B.E. 2562 (2019) in order to ensure personal data security, including storing and managing personal data properly. It has a transactional processing system, which uses a computer to process various transaction data to obtain information to support daily operations. This results in better operational efficiency [6] and a multi-domain system, with a shared resource [7], such as connecting through API (Application Programing Interface). It made the researcher realize the significance of gaining access to personal data. This study is a comparative study on privacy impact assessment metrics on multi-domain transactional processing: case study of Registration Office, Chiang Mai University. That is, a privacy impact assessment should be conducted on which personal data, and what the high-risk data are, in order to guide other entities that have multi-domain linkage for doing a DPIA on high-risk data.

1.2 Objectives of the Study

To conduct a comparative study on privacy impact assessment metrics according to the Personal Data Protection Act, B.E. 2562 (2019) on multi-domain transactional processing of Registration Office, Chiang Mai University.

1.3 Scope of the Study

Since the data of Registration Office, Chiang Mai University was considered personal data, there were limitations in terms of requesting permission for data usage. The researcher designed the assessment and had the experts or relevant parties carried out the assessment of high-risk data. Thus, there was no requesting permission for personal data usage from using such database. The researcher used only the data of Registration Office, Chiang Mai University. the tools used, which include GS1 tool, iPIA tool, and SPIA tool. Presenting analysis results with Microsoft Power BI.

1.4 Methodology of the Study

The research designed methodology of the study by following steps: First, asking for permission to use the data from Registration Office, Chiang Mai University according to the Personal Data Protection Act, B.E. 2562 (2019). Next, collecting accessible data. Then, preparing data. Understanding the data for an analysis in order to conduct a DPIA. After that studying the tools used, which include GS1 tool, iPIA tool, and SPIA tool. Conducting a DPIA using the ISO-IEC-27001-2013 Standard Framework and NIST Cybersecurity Framework to be guidelines for designing the specified DPIA. Then, using the assessment tools to analyze the specified DPIA. Comparing the analysis results based on using the three tools. Summarizing the results for which data should be conducted a DPIA and of which is high-risk data. Next, presenting the analysis results to stakeholders using a focus group with executives and relevant personnel of Registration Office, Chiang Mai University. Finally, preparing documents, and submit the complete documents.

1.5 Expected Benefits

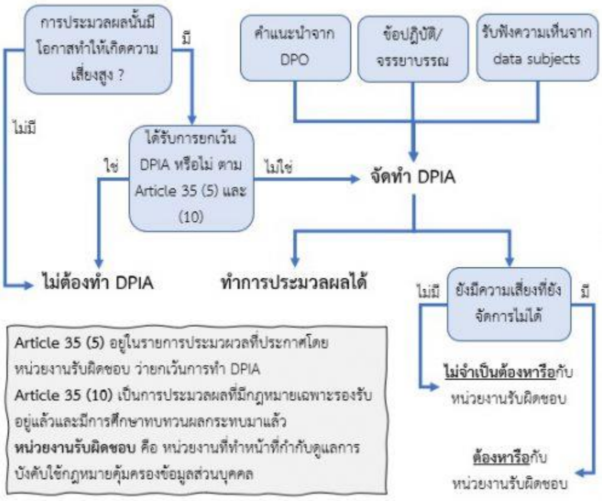
To be as a guideline for a comparative study on privacy impact assessment metrics according to the Personal Data Protection Act, B.E. 2562 (2019) on multi-domain transactional processing in performing a DPIA on high-risk data.

2 Literature Review

2.1 Basic Steps and Principles of Conducting a DPIA (Data Protection Impact Assessment)

The basic steps and principles of conducting a DPIA are governance and early warning mechanisms. The aim is to identify potential negative impacts and mitigate potential risks to personal data. Under the Personal Data Protection Act, B.E. 2562 (2019), a DPIA should be conducted where data processing is likely to result in a high risk to the rights and freedoms of individuals, such as:

- Automated processing for profiling purposes and similar activities that have a legal impact or a similarly significant impact on the data subject.
- Processing on a large scale of special categories of personal data, such as revealing racial origin, political opinions, and similar data, or relating to criminal convictions and offences.
- A systematic monitoring of a publicly accessible area on a large scale.


การประมวลผลนั้นมีโอกาสทำให้เกิดความเสี่ยงสูง ?
มี
ไม่มี
คำแนะนำจาก DPO
ข้อปฏิบัติ/จรรยาบรรณ
รับฟังความเห็นจาก data subjects
ได้รับการยกเว้น DPIA หรือไม่ ตาม Article 35 (5) และ (10)
ใช่
ไม่ใช่
จัดทำ DPIA
ไม่ต้องทำ DPIA
ทำการประมวลผลได้
ไม่มี
ยังมีความเสี่ยงที่ยังจัดการไม่ได้
มี
ไม่จำเป็นต้องหารือกับหน่วยงานรับผิดชอบ
ต้องหารือกับหน่วยงานรับผิดชอบ

Article 35 (5) อยู่ในรายการประมวผลที่ประกาศโดยหน่วยงานรับผิดชอบ ว่ายกเว้นการทำ DPIA

Article 35 (10) เป็นการประมวลผลที่มีกฎหมายเฉพาะรองรับอยู่แล้วและมีการศึกษาทบทวนผลกระทบมาแล้ว

หน่วยงานรับผิดชอบ คือ หน่วยงานที่ทำหน้าที่กำกับดูแลการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

Figure 1 shows the basic steps and principles of conducting a DPIA [8]

2.2 Privacy Impact Assessment Tools

The researcher used three tools for a privacy impact assessment: GS1 tool, iPIA tool, and SPIA tool.

2.2.1 GS1 (GS1 Privacy Impact Assessment Tool (2012)) [2]

The Global Language of Business developed a software application intended to help European companies in a privacy risk assessment. Risk assessment is used for privacy risks. Scope risks are defined, including probability, impacts, and efficiency control according to equation.

Risk = Impact x Likelihood - (C1 + C2 + C3 + C4 + C5)

(If a risk score of GS1 is negative, define the risk score of GS1 to zero.)

Risk likelihood and impact scores will be categorized into a scale of 1-5 (risk does not occur, risk may occur occasionally, risk occurs occasionally, risk occurs, and risk highly occurs respectively). The following table shows impact, probability, and efficiency control which are defined for scoring techniques used in GS1 tool.

Table 1. the likelihood score of the GS1 tool

Score	Likelihood
5	It is very likely that this risk will occur in the organization
4	It is likely that this risk will occur in the organization
3	This risk may occur in the organization
2	It is very unlikely that this risk will occur
1	It is unlikely that this risk will occur

Table 2. the impact score of the GS1 tool

Score	Impact
5	The impact to the data subject will be highly detrimental and cause residual effects to the organization
4	The impact to the data subject will be detrimental and cause residual effects to the organization
3	The impact to the data subject will be minor and cause some residual effects to the organization
2	There could be minor impact to the data subject with some residual effects to the organization
1	There would be no impact to the data subject with no residual effects to the organization

Table 3. the control effectiveness

Score	Control effectiveness
5	Risk mitigation strategy or control process in place – proven highly effective in the previous 12 months
4	Risk mitigation strategy or control process in place – proven effective in the past 6 months
3	Risk mitigation strategy or control process in place – proven largely effective
2	Risk mitigation strategy or control process recently implemented - effectiveness is questionable or unknow
1	Risk mitigation strategy or control process is not in place or is under development

2.2.2 iPIA (The Intelligent Privacy Impact Assessment tool) [3]

The iPIA tool was developed by the Institute for Management Information Systems at the University of Vienna. It is a privacy risk assessment based on two perspectives as shown in the table.

Table 4. scoring techniques used in the iPIA tool

Category	Subcategory	Score
Operator perspective	Impact on reputation and brand value	Low, Med, High
	Financial loss	
Consumer perspective	Social standing	
	Financial well being	
	Personal freedom	
Overall category		

Regarding Table 4, scope risks are defined, which include:

- An operator's perspective, such as reputational risks and financial loss.
- A data subject's perspective, such as social status, financial well-being, freedoms of individuals.

Risk likelihood and impact scores will be categorized into a scale of 1-5 (risk does not occur, risk may occur occasionally, risk occurs occasionally, risk occurs, and risk highly occurs respectively). The following table shows impact, probability, and efficiency control which are defined for scoring techniques used in iPIA tool.

Table 5. the likelihood score of the iPIA tool

Score	Likelihood
5	The impact to the data subject will be highly detrimental and cause residual effects to the organization
4	The impact to the data subject will be detrimental and cause residual effects to the organization
3	The impact to the data subject will be minor and cause some residual effects to the organization
2	There could be minor impact to the data subject with some residual effects to the organization
1	There would be no impact to the data subject with no residual effects to the organization

Table 6. the impact score of the iPIA tool

Score	Impact
5	Risk mitigation strategy or control process in place – proven highly effective in the previous 12 months
4	Risk mitigation strategy or control process in place – proven effective in the past 6 months
3	Risk mitigation strategy or control process in place – proven largely effective
2	Risk mitigation strategy or control process recently implemented - effectiveness is questionable or unknow
1	Risk mitigation strategy or control process is not in place or is under development

2.2.3 SPIA (Signaling Pathway Impact Analysis) [4]

The SPIA tool was developed by Penn Medicine and other departments at the University of Pennsylvania. It is a privacy risk assessment. This tool has two risk scores for threat scenarios: predefined and current states.

Risk = Probability * Consequences

Risk probability and consequences scores will be categorized into a scale of 0-5.

(Risk does not occur, risk may occur occasionally, risk occurs occasionally, risk occurs, and risk highly occurs respectively).

As for defining a data security policy and procedures, and risk management through specified controls, the outstanding benchmarks for policy monitoring and corrective actions and best practices include:

- Computer policies and practices.
- Data security best practices.
- Acceptable use policy on electronic resources.
- Policy on unauthorized copying of copyrighted materials.
- Policy on computer disconnection from PennNet.

Table 7. the probability score of the SPIA tool

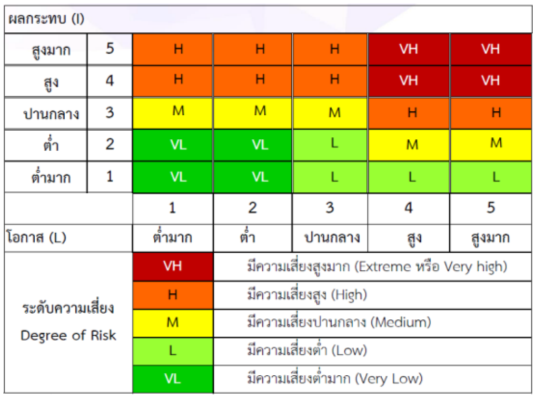
Score	Probability
5	The event is expected to occur in most circumstances Consequence
4	The event will probably occur at some time
3	The event should occur at some time
2	The event could occur at some time, but probably will not
1	The event would only occur under exceptional circumstances
0	Threat does not apply to this application / database

Table 8. the consequences score of the SPIA tool

Score	Consequences
5	Comprehensive impact on ability to plan and conduct business activities with total disruption in customer service, operational efficiency and staff morale. Devastating financial or political impact
4	Major impact on ability to plan and conduct business activities with significant reduction in customer service, operational efficiency and staff morale. Considerable financial or political impact
3	Medium impact on ability to plan and conduct business activities with a moderate reduction in customer service, operational efficiency, and staff morale. Some financial or political impact is experienced.
2	Minor impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Minimal financial or political impact.
1	Negligible impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Very limited, or no financial/political impact
0	Threat is not applicable to this application

2.3 Assessment in Analyzing the Specified DPIA

The researcher chose to use the assessment in analyzing the specified DPIA. This assessment classifies the risk scores into the following 5 levels: very low risk, low risk, medium risk, high risk, and very high risk, respectively.



ผลกระทบ (I)						
สูงมาก	5	H	H	H	VH	VH
สูง	4	H	H	H	VH	VH
ปานกลาง	3	M	M	M	H	H
ต่ำ	2	VL	VL	L	M	M
ต่ำมาก	1	VL	VL	L	L	L
		1	2	3	4	5
โอกาส (L)		ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
ระดับความเสี่ยง Degree of Risk		VH	มีความเสี่ยงสูงมาก (Extreme หรือ Very high)			
		H	มีความเสี่ยงสูง (High)			
		M	มีความเสี่ยงปานกลาง (Medium)			
		L	มีความเสี่ยงต่ำ (Low)			
		VL	มีความเสี่ยงต่ำมาก (Very Low)			

Figure 2 shows degree of risk or risk level [11].

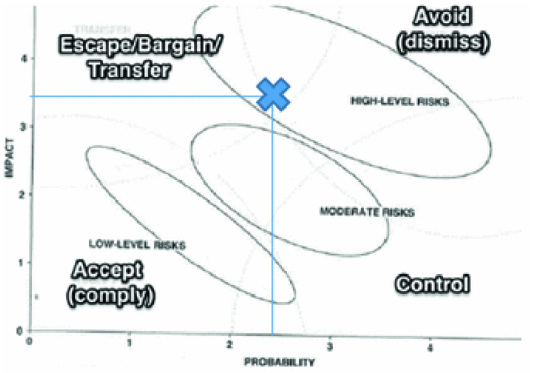


Figure 3 shows data risk classification and a graph showing impact trends.

Three tools were used for a privacy impact assessment: GS1 tool, iPIA tool, and SPIA tool to conduct analysis results on privacy using the average score of the privacy impact assessment, and the results were presented in Power BI. Since the DPIA data used in the study is large data, it is much simpler to visualize it using Power BI, enabling to drill down to the data or filter the data as necessary. For example, the assessment results using the three types of privacy impact assessment tools, which include GS1tool, iPIA tool and SPIA tool, were chosen to compare the scores of each assessment aspect of the specified DPIA data.

This comparative study on privacy impact assessment metrics on multi-domain transactional processing: case study of Registration Office, Chiang Mai University was expected to be as a guideline for other entities that have multi-domain linkage for doing a DPIA on high-risk data as follows:

1) Scope of the study
2) Research methodology
3) Tools used in the study
4) Research facilities/sites

3 Data and Methodology

3.1 Tools Used in the Study

- Calculations performed by Microsoft Excel will be used in risk assessment.
- Data collection in Microsoft Excel or CSV.

3.2 Research Sites

- Registration Office, Chiang Mai University
- Faculty of Engineering, Data Science Program, Chiang Mai University

4 Results

From Comparative Study on Privacy Impact Assessment Metrics on Multi-domain Transactional Processing: Case Study of Registration Office, Chiang Mai University

Table 9. shows the details of assessors.

Pre/Gap Assessment	
Standard	Defines DPIA based on standards. ISO-IEC-27001-2013 and the NIST Cybersecurity Framework.
Audit date(s)	2/2/2023
Auditor(s) name	Deputy Director and Computer Network/Information System Administrator of Registration Office, Chiang Mai University

Client Information	
Company name:	Registration Office, Chiang Mai University
Company address:	239 Huay Kaew Road, Suthep Subdistrict, Mueang District, Chiang Mai 50200
Contact person:	Deputy Director of Registration Office, Chiang Mai University
Email:	dussadee.p@cmu.ac.th

4.1 Risk Assessment from the Specified DPIA Using GS1 Tool

As for the results of risk prioritization using GS1 tool, they were all above 80%, with the results in the range of 0.00 - 4.86. Risk priority given to creating a process to deal with anomalies that occurred and creating a process to enable business continuity and restore the system to its previous state was in the top priority, which was 100%. It was followed by 99.41 % for risk management, 92.78 % for data protection system in an organization, and 84.48 %, which was in the least priority, for anomaly detection.

The findings of the risk assessment carried out with GS1 tool ranged from 0.00 - 0.48, indicating that the risks were all extremely low. Anomaly detection had the highest risk assessment result, coming in at 0.48, followed by the risk management, which was 0.13. The risk assessment results of creating a process to deal with anomalies that occurred was 0.10, of data protection system in an organization was 0.08, and of creating a process to enable business continuity and restore the system to its previous state was 0.00, which was the lowest risk. The assessment summary of GS1 tool is shown in Tables 10.

Table 10. shows an assessment summary of GS1 tool.

DPIA	Likelyhood	Impact	% Compliance	GS1
1. Identify (ID)	very low	very low	99.41	0.13
2. Protect (PR)	very low	very low	92.78	0.08
3. Detect (DE)	very low	very low	88.48	0.48
4. Respond (RS)	very low	very low	100.00	0.10
5. Recover (RC)	very low	very low	100.00	0.00

4.2 Risk Assessment from the Specified DPIA Using iPIA Tool

All of the results of risk prioritization using iPIA tool were at a high level of more than 80%, with the results in the range of 0.00 - 4.86. Risk priority given to creating a process to deal with anomalies that occurred and creating a process to enable business continuity and restore the system to its previous state was in the top priority, which was 100%. It was followed by 99.41 % for risk management, 92.78 % for data protection system in an organization, and 84.48 %, which was in the least priority, for anomaly detection.

All findings of the risk assessment carried out with iPIA tool were low and extremely low, which ranged from 1.98 - 4.86. The assessment result of low risk level included creating a process to enable business continuity and restore the system to its previous state, which had the highest risk assessment result, coming in at 4.86. It was followed by the risk of creating a process to deal with anomalies that occurred, which was 4.40. As for the assessment results of extremely low risk level, anomaly detection came in at 2.33, data protection system in an organization was 1.98, and the risk management was 0.48, which had the lowest risk assessment result. The assessment summary of iPIA tool is shown in Tables 11.

Table 11. shows an assessment summary of iPIA tool.

DPIA	Likelyhood	Impact	% Compliance	iPIA
1. Identify (ID)	very low	very low	99.41	0.48
2. Protect (PR)	very low	very low	92.78	1.98
3. Detect (DE)	very low	very low	88.48	2.33
4. Respond (RS)	very low	low	100.00	4.40
5. Recover (RC)	very low	low	100.00	4.86

4.3 Risk Assessment from the Specified DPIA Using SPIA Tool

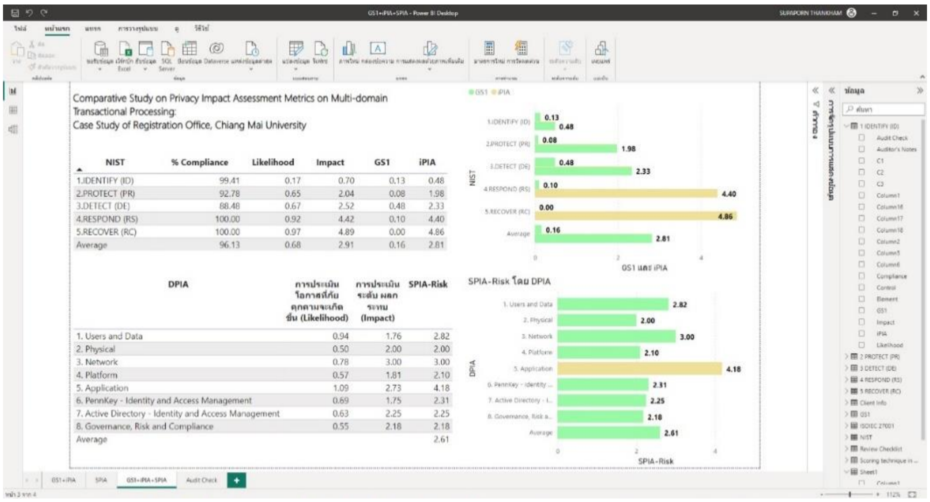
All findings of the risk assessment carried out with SPIA tool were low and extremely low, which ranged from 2.00 - 4.18. The assessment result of low risk level included applucatoion which had the highest risk assessment result, coming in at 4.18.

As for the assessment results of extremely low risk level, Users and Data was 2.82, Physical was 2.00, Network was 3.00, Platform was 2.10, PennKey - Identity and Access Management was 2.31, Active Directory - Identity and Access Management was 2.25, and Governance, Risk and Compliance was 2.18, which had the risk assessment result. The assessment summary of SPIA tool is shown in Tables 12.

Table 12. shows a summary of risk assessment using SPIA tool.

Category	Probability	Consequences	SPIA
1. Users and Data	very low	very low	2.82
2. Physical	very low	very low	2.00
3. Network	very low	very low	3.00
4. Platform	very low	very low	2.10
5. Application	very low	low	4.18
6. PennKey - Identity and Access Management	very low	very low	2.31
7. Active Directory - Identity and Access Management	very low	very low	2.25
8. Governance, Risk and Compliance	very low	very low	2.18

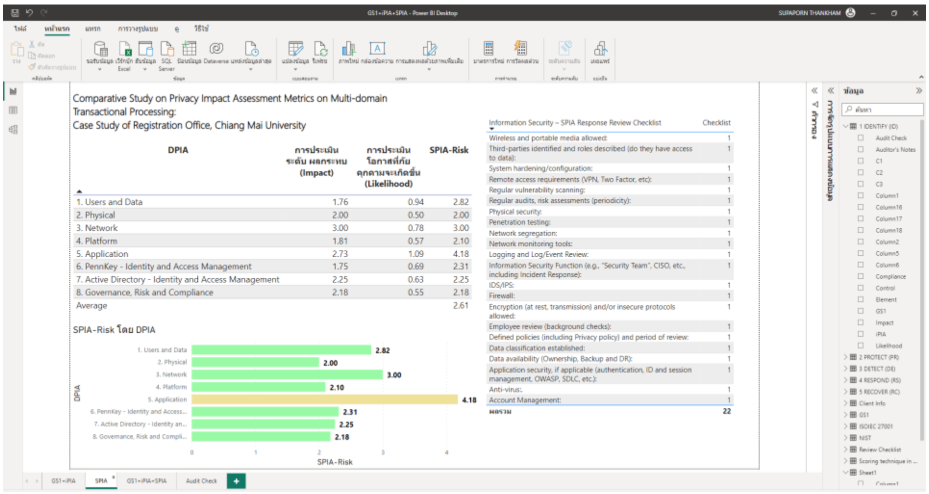
4.4 The Chart Presents a Comparison of Risk Assessment Results Using GS1 tool, iPIA tool, and SPIA Tool from the Specified DPIA.



Comparative Study on Privacy Impact Assessment Metrics on Multi-domain Transactional Processing:
Case Study of Registration Office, Chiang Mai University

NIST	% Compliance	Likelihood	Impact	GS1	iPIA
1.IDENTIFY (ID)	99.41	0.17	0.70	0.13	0.48
2.PROTECT (PR)	92.78	0.65	2.04	0.08	1.98
3.DETECT (DE)	88.48	0.67	2.52	0.48	2.33
4.RESPOND (RS)	100.00	0.92	4.42	0.10	4.40
5.RECOVER (RC)	100.00	0.97	4.89	0.00	4.86
Average	96.13	0.68	2.91	0.16	2.81

DPIA	การประเมินโอกาสที่ภัยคุกคามจะเกิดขึ้น (Likelihood)	การประเมินระดับ ผลกระทบ (Impact)	SPIA-Risk
1. Users and Data	0.94	1.76	2.82
2. Physical	0.50	2.00	2.00
3. Network	0.78	3.00	3.00
4. Platform	0.57	1.81	2.10
5. Application	1.09	2.73	4.18
6. PennKey - Identity and Access Management	0.69	1.75	2.31
7. Active Directory - Identity and Access Management	0.63	2.25	2.25
8. Governance, Risk and Compliance	0.55	2.18	2.18
Average			2.61



Comparative Study on Privacy Impact Assessment Metrics on Multi-domain Transactional Processing:
Case Study of Registration Office, Chiang Mai University

DPIA	การประเมิน ระดับ ผลกระทบ (Impact)	การประเมิน โอกาสที่ภัยคุกคามจะเกิดขึ้น (Likelihood)	SPIA-Risk
1. Users and Data	1.76	0.94	2.82
2. Physical	2.00	0.50	2.00
3. Network	3.00	0.78	3.00
4. Platform	1.81	0.57	2.10
5. Application	2.73	1.09	4.18
6. PennKey - Identity and Access Management	1.75	0.69	2.31
7. Active Directory - Identity and Access Management	2.25	0.63	2.25
8. Governance, Risk and Compliance	2.18	0.55	2.18
Average			2.61

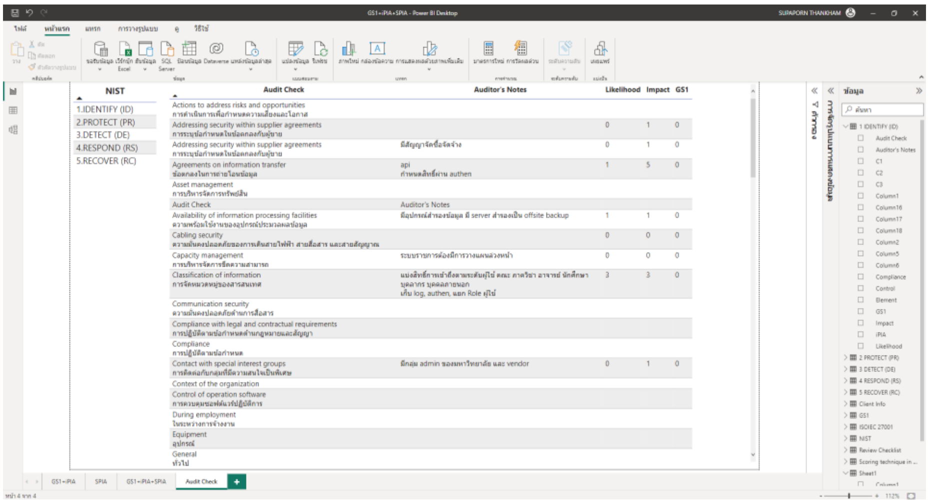
SPIA-Risk โดย DPIA

Information Security – SPIA Response Review Checklist	Checklist
Wireless and portable media allowed:	1
Third-parties identified and roles described (do they have access to data):	1
System hardening/configuration:	1
Remote access requirements (VPN, Two Factor, etc):	1
Regular vulnerability scanning:	1
Regular audits, risk assessments (periodicity):	1
Physical security:	1
Penetration testing:	1
Network segregation:	1
Network monitoring tools:	1
Logging and Log/Event Review:	1
Information Security Function (e.g., "Security Team", CISO, etc., including Incident Response):	1
IDS/IPS:	1
Firewall:	1
Encryption (at rest, transmission) and/or insecure protocols allowed:	1
Employee review (background checks):	1
Defined policies (including Privacy policy) and period of review:	1
Data classification established:	1
Data availability (Ownership, Backup and DR):	1
Application security, if applicable (authentication, ID and session management, OWASP, SDLC, etc.):	1
Anti-virus:	1
Account Management:	1
ผลรวม	22

Figure 4 shows a comparison of risk assessment results using GS1 tool, iPIA tool, and SPIA tool from the specified DPIA.

According to Figure 4, it shows a comparison of risk assessment results using GS1 tool, iPIA tool, and SPIA tool from the specified DPIA as follows:

- The use of the GS1 tool demonstrated the lowest risk score because efficiency control scores were taken into the computation. When risk control measures were implemented, the risk or damage could be mitigated.
- Using iPIA tool took into account an operator's perspective. Therefore, the risk score was higher than when using GS1tool as it recognized the likelihood that threat scenarios would occur as well as impact level that directly affected an operator.
- SPIA tool was used as a privacy risk assessment. This tool has two risk scores for threat scenarios: predefined and current states. If a predefined risk management on any aspect of the DPIA was planned, the score clearly would be very high.



NIST
1.IDENTIFY (ID)
2.PROTECT (PR)
3.DETECT (DE)
4.RESPOND (RS)
5.RECOVER (RC)

Audit Check	Auditor's Notes	Likelihood	Impact	GS1
Actions to address risks and opportunities การดำเนินการเพื่อกำหนดความเสี่ยงและโอกาส				
Addressing security within supplier agreements การระบุข้อกำหนดในข้อตกลงกับผู้ขาย		0	1	0
Addressing security within supplier agreements การระบุข้อกำหนดในข้อตกลงกับผู้ขาย	มีสัญญาจัดซื้อจัดจ้าง	0	1	0
Agreements on information transfer ข้อตกลงในการถ่ายโอนข้อมูล	api กำหนดสิทธิ์ผ่าน authen	1	5	0
Asset management การบริหารจัดการทรัพย์สิน				
Audit Check	Auditor's Notes			
Availability of information processing facilities ความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล	มีอุปกรณ์สำรองข้อมูล มี server สำรองเป็น offsite backup	1	1	0
Cabling security ความมั่นคงปลอดภัยของการเดินสายไฟฟ้า สายสื่อสาร และสายสัญญาณ		0	0	0
Capacity management การบริหารจัดการขีดความสามารถ	ระบบราชการต้องมีการวางแผนล่วงหน้า	0	0	0
Classification of information การจัดหมวดหมู่ของสารสนเทศ	แบ่งสิทธิ์การเข้าถึงตามระดับผู้ใช้ คณะ ภาควิชา อาจารย์ นักศึกษา บุคลากร บุคคลภายนอก เก็บ log, authen, แยก Role ผู้ใช้	3	3	0
Communication security ความมั่นคงปลอดภัยด้านการสื่อสาร				
Compliance with legal and contractual requirements การปฏิบัติตามข้อกำหนดด้านกฎหมายและสัญญา				
Compliance การปฏิบัติตามข้อกำหนด				
Contact with special interest groups การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ	มีกลุ่ม admin ของมหาวิทยาลัย และ vendor	0	1	0
Context of the organization				
Control of operation software การควบคุมซอฟต์แวร์ปฏิบัติการ				
During employment ในระหว่างการจ้างงาน				
Equipment อุปกรณ์				
General ทั่วไป				

Figure 5 shows the details of risk assessment and risk control by assessors using GS1 tool from the specified DPIA.

According to Figure 5, it shows the details of risk assessment and risk control by assessors using GS1 tool from the specified DPIA. The use of GS1 tool demonstrated the lowest risk score because efficiency control scores were taken into the computation. When risk control measures were implemented, the risk or damage could be mitigated. The assessors had risk control measures, which can be seen in detail by drilling down to the data or filtering the data as shown in the figure.

Regarding the assessment to conduct a comparative study on privacy impact assessment metrics according to the Personal Data Protection Act, B.E. 2562 (2019) on multi-domain transactional processing of Registration Office, Chiang Mai University, and presenting the analysis results with Microsoft Power BI using a focus group with executives and relevant personnel of Registration Office, Chiang Mai University, this chapter will present a summary of the study results, problems and obstacles arising during the study and recommendations for future development and improvement.

5 Discussion and Conclusion

5.1 Summary of the Study Results

According to this independent study, in accordance with guidelines for a comparative study on privacy impact assessment metrics according to the Personal Data Protection Act, B.E. 2562 (2019) on multi-domain transactional processing in performing a DPIA for high-risk data, it then can be interpreted into metrics. The researcher carried out the assessment using GS1 tool, iPIA tool, and SPIA tool, offering a privacy risk metric in which a risk score enables the progress in mitigating privacy risks during system development to be measured quantitatively. As for risk measures, potential risks and impacts was used, except for the risk assessment from GS1tool, controllers were used to assess risk scores as well. The risk scores were calculated using all the three tools. The weights and magnitudes of all impacts were equally used in the assessment. However, the magnitude of the impacts could have different weights depending on the situation.

A comparison of the results with those of other relevant studies: When comparing the results of the privacy impact assessment with other studies using the same assessment tools, the results included the following:

- Using GS1 tool for relevant research. For example, Thai Health Database Integration [13] used GS1 tool to assess the health device risk. The devices with privacy risks were grouped according to specified criteria, which were categorized into low, moderate and high-risk groups. Standardized controls for risk mitigation were also used the same as in this independent study. If the risk assessment score is high, immediate action must be taken to mitigate the risk.
- Using iPIA tool. The Institute of Management Information Systems, the University of Vienna [10] carried out a privacy risk assessment by having operators and data subjects to be assessors. If the risk assessment score is high, immediate action must be taken to mitigate the risk.
- Using SPIA tool for relevant research, such as the privacy risk assessment of the Information Security Special Program [4] to improve the University of Pennsylvania data protection. It was divided into three categories according to sensitivity level of data: low, moderate, and high. In the event that it is high, the university is required to report to the government and/or notify an individual if the data was accessed inappropriately.

Therefore, the researcher believed that the assessment using SPIA tool is most suitable for a comparative study on privacy impact assessment metrics on multi-domain transactional processing: case study of Registration Office, Chiang Mai University because it has a comprehensive DPIA and is designed specifically for privacy impact assessments in university work.

A summary of the results and a comparison of risk acceptance criteria. Determining threshold criteria from relevant research related risk acceptance criteria, the risk assessment scores are at an extremely low to moderate level. If the risk assessment score is high and extremely high, a risk management plan must be prepared urgently and risk management is carried out in the next stage.

5.2 Problems and Obstacles

According to this independent study, the problems and obstacles encountered can be classified as follows: The assessment process for a comparative study on privacy impact assessment metrics according to the Personal Data Protection Act, B.E. 2562

(2019) on multi-domain transactional processing of Registration Office, Chiang Mai University. Assessors were mainly the ones who filled out the assessment form. Assessment with a large amount of data required careful analysis and considerable time. Comparing the specified DPIA with assessments from other assessors may result in different assessment results. As for the limitation of this independent study, the researcher used only the data of Registration Office, Chiang Mai University. It is possible that the results will be different if the risk assessment is applied to other populations. Assessors only used GS1 tool, iPIA tool, and SPIA tool to analyze the specified DPIA. If other risk assessment tools are used, different results may be obtained.

5.3 Comments and Recommendations

The risk assessment carried out by the 3 tools using the same weights, and magnitudes of all impacts were equally used in the assessment. However, the magnitude of the impacts could have different weights depending on the situation. For example, consider a circumstance where CCTV cameras are used in a company. If the cameras were placed around the bathroom, it could violate customer privacy. Weighting for 'disclosure' should be higher than the assessment from other CCTV cameras. Thus, in the future, proper weights and magnitudes of impacts should be decided to include magnitudes of impacts along with assigning appropriate weights to the assessment. Interested parties should study further to find other risk factor variables used in the study to cover all risk factors. Also, external risk factors should be assessed to cover all types of privacy risks that will occur. GS1tool, iPIA tool, and SPIA tool were used in this independent study to analyze the specified DPIA. Subsequent users may need to modify the tool and make the DPIA more suitable. As for the development of privacy risk assessment criteria, it should be adjusted to suit the data being assessed because the researcher used only the data of Registration Office, Chiang Mai University.

References

1 Informatio[1] ศุภวัชร์ มาลานนท์, "การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล, มหาวิทยาลัยสงขลานครินทร์, 2020.

2 GS1: GS1 EPC/RFID Privacy Impact Assessment Tool (2012)

3 Oetzel, M.C., Spiekermann, S.: A systematic methodology for privacy impact assessments: a design science approach. Eur. J. Inf. Syst. 23, 126–150 (2013)

4 University of Pennsylvania: Introduction to the SPIA Program. http://www.upenn.edu/computing/security/spia/spia_step_by_step.pdf

5 สำนักเลขาธิการคณะรัฐมนตรี, "ราชกิจจานุเบกษา," 27 05 2562. [Online]. Available: http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF. [Accessed 30 05 2565].

6 จิตติมา เทียมบุญประเสริฐ. พิมพลักษณ์, กรุงเทพฯ : คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนดุสิต, 2546:117

7 WHMCompleteSolution, "ZimpleCloud," 2023. [Online].. Available: https://support.zimple.cloud/index.php. [Accessed 21 03 2023].

8 PRESS.in.th, "PRESS RELEASE," 28 05 2022. [ออนไลน์]. Available: https://www.press.in.th/pdpa-dpia-gdpr/. [%1 ที่เข้าถึง 22 03 2023].

9 GS1, "GS1 EPC/RFID Privacy Impact Assessment Tool," GS1, 07 2015. [Online]. Available: https://www.gs1.org/standards/rfid/pia. [Accessed 30 05 2022].

10 Oetzel, Marie Caroline, and Sarah Spiekermann. "A systematic methodology for privacy impact assessments: a design science approach." European Journal of Information Systems 23.2 (2014): 126-150.

11 "แผนบริหารความเสี่ยง สำนักทะเบียนและประมวลผล มหาวิทยาลัยเชียงใหม่ ประจำปีงบประมาณ พ.ศ. 2565 (1 ตุลาคม 2564 - 30 กันยายน 2565)", โดย สำนักทะเบียนและประมวลผล มหาวิทยาลัยเชียงใหม่, 2565, แผนบริหารความเสี่ยง, หน้า 11.

12 Vose, D.: Risk Analysis: A Quantitative Guide. John Wiley & Sons, Chichester (2008)

13 สถาบันรหัสสากล สภาอุตสาหกรรมแห่งประเทศไทย, "GS1 THAILAND," GS1 THAILAND, 7 2016. [ออนไลน์]. Available: https://gs1th.org/wp-content/uploads/2018/01/vol.23-no.3-2016.pdf. [%1 ที่เข้าถึง 10 4 2023].n Commissioner's
Office UK: Conducting privacy impact assessments code of practice. 50 (2014)