Available online at http://www.ssstj.sci.ssru.ac.th

Suan Sunandha Science and Technology Journal
©2021 Faculty of Science and Technology, Suan Sunandha Rajabhat University

The Utilization of ISO/IEC 27001:2013 as a Framework for Security Improvement in Accordance with GDPR for SMEs

Pongporn Pawanawichien*, **Thossaporn Thossansin***, **Auttapon Pomsathit**

College of Digital Innovation Technology, Rangsit University,
52/347 Lak Hok, Mueang Pathum Thani District, Pathum Thani 12000, Thailand
Corresponding author e-mail: *Pongporn.pa58@rsu.ac.th, Thossaporn@rsu.ac.th

Received: *22 March 2020*/**Revised:** *29 Jan 2021* /**Accepted:** *15 June 2021*

Abstract

General Data Protection Regulation (GDPR) – a regulation from European Union (EU) aims for the security of 'Personally Identifiable Information' (PII) of EU residents. It gives an individual a power to have control over the processing of their personal data by organizations. As it is, the regulation does refer to the information security controls needed to ensure the security of PII. In this paper, we propose an information security assessment on management of PII for Small and Medium-sized Enterprises (SMEs) by incorporating 'ISO/IEC 27001:2013 Annex A. Reference control objective and controls.' into the management of PII in accordance with GDPR for PII security improvement. We have determined that following the quantitative research method is appropriate as this research is aimed to determine the existence of information security controls applicable to the management of PII within the organization. A set of questions was created for interview with sampled organizations to determine the existence of information security controls according to 'ISO/IEC 27001:2013 Annex A. Reference control objective and controls.'. Content analysis where pre-existing records and evidence will be requested and reviewed will also be applied to ensure that the information security controls is actually implemented.

It was found that in most organizations, however, there exists a good coverage of the information security controls according to 'ISO/IEC 27001:2013 Annex A. Reference control objective and controls.', but have difficulty providing evidence justifying the adequacy of the information security control implemented. This is mainly due to the lack of management systems to justify the adequacy of various security controls implemented in the first place.

'ISO/IEC 27001:2013' may be used as a framework for PII security control assessment to justify the adequacy or improve upon various security controls implemented for PII.

Keywords: ISO/IEC 27001:2013, GDPR, Data privacy, SMEs and Personally Identifiable Information

1. Introduction

General Data Protection Regulation (GDPR) – a regulation from European Union (EU) aims for the security of personally identifiable information (PII) of EU residents. It gives an individual a power to possess control over the processing of their personal data by organizations.

GDPR is a set of regulation which defines how an organization will process PII of an EU individual person. Individual person is referred to as 'data subjects'.

GDPR regulations covers:

- "What is expected from an organization on various data processing activities within the organization."
- "Data subject rights to their own PII. "
- "Jurisdiction of supervisory authority."

(Punit, 2018).

Implementing the organizational management of PII according to GDPR will provide benefits for the organizations, which includes:

- "**Providing insight of the data that exists within the company**" (Punit, 2018): Implementing GDPR regulations means you will have to create a list of personal data under the responsibilities within the organization, as well as the duration of storage, purpose of processing, and so on. This will give insight to the data under the responsibilities of the company and will benefits greatly for future investments in data analytics and information security controls.
- "**Exhibit transparency**" (Punit, 2018): Implementing GDPR regulations also means you must list all of PII you collect, specify how you will process it. If done correctly, will induce trust from customers as you are clear on what you do and why you do it.
- "**Data efficiency**" (Punit, 2018): Implementing GDPR regulations also means minimizing data collected. This can lead to immense business benefits e.g. efficient data processing and reduced data storage cost.
- "**Personal data security**" (Punit, 2018): Implementing GDPR regulations also means you have to implement various information security controls to ensure confidentiality, integrity and availability of PII. If implemented properly, will reduce incidents of data breach, loss or destruction of PII, boosting reputation of the organization.

GDPR have requirements for information security which includes:

- Protection from unlawful / unauthorized access, loss or damage to PII.
- Protection from insiders's threat.
- Protection from external threat.
- Data breach notification.
- Demonstration of data protection.

(Díaz, 2016; The European Parliament and the Council of the European Union, 2016).

However, GDPR does not refer to information security controls needed for those requirements.

There is a standard published by International Organization for Standardization (ISO) on the management of information security, namely ISO/IEC 27001:2013 which defines the structure for information security management, risk assessment, documentations, and security controls necessary to ensure security of information under its scope of management (ISO27k Forum, 2016; Tzolov, 2018).

Within ISO/IEC 27001:2013 standard, there is a set of information security controls, specifically 'ISO/IEC 27001:2013 Annex A. Reference control objective and controls.' which outlines 114 information security controls on 14 different information security control topics which includes:

- "A.5 Information security policies."
- "A.6 Organization of information security."
- "A.7 Human resource security."
- "A.8 Asset management."
- "A.9 Access Control."
- "A.10 Cryptography."
- "A.11 Physical and environmental security."
- "A.12 Operations security."
- "A.13 Communications security."
- "A.14 System acquisition, development, and maintenance."
- "A.15 Supplier relationships."
- "A.16 Information security incident management."

- "A.17 Information security aspects of business continuity management."
- "A.18 Compliance."

(ISO Copyright Office, 2013).

In this paper, we propose an information security assessment on management of Personally Identifiable Information (PII) for Small and Medium-sized Enterprises (SMEs) (Thai Winner, 2020) by incorporating 'ISO/IEC 27001:2013 Annex A. Reference control objective and controls.' into the management of PII in accordance with GDPR for PII security improvement.

2. Research Methodology

The choice of method must be made in accordance with the problem addressed which is to identify the information security controls implemented within the organization. We have determined that following the quantitative research method is appropriate as this research is aimed to determine the existence and justification of information security controls applicable to the management of PII within the organization.

The data for this research was collected by the means of surveys. A set of questions was created for interview with sampled organizations to determine the existence of information security controls according to ' ISO/ IEC 27001: 2013 Annex A. Reference control objective and controls.'

The participants were selected from Small and Medium-sized Enterprises (SMEs) which have a history of dealing with European customer(s) and were willing to contribute to this research by providing their representative to answer in person, a set of questions which were provided to determine the existence of the information security controls applicable, implemented and justified.

Content analysis where pre-existing records and evidence were requested and reviewed, were also applied to ensure that the information security controls are implemented and justified.

Out of 17 organizations inquired, 4 were willing to provide a representative to be interviewed for this research provided that they and their representative identities were kept confidential.

A Statement of Applicability, a document specific to ISO/ IEC 27001 which lists all information security controls within ' ISO/ IEC 27001:2013 Annex A. Reference control objective and controls' . and their applicability to the organization was modified to record the list of information security controls implemented within the sampled organization (Middleton-Leal, 2018).

The applicability of each information security controls for each sampled organization was determined first, based on whether the organization has an activity associated with the list of information security controls within ' ISO/ IEC 27001: 2013 Annex A.' or not.

Then, the number of information security controls implemented was determined. In order for the information security controls that existed within the company to qualify, said controls must:

- Be implemented fully or partially for the purpose of securing PII or activities regarding PII.
- Have reviewable records of implementation and operation dated back at least 3 months prior to the date of assessment.

Finally, the number of justified security controls (i.e. information security controls with evidence to justify the adequacy of information security controls implemented for the security of PII) were determined.

The results were separated into 3 groups:

- % Controls Applicable i.e.

$$\frac{Number\ of\ Applicable\ Controls}{Number\ of\ ISO/IEC\ 27001\ Controls} \times 100\%$$

- % Controls implemented i.e.

$$\frac{Number\ of\ Implemented\ Controls}{Number\ of\ Applicable\ Controls} \times 100\%$$

And,

- % Controls Justified i.e.

$$\frac{Number\ of\ Justified\ Controls}{Number\ of\ Applicable\ Controls} \times 100\%$$

The results were represented into bar graphs of percentage for each sampled organization.

3. ISO/IEC 27001:2013 and GDPR

ISO/IEC 27001:2013 standard provides framework for information security management and GDPR defined PII as a critical information which need protection (Lopes, Guarda, & Oliveita, 2019).

ISO/IEC 27001:2013 could be implemented in a way that treats PII as information asset and set the framework for the implementation of security controls (Irwin, 2018).

For example, GDPR requirements for the security of PII includes 3 main topics:

- "Security of processing."
- "Notification of a personal data breach to the supervisory authority."
- "Communication of a personal data breach to the data subject."

(The European Parliament and the Council of the European Union, 2016).

Each topic could be managed based on ISO/IEC 27001:2013 as described below:

- "Security of processing" (The European Parliament and the Council of the European Union, 2016) : This topic deals with the implementation of information security controls appropriate to the risk associated. The risk to the privacy could be integrated with risk assessment required by ISO/IEC 27001:2013 standard to determine the appropriate level of security controls implemented.
- "Notification of a personal data breach to the supervisory authority" (The European Parliament and the Council of the European Union, 2016): This topic requires data controller to notify the supervisory authority of data breach within 72 hours of breach detection. This activity could be managed through 'ISO/IEC 27001:2013 Annex A.16.1 : "Management of information security incidents and improvements' which is a set of information security controls with an objective 'To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses" (ISO Copyright Office, 2013). Which by incorporating PII data breach notification as part of data breach incident handling process, the organization would be able to comply with this topic of GDPR.
- "Communication of a personal data breach to the data subject" (The European Parliament and the Council of the European Union, 2016): This topic requires that "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay" (The European Parliament and the Council of the European Union, 2016). This activity can also be incorporated with ISO/IEC 27001:2013 Annex A.16.1 as part of data breach incident handling process too.

As shown above, GDPR may lack on defining the set of information security control for PII and ISO/IEC 27001:2013 could be used as a framework for information security controls implementation and management in accordance with GDPR (Clements & Milton, 2018).

4. Results

The result from 4 organizations were summarized into bar graphs as shown.

Organization 1: A medium sized tech company i.e. tech company with 51-200 employees with less than 200 million baht asset valuation, which has implemented ISO/IEC 27001:2013 for 1 year and was certified with ISO/IEC 27001:2013.

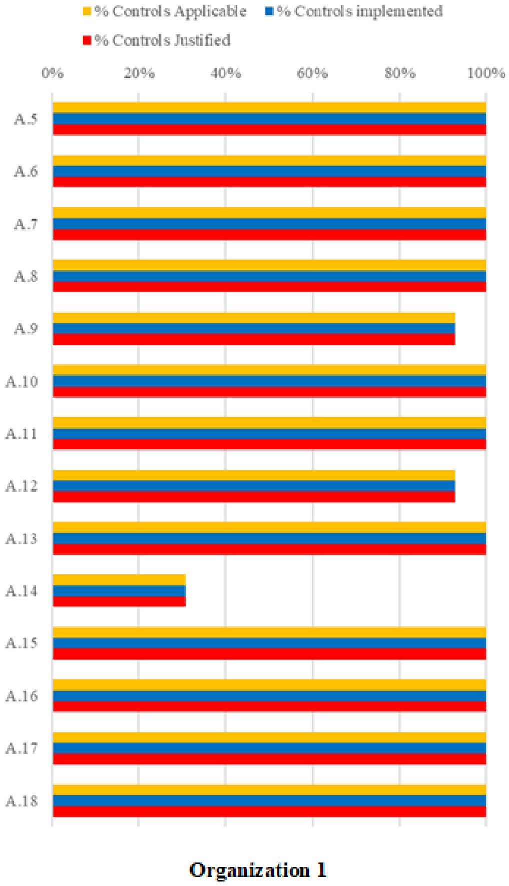

Figure 1. Figure showing the results from 'Organization 1'.

'Organization 1' shows a strong information security controls and management implemented within the organization where all information security controls applicable were implemented and justified. The applicability and justification were supported by a risk assessment and treatment plan where PII is a part of, by being incorporated within an asset inventory which is then under the scope of each risk assessment.

Organization 2: A medium sized trading company i.e. trading company with 26-50 employees with less than 100 million baht asset valuation, which deals with international trading of tech commodities.

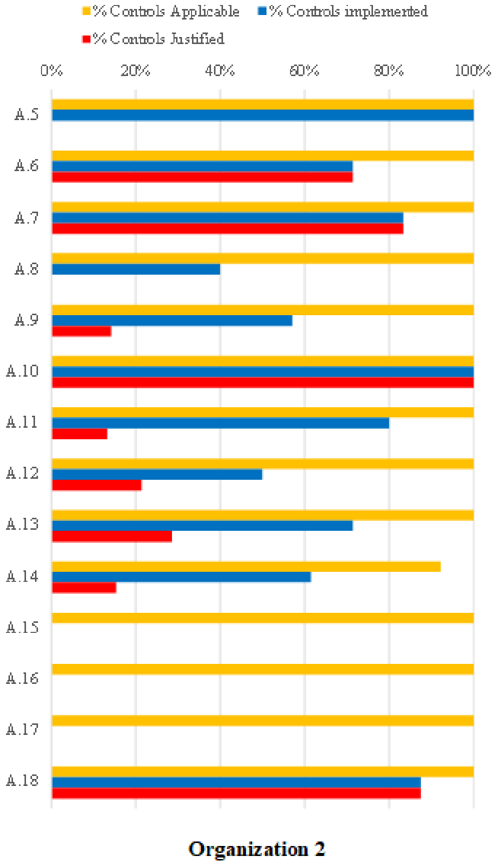

Figure 2. Figure showing the results from 'Organization 2'.

'Organization 2' shows a high coverage of applicable security controls, where existing security controls however implemented, reveals that a huge portion does not covers the aspects of the security for PII. Existing controls adequacy were only justified by contractual requirements but not based on systematic risk assessmentand there's a high risk of infringement with GDPR.

It is recommended that 'organization 2' should consider establishing a management system for the management of information security with regards to PII in order to plan for, implement the necessary controls, internally check for improvement and continually improve upon information security and PII management.

Organization 3: A small sized trading company i.e. trading company with less than 25 employees and less than 50 million baht asset valuation, undergoing

ISO/IEC 27001:2013 implementation. The organization has occasional EU customers.

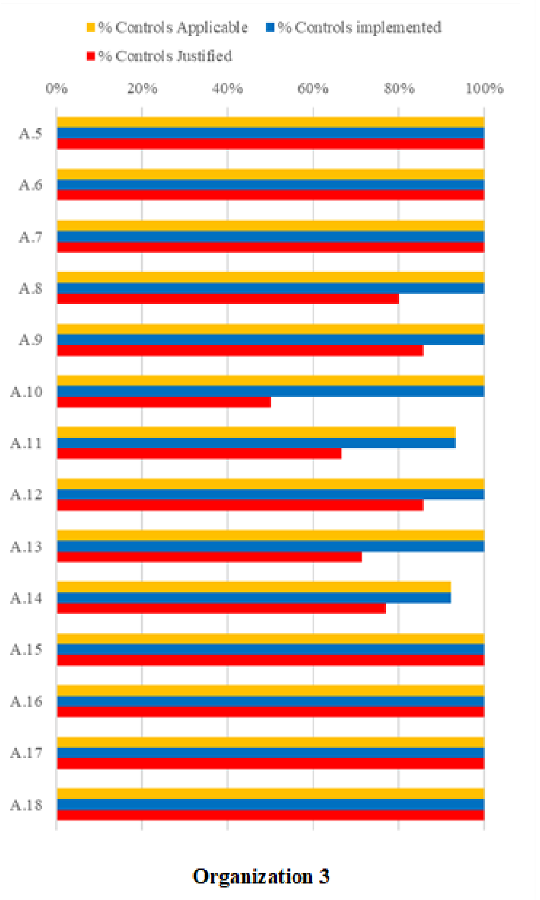

Figure 3. Figure showing the results from 'Organization 3'.

'Organization 3' also shows a strong information security controls and management implemented within the organization. All information security controls applicable were implemented. The justification was a bit lacking due to the fact that risk assessment done is yet to cover the whole range of information security controls applicable. The applicability and justification were supported by a risk assessment and treatment plan where PII is a part of, by being incorporated as part of asset inventory.

As 'Organization 3' has an established management system in place for the management of PII, however it is lacking in some parts. It is recommended that the organization should seek expert audit or consult from 3rd party to provide additional aspects to the management of information security and PII management.

Organization 4: A small estate management company i.e. an estate management company with less than 50 employees and less than 50 million baht asset valuation, with an occasional EU client.

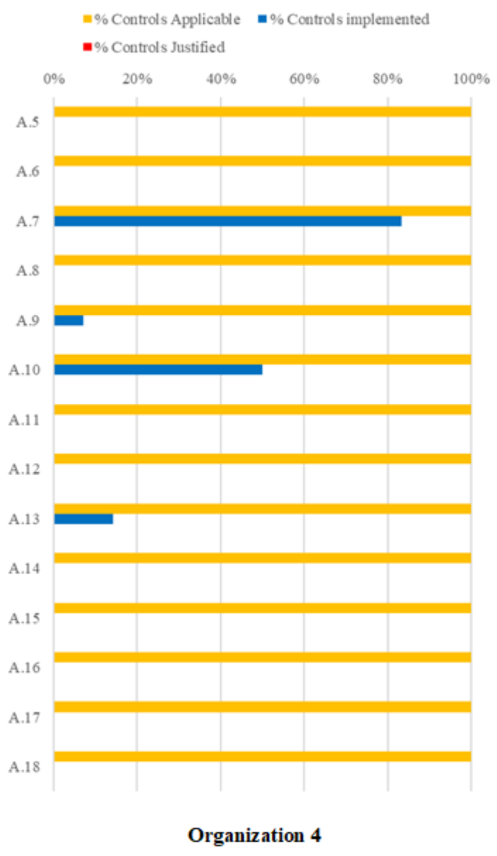

Figure 4. Figure showing the results from 'Organization 4'.

'Organization 4' also shows a high coverage of applicable security controls. However, they are unaware of their inadequacy of information security controls that existed. The security controls for PII exists only in part. Existing implemented security controls are inevidently justifiable. GDPR infringement is certain.

It is strongly recommended that 'organization 4' should immediately consider to seek an expert consultation for an establishment of an information security and PII management system for the management of information security with regards to PII in order to plan for, implement the necessary controls, internally check for improvement and continually improve upon information security and PII management.

5. Conclusions

It is observed that Organizations 2 and 4, while they are not implementing ISO/IEC 27001 standard, they could show the implementation and justification of the security of PII by contractual and legal means. This is in contrast with Organizations 1 and 3 which have implemented ISO/IEC 27001 as an information security framework and justify the security controls via risk assessment records. This may indicate that by setting a specific contractual or legal specification, the organization could use them as a basis for implementing and justifying information security control for PII. However, more research on this aspect may be needed.

It was found that organizations with ISO/IEC 27001:2013 implementation have less difficulty providing a good coverage of the information security controls according to 'ISO/IEC 27001:2013 Annex A. Reference control objective and controls.', on PII and have less difficulty providing evidence justifying the implementation and adequacy of the information security control for PII implemented. In contrast with an organization with unmanaged security management where they were unaware that their existing information security controls does not justifiably cover the security of PII mainly due to the lack of management systems to justify the adequacy of various security controls implemented in the first place.

'ISO/IEC 27001:2013' May be used as a framework for PII security control assessment to justify the adequacy or improve upon various security controls implemented for PII.

6. References

Clements, T., & Milton, S. (2018). *Maintaining data protection and privacy beyond GDPR implementation*. ISACA.

Díaz, E. D. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions. *Church, Communication and Culture*, *1*(1), 206-239.

Irwin, L. (2018, August 31). *How ISO 27001 can help you achieve GDPR compliance*. Retrieved from itgovernance: https://www.itgovernance.co.uk/blog/how-iso-27001-can-help-you-achieve-gdpr-compliance

ISO Copyright Office. (2013). ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements. *INTERNATIONAL*. ISO Copyright Office.

ISO27k Forum. (2016). ISO 27001 Security. *Mapping between GDPR (the EU General Data Protection Regulation) and ISO27k*, 1-19.

Lopes, I., Guarda, T., & Oliveita, P. (2019). How ISO 27001 can help achieve GDPR compliance. *14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-6.

Middleton-Leal, M. (2018). *GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance?* Retrieved from netwrix: https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/

Punit, B. (2018). *Intro to GDPR - A Plain English Guide to Compliance*. Croatia, EU: Advisera Expert Solutions Ltd.

Thai Winner. (2020, August 11). Retrieved from https://thaiwinner.com/what-is-sme/

The European Parliament and the Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. Official Journal of the European Union.

Tzolov, T. (2018). One model for implementation GDPR based on ISO standards. *International Conference on Information Technologies (InfoTech-2018)*, 1-3.