International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 11, Number 4 (2018), pp. 649-660

http://www.irphouse.com

Personal Data Protection Maturity Model for the Micro Financial Sector in Peru

Arturo García
Escuela de Ingeniería de, Sistemas y Computación
Universidad Peruana de Ciencias Aplicadas, Lima, Perú

Francisco Dominguez
Facultad de Informática, Universidad Rey Juan Carlos, Madrid, España

Luis Calle
Escuela de Ingeniería de, Sistemas y Computación
Universidad Peruana de Ciencias Aplicadas, Lima, Perú

Javier Martinez
Facultad de Informática, Universidad Rey Juan Carlos, Madrid, España

Carlos Raymundo
Escuela de Ingeniería de, Sistemas y Computación
Universidad Peruana de Ciencias Aplicadas, Lima, Perú

Abstract

The micro financial sector is a strategic element in the economy of developing countries since it facilitates the integration and development of all social classes and let the economic growth. In this point is the growth of data is high every day in sector like the micro financial, resulting from transactions and operations carried out with these companies on a daily basis. Appropriate management of the personal data privacy policies is therefore necessary because, otherwise, it will comply with personal data protection laws and regulations and let take quality information for decision-making and process improvement. The present study proposes a personal data protection maturity model based on international standards of privacy and information security, which also reveals personal data protection capabilities in organizations. Finally, the study proposes a diagnostic and tracing assessment tool that was carried out for five companies in the micro

financial sector and the obtained results were analyzed to validate the model and to help in success of data protection initiatives.

Keywords: Maturity model; data protection; personal data; micro financial; information security.

1. INTRODUCTION

Information is currently an important asset for companies, ranging from strategic planning data, to employee data and remuneration. These include personal, numeric, alphabetical, graphic or any other type of data related to natural persons made identifiable through means or procedures. The Peruvian Law 29733 of personal data protection was published in order to protect natural persons and their personal data. Organizations must acquire resources, implement controls, and develop processes to protect their assets. Despite efforts, some companies still do not fully comply with regulations. Some organizations choose to hire security consulting services; however, small and medium size enterprises have greater difficulties to implement controls and procedures related to data protection. According to the National Superintendence of Banking and Insurance (SBS in Spanish), to date, municipal and rural banks, which make up a large majority of the micro financial sector, do not fully comply with sector regulations.

We propose a data protection maturity model based on international standards and information security best practices (ISO 17944, ISO 27001, ISO 29100). In addition, we aim at improving controls and processes to help comply with regulations. The Peruvian micro financial sector was considered as a case study because client data is sensitive due to the nature of the operations carried out. The g140 regulation of the SBS is also included in the model. The evaluation method consists of a questionnaire that must be answered, ideally, by the organization security officers, in the most honest way possible, in order to obtain reliable information in comparing the current state of their organization regarding their security practices.

2. STATE OF THE ART

A maturity model evaluates capabilities of organizations in given discipline and compares them with standards, allowing the identification of weaknesses and establishing processes for continuous improvement. In the reviewed literature a data governance maturity model prevails, designed under ISO standards in data management, records, archives, assets, and digital preservation domains, consisting in three dimensions: management, processes and infrastructure [5]. Focusing more on case studies, we see a financial information security maturity model grouped into 3 areas: management, operation and technique, with 5 levels: vulnerable, poor, medium, good and excellent [25]. A cyclic maturity assessment model in information security was also reviewed [8]. De Bruin [19] presents a cybersecurity governance model oriented to capabilities organizations must developed to have adequate data security management. In addition, organization characteristics influencing information security maturity are

divided in four categories: general (sector, earnings, number of employees), outsourcing, IT dependence and IT complexity [10]. The main objective of information security is to ensure confidentiality, integrity, and availability of information in an organization without impairing its productivity. In Turkey a questionnaire was applied to a sample of 97 companies [6] to analyze factors that influence information security in Small and Medium Enterprises (SMEs). Necessary factors to successfully implement information security procedures for governmental organizations [16]. Burdon et al. [15] examined how organizations understand and construct information security processes. After analysis in the SME sector in Australia, it was shown that cloud security and privacy factors in general are not priorities for this sector [12]. Impacts of losing financial information are also mentioned, reviewing current regulations on cyber security [23]. Finally, Beckers et al. [13] propose a method for risk management which supports ISO 27001 compliance with Information Security Management Systems. Data Protection is the process of safeguarding important data regarding corruption or loss, prioritizing personal data. Many laws and regulations exist in the world seeking to protect natural persons from being identified without their consent. Chao Li [4] shows the value of private information by presenting an algorithm which allows us to price this information. Mikkonen [24] research about the perception of final consumers regarding security of personal data. A survey with the objective of measuring compliance, using data protection principles, determined that private organizations have higher compliance levels [11]. Cradock [9] mentions the importance of classifying personal data protection [17], given that it is necessary to measure the impact of data protection regulations on company operations. Aserkar and others [18] present possible solutions to problems related to technology, regulations, and compliance policies. Future certifications options are also proposed for data protection, regime compliance, accreditation with bodies of knowledge (BoK), and authorized national entities [20]. A survey show us that people are more prone to share personal information, depending on type of information, or if it involves receiving some type of benefit, highlighting economic benefits [3]. Da Veiga and Martins [1] argue that the concepts of protection and security are interrelated and should be considered when dealing with information risks. In addition, investigations have proposed that the object of data protection laws, for the Personal Data Community, should be considered a complex adaptive system based on diversity and personal information value [14]. In addition, Van der Sloot [2] proposes that the object of the law be separated into two: natural persons and legal persons, indicating differences such as data correction. Harbinja [7] discusses post-mortem privacy and how to apply it in a practical way. Finally, there are emerging topics such as privacy engineering, research focusing on design implementation, adaptation and evaluating theories, methods and techniques [22]. Gurses [21] investigates challenges and potential problems that must be addressed by this discipline.

3. PERSONAL DATA PROTECTION MATURITY MODEL

3.1 Basis

Based on reviewed literature, we selected five maturity models related to data

protection and security. Each of these models provide relevant topics to improve data protection capabilities in an organization, these topics are called domains. Table 1 compares the selected maturity models and corresponding themes or domains. In relation to maturity levels, two of the selected models use their own maturity level definitions and the remaining models adapt CMMI levels. Of the models that use their own maturity level definitions, the Financial Information Security model focuses on data security procedures and controls, while the Data Security model for Medium-sized Companies proposes 13 maturity levels for each criterion. Levels are grouped in such a way that you can see the evolution of data security, from design stages to monitoring of controls.

Table 1: Model domain comparison matrix

Models	**Domains**			
	Data	**Information Security**	**Risks**	**Organization**
Information Governance [5]	X	X	X	X
Financial Information Security [25]	X	X		X
Cybersecurity Governance [19]		X		X
Information Security for SMEs [10]		X	X	X
Cyclical Evaluation of Information Security [8]	X	X	X	

The remaining models used adaptations of CMMI levels. The Cyber Security Governance model raised its levels as an indication of improvement in cyber security processes, from Level 1 where there is no knowledge regarding cyber security, to the Optimized Level, where processes are constantly improved. The Cyclical Data Security Assessment model, like the previous model, went through repetitive and intuitive processes until reaching continuous improvement, raising its level from the first level to the last. Finally, the information governance model uses levels proposed by CMMI. Table 2 compares aforementioned model maturity levels to select the best approach for choosing our maturity levels. After analyzing components of each model, we arrived at the resolution that no model refers to all domains, subject which could greatly improve the proposal, except for the first model, although from the governance perspective. Regarding maturity levels, we considered taking the best of both approaches and proposing an adaptation of CMMI levels, adding "organization does not recognize the importance of data protection", as the first level.

Table 2: Maturity level comparison matrix

Models	**Levels**					
	0	**1**	**2**	**3**	**4**	**5**
Information Governance [5]		Initial	Managed	Defined	Quantitatively Managed	Optimized
Financial Information Security [25]		Vulnerable	Poor	Correct	Good	Excellent
Cybersecurity Governance [19]	None		Initial	Managed		Optimized
Information Security for SMEs [10]		Designed		Implemented	Operative Efficiency	Monitored
Cyclical Evaluation of Information Security [8]	None	Initial	Repetitive	Defined	Managed	Optimized

3.2 Models

Developing a personal data protection maturity model (PDPMM) involves different factors presented in this section. In order to reach maturity, evaluated organizations go through three phases:

- Immaturity: Organizations have basic knowledge and processes to protect personal data.
- Maturity: Organizations have controlled, and defined activities related to data protection. As maturity levels increase, performance on the subject is greater.
- Excellence: Organizations are prepared for changes and activities are continuously improved.

3.3 Maturity levels

Maturity levels are a way to show degrees of optimization in company processes, in this case, personal data protection. The PDPMM has five maturity levels, throughout the immaturity, maturity, and excellence phases. The five levels are the following: • Level 1 - None: Organizations are totally or partially unaware of personal data protection

- Level 2 - Initial: Organizations know data protection aspects and make efforts to establish initial protection and privacy processes.
- Level 3 - Defined: Organizations have defined processes related to data

protection.

- Level 4 - Managed: Organization processes related to data protection are managed in such a way that identification, analysis, and evaluation activities exist.
- Level 5 - Optimized: Organizations have reached a level of excellence in its activities, periodically evaluating its processes in order to improve and eliminate errors, thus reaching high effectiveness levels.

3.4 Domains

The PDPMM is divided into four domains, grouping twenty-two criteria, as shown in Figure 1. Groups represent different data protection viewpoints in an organization.

- Data: Domain in which data life cycle is considered, in addition to security and availability.
- Information Security: Covers preventive and reactive measures by organizations allowing data protection
- Risks: Involves necessary activities for risk management such as: context definition, identification, analysis, evaluation, treatment and monitoring.
- Organizations: Evaluates involvement and knowledge in organizations and its people in relation to data protection.

3.5 References and criteria

The PDPMM consists of twenty-two criteria grouped in domains. Criteria are related to elements of the following standards, regulations, and recommendations:

- Personal Data Protection Law No. 29733: One of the main objectives of PDPMMs is for the organizations to satisfactorily comply with this law, for which different clauses and, above all, eight principles established in the law are taken into account.
- Circular No. G-140: Because the PDPMM target sector is the Peruvian microfinance sector, it is necessary to consider this SBS standard related to information security management and its subparagraphs concerning data protection.
- ISO/IEC 27002: Controls for implementation of an Information Security System (ISMS).
- ISO/IEC 29100: Privacy Framework which considers eleven privacy principles applied to legal, contractual and commercial factors, among others.
- ISO/TR 17944: Security Framework in Financial Systems from which relevant standardization areas related to data protection relevant to the Peruvian micro financial sector.

On the other hand, criteria were selected based on the recurrence of these issues in other data security maturity models. In addition, criteria are directly linked to elements mentioned above. Criteria, divided by domain, is presented in Figure 1:

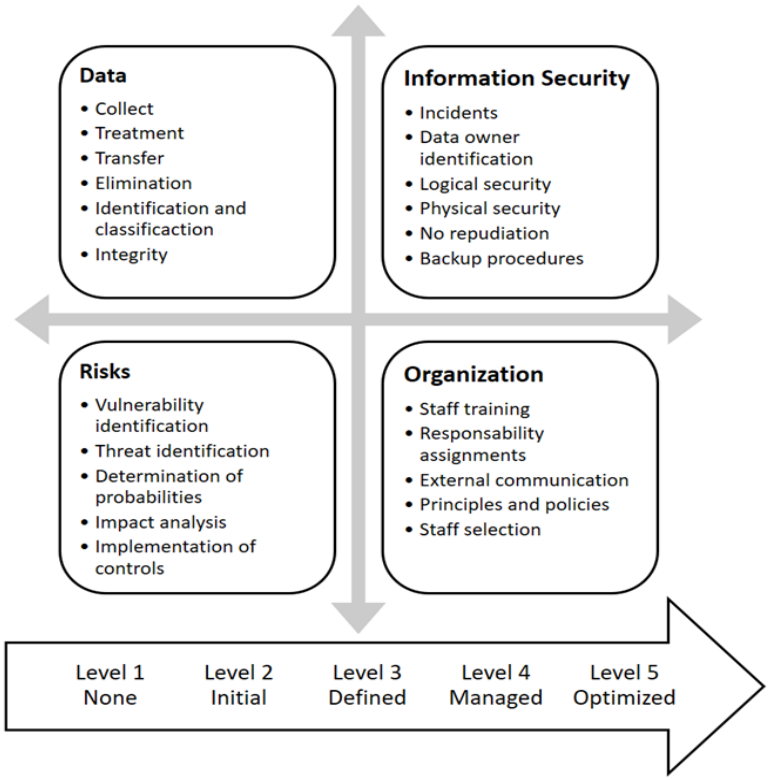

Figure 1: Personal Data Protection Maturity Model

$$Score_{Domain} = \frac{\sum_q^q w_{criteria} \cdot w_{option}}{Score_{max}} \times 100$$

$$Score_{Model} = \frac{\sum_d^d Score_{Domain}}{MScore_{max}} \times 100$$

q: Assessment questions

d: Model's domains

$w_{criterio}$: Criteria weight

$w_{opción}$: Chosen option weight

$DScore_{máx}$: Max score of the domain

$MScore_{máx}$: Max score of the model

Figure 2: Maturity model equations

3.6 Evaluation

Finally, an evaluation tool was developed, allowing organizations to self-evaluate with respect to personal data protection. The tool has four sections, one for each domain, within which there are a series of topics and questions directly related to criteria. Each question is assigned a value between one and five, given by criterion importance according to Peruvian laws protecting personal data. The equation presented in Fig. 2 was applied:

Once the formula is applied, maturity levels are applied both generally and at the domain level (Table 4).

Table 3: Score equivalence

Score	**Maturity Level**
0% < Score <= 20%	Level 1: None
20% < Score <= 40%	Level 2: Initial
40% < Score <= 60%	Level 3: Defined
60% < Score <= 80%	Level 4: Managed
80% < Score <= 100%	Level 5: Optimized

4. VALIDATION

Maturity model validation processes are separated into four activities: planning, evaluation, diagnosis, and result analysis. Planning includes selection of organizations targeted by the case study. Organizations were required to: have areas or processes related to information security, be registered in the Peruvian financing system, and be located in Peru. Five microfinance institutions were selected for the case study, with different economic and geographic characteristics, thus covering a broad spectrum. The main objective of these micro-finance companies is to aid economic and social development of clients through financial services. Among clients are natural persons and small and medium-sized entrepreneurs. Organizations were assigned fictitious names in order to safeguard information.

After selecting microfinance institutions, the model was applied. Evaluation tools were sent to contact persons. The evaluation tool has an instructive section, a section for each domain and a results section, which shows general company diagnoses, as well as maturity levels for each domain. Organizations can compare their results with average sector results and a record of evaluations made in order to auto-evaluate, improving data protection capabilities. The evaluation must be carried out by organization employees, with knowledge of each maturity model domain, for example, the information security officer for the information security domain, the risk manager for the risk domain and so on. Table 4 show us the general results for each company.

Table 4: General results

Micro Financial Organization	General Results	
	Score	**Maturity Level**
A	31%	Level 2: Initial
B	28%	Level 2: Initial
C	43%	Level 3: Defined
D	64%	Level 4: Managed
E	74%	Level 4: Managed

In order to include all data protection perspectives, results are presented for each domain, in a comparative matrix of all microfinanciers in the case study and are shown in Table 5. Analyzing results, it is evident that the risks domain obtains the lowest score of the first three organizations, which are those that have less income than micro financial D and E, needing to be prioritized in order to assure clients their data is not in danger. In addition, it is evident that the data domain is the most stable among the institutions, however, only one organization is at managed level in this domain, all the others vary between level two and three, which means that it is a domain that needs to be addressed urgently in order to comply with regulatory standards. Our personal data protection maturity model differs from other existing models, in that it covers all relevant domains for data protection, referencing international standards and conducing evaluations for final presentation of results, which are individual, by domain, and comparative with sector averages.

Table 5: Results by domain

Micro Financial Organization	Domains			
	Data	**Information Security**	**Risks**	**Organization**
A	50%	22%	17%	17%
B	28%	30%	10%	31%
C	57%	26%	10%	67%
D	57%	66%	83%	69%
E	69%	77%	73%	77%

5. CONCLUSIONS

We analyzed maturity models directly related to information security and data protection, identifying, and comparing their most important components such as maturity levels, domains, and criteria. We used this information as input for designing our model. In addition, international accepted standards and regulatory standards

applied to the microfinance sector were taken as references.

The evaluation tool allowed micro-financiers of the case study to know the current personal data protection level they possess, as well as indicating which domains and criteria they should prioritize in order to improve data protection capabilities. In addition, in the history section, organizations can make improvements and re-take the assessment, so they can visualize their evolution over time in terms of data protection capabilities.

In addition, our study gives insight into personal data protection in the Peruvian microfinance sector, in order to improve current maturity models, adapting them to current security needs in the sector.

6. REFERENCES

[1] Adéle Da Veiga and Nico Martins (2015). Information security culture and information protection culture: A validated assessment instrument in Computer Law and Security Review.

[2] B. van der Sloot (2015). Do privacy and data protection rules apply to legal persons, and should they? A proposal for a two-tiered system in Computer Law and Security Review.

[3] Bjoern, Roeber, Rehse Olaf, Knorrek Robert and Thomsen Benjamin (2015). Personal data: how context shapes consumers' data sharing with organizations from various sectors in Electronic Markets.

[4] Chao Li, Daniel Yang Li, Gerome Miklau and Dan Suciu (2014). A theory of pricing private data in Association for Computing Machinery.

[5] Diogo Proenca, Ricardo Vieira and José Borbinha (2016). A maturity model for information governance in nformation Systems and Technologies.

[6] Ebru Yeniman Yildirim, Gizem Akalp, Serpil Aytac and Nuram Bayram (2011). Factors influencing information security management in small- and medium sized enterprises: A case study from Turkey in International Journal of Information Management.

[7] Edina Harbinja (2017). Post-mortem privacy 2.0: theory, law, and technology in International Review of Law, Computers and Technology.

[8] Evandro Alencar Rigon, Carla Merkle Westphall, Daniel Ricardo dos Santos and Carlos Becker Westphall (2014). A cyclical evaluation model of information security maturity Approach in Lectures Notes in Computer Science.

[9] Emma Cradock, Sophie Stalla-Bourdillon and David Millard (2017). Nobody puts data in a corner? Why a new approach to categorising personal data is required for the obligation to inform in Computer Law and Security Review.

[10] Frederik Mijnhardt, Thijs Baars and Marco Spruit (2016). Organizational characteristics influencing SME information security maturity in International

Association for Computer Information Systems.

[11] Hui Na Chua, Anthony Herbland, Siew Fan Wong and Younghoon Chang (2017). Compliance to Personal Data Protection Principles: A Study of How Organizations Frame Privacy Policy Notices in Telematics and Informatics.

[12] Ishan Senarathna, William Yeoh, Matthew Warren and Scott Salzman (2016). Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs in Australasian Journal of Information Systems

[13] Kristian Beckers, Maritta Heisel, Bjornar Solhaug and Ketil Stolen (2014). ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system in ACM Transactions on Database Systems.

[14] Kunbei Zhang, Aernout H.J. Schmidt (2016). Thinking of data protection law's subject matter as a complex adaptive system: A heuristic display in Computer Law and Security Review.

[15] Mark Burdon, Jodie Siganto and Lizzie Coles-Kemp (2016). The regulatory challenges of Australian information security practice in Computer Law and Security Review.

[16] Maryam Al-Awadi and Karen Renaud (2016), Information security management system implementation success factors in Advance Science Letters.

[17] O.M. Fal (2014). Standardization in personal data protection in Cybernetics and System Analysis.

[18] Rajiv Aserkar, A. Seetharaman, Joy Ann Macaso Chu, Veena Jadhav and Shivani Inmdar (2017). Impact of personal data protection (PDP) regulations on operations workflow in Human Systems Management.

[19] Rossouw de Bruin and SH von Solms (2016). Modelling Cyber Security Governance Maturity in Institute of Electrical and Electronics Engineers Inc.

[20] Rowena Rodrigues, David Barnard-Wills, Paul De Hert and Vagelis Papakonstantinou (2016). The future of privacy certification in Europe: an exploration of options under article 42 of the GPDR in International Review of Law, Computers and Technology.

[21] Seda Gurses (2014). Privacy and security: Can you engineer privacy? The challenges and potential approaches to applying privacy research in engineering practice in Association for Computing Machinery.

[22] Seda Gurses and Jose M. del Alamo (2016). Privacy Engineering: Shaping an Emerging Field of Research and Practice in Institute of Electrical and Electronics Engineers Inc.

[23] Thomas A. Hemphill and Phil Longstreet (2016). Financial data breaches in the

U.S. retail economy: Restoring confidence in information technology security standards in Technology in Society.

[24] Tomi Mikkonen (2015). Perceptions of controllers on EU data protection reform: A Finnish perspective in Computer Law and Security Review.

[25] Youn-Rai Park, Yoon-Chul Choy and Won-Sung Shon (2014). Study on financial-sector information security level assessment and improvement anticipation model in Science and Engineering Research Support Society.