Information Security Frameworks for Assisting GDPR Compliance in Banking Industry

Abstract

Purpose – Data can nowadays be seen has the main asset of organizations and data leaks have a considerable impact on organizations image, revenues, and possible consequences to the affected clients. One of the most critical industries is Banking. Information security frameworks (ISF) have been created to assist organizations, and other frameworks evolved to update this domain practices. Recently, the European Union decided to create the General Data Protection Regulation (GDPR), applicable to all organizations dealing with personal data of citizens residing in the European Union. Although considered a general regulation, GDPR implementation needs to align with some industries laws and policies. Specially in banking industry. How these ISF can assist the implementation of GDPR is not clear.

Design/methodology/approach – Design Science Research process was followed, and semi-structured interviews performed.

Findings – A list of practices to assist banking industry in GDPR implementation is provided. How each practice map with assessed ISF and GDPR requirements is also presented.

Research limitations/implications – Since GDPR is a relatively recent subject, it is hard to find experts in the area. It is more difficult if we intend to find experienced people in GDPR and banking industry. That is one of the main reasons this study do not include more interviews.

Originality/value –This research provides a novel artefact to the body of knowledge. The proposed artefact lists which ISF practices banks should implement to comply with GDPR. By doing it our artefact provides a centralized view about which ISF frameworks (or part of them) could be implemented to help banks comply with GDPR.

Keywords General Data Protection Regulation, GDPR, Data Protection, Information Security, Frameworks.

1.Introduction

The rapid development of computers in the last 20 years, with the reduced prices for data storage, allows the processing of large amounts of personal data (PD) (Martin, Matt, Niebel, & Blind, 2019; Radvanovsky & Brodsky, 2013). Plus, with the large volume of PD collected, companies are facing serious vulnerabilities, like the misuse, that could result in privacy breaches (Agarwal, 2016).

The roles between governments, data subject (DS) rights, and data protections authorities (DPA) are different across the countries, due to significant levels of enforcement and legal competencies (Custers, Dechesne, Sears, Tani, & van der Hof, 2018). Therefore, The European Union (EU) published their own directive for data protection (DP), since the adoption in 1995, the Data Protection Directive 95/46/EC (Council, 1995) has been the central legislative for PD privacy instrument in the EU (Tikkinen-Piri, Rohunen, & Markkula, 2018). Considering this is not a regulation, all member states must translate it into local laws, which makes a non-uniformization of the laws across EU.

Since its inception, DP has, in turn, been driven by the development of information technology (IT) (Phillips, 2018), and in the last years with the increase use of IT by the citizens, in particularly the residents in EU, the Data Protection Directive 95/46/EC no longer meets the privacy requirements of the present-day digital environment. To solve this problem the European Commission (EC) has been developing, since 2009, the General Data Protection Regulation (GDPR), that has published a proposal for the DP reform in 2012 (Tikkinen-Piri et al., 2018).

In May 2018, the GDPR came into effect to replace the Data Protection Directive 95/46/EC, to meet current challenges related to personal DP and to harmonise DP across the EU (Tikkinen-Piri et al., 2018).

One major difference from the old directive is, that GDPR is a regulation and not a directive. This means that it will apply directly in all member states without them translating it into local laws. One of the main objectives of GDPR is to lead to consistency of DP in EU and this justifies the transition from a Directive to Regulation (Malatras et al., 2017; Randolph, 2020).

The regulation challenge the way that companies process data, where our data is a product companies trade and sell (Krempel & Beyerer, 2018). Therefore, since every industry has their own specifications (for instance, financial services or healthcare), and since GDPR is not regulated by a specific sector, it requires significant time effort to understand the specific requirements of each industry (Díaz Díaz, García-Ramos, & García Olalla, 2020; Lopes, Guarda, & Oliveira, 2020; Martin et al., 2019).

The creation of digital single market in EU has motivated that digital economy in EU has become increasingly reliant on the control and processing of PD. This progression creates enormous opportunities for business, but in another way leaves open serious issues like the implementation of new technologies, and the increasing public awareness and concern for the importance of personal DP (Lucic, Boban, & Mileta, 2018), and generate serious privacy, trust and security risks (Almeida Teixeira, Mira da Silva, & Pereira, 2019). To answer these challenges nowadays exists in the market a set of information security frameworks (ISF) to improve the organizations security (Srinivas, Das, & Kumar, 2019).

The lack of trust can reduce the development, use and adoption of new technologies (Radvanovsky & Brodsky, 2013), and many new business opportunities may be missed if appropriate DP practices are not implemented (Ayala-Rivera & Pasquale, 2018). So the GDPR came to bring and benefit companies by offering DP practices across the EU member states and others that deal with PD of EU citizens and by enabling more integrated EU DP policies (Tikkinen-Piri et al., 2018), moreover the adoption of the requirements in addition to ensuring compliance with the GDPR also brings competitive advantage to the companies.

The GDPR aims to meet the current challenges related to PD, consolidate online privacy rights and improvement Europe digital economy, and provide individuals with better capabilities for controlling and managing their PD (Mantelero, 2013; Randolph, 2020), hence striving to reinforce the DS trust in PD collecting companies. Within the new DP framework, individual

service users may also benefit from the free movement of data if it results in growing businesses with improved and personalised services (Ayala-Rivera & Pasquale, 2018).
Banking industry is one of the most regulated industries in the world, mainly because the giant reserves of rich data and its large scope for ambitious hackers, the DS expect their PD to be secure and protected by the most robust processes and technologies. It means that information security (IS) must be a priority throughout this industry to ensure that all transactional processes are efficient, reliable, secure and compliant (Sydekum & Networks, 2018).
Based on this information and since organizations need to rearrange their own processes and technologies to be compliant with GDPR, especially a set of critical sectors, this research focuses on banking industry. Therefore, this research aims to investigate how can current ISF help banks comply with GDPR.

2.GDPR

The GDPR was designed to harmonize DP laws across Europe in order to give greater protection and capabilities to individuals for controlling their PD in the face of new technological developments. Plus, GDPR applies to all the organizations that handle PD about EU residents, regardless of their physical locations (Ayala-Rivera & Pasquale, 2018; Cardoso-Cachopo & Oliveira, 2003).
GDPR comes with two new elements never seen before in DP. First, DP is mandatory, and fines are huge. Infringements are fined up to 20 million € or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The second part is called territorial scope. The regulation does not only apply to EU companies but to every company selling into the EU or marketing to EU citizens (Krempel & Beyerer, 2018), this means that applies to companies outside the EU, not just because they have a website accessible to a citizen in the EU, but because compliance is required when offering of goods or services to DS.
This regulation has four major focus points: accountability, transparency, protection and reliability. GDPR brings an onus to collect PD for specific purpose only, to uphold the trust of the person who gives their PD, to maintain and protect the information and to erase it when no longer required. PD and the special category personal data (SCPD) should be protected and EU is safeguarding the economic value of digitally kept information of citizens through GDPR. In the wrong hands an amalgamation of multiple data points from the same individual potentially leads to identity frauds (Philip, 2019).
Moreover, although some of the GDPR obligations were already specified in the Data Protection Directive 95/46/EC, these have mainly been perceived as “recommendations”. Therefore, most organizations have only started recently to implement measures to comply with the GDPR (Ayala-Rivera & Pasquale, 2018).
So, the major challenge related to a solid implementation of the GDPR is the organizations lack awareness and understanding of the forthcoming changes and requirements that the GDPR enforces through its new rules. These requirements have various practical implications for organisational design of systems, practices and processes, as well as personnel training (awareness) and assignment of new responsibilities in the organisations (accountability). In short, it brings out the need to review the current DPR practices, technological DP measures and IS measures, as well as possibly plan new ones to ensure compliance with the GDPR (Ayala-Rivera & Pasquale, 2018). Additionally frequency in communication between IS and privacy teams is considered crucial for effective overall enterprise cybersecurity (Heimes, 2016).

3. Related Work

This section aims to explore what the scientific community has been studying regarding the application of ISF in the GDPR domain or GDPR implementation.

Table 1 presents seven relevant documents were found relating this research topics. From this universe, only two explore the implications during the implementation of GDPR and four explore the use of ISF.

Table 1 – Related Work

ID	Author	Title	ISF?	Industry
RS.1	*Tankard & Pathways (2016)*	*What the GDPR means for businesses*	*ISO27001*	*Generic*
RS.2	*Teixeira et al.* (Almeida Teixeira et al., 2019)	*The Critical Success Factors of GDPR Implementation: a Systematic Literature Review*	*ISO27001*	*Generic*
RS.3	*Freitas & Mira (2018)*	*GDPR Compliance in SMEs: There is much to be done*	*-*	*Industrial SME*
RS.4	*Krystlik (2018)*	*With GDPR, preparation is everything*	*-*	*Generic*
RS.5	*Wilson (2018)*	*A framework for security technology cohesion in the era of the GDPR*	*-*	*Generic*
RS.6	*Lopes, Guarda, & Oliveira (2019)*	*How ISO 27001 can help achieve GDPR compliance*	*ISO27001*	*Generic*
RS.7	*Centro Nacional de Cibersegurança (2019)*	*Quadro Nacional De Referência para a Cibersegurança*	*ISO27001&COBIT*	*Generic*

Overall, the related articles mention the difficulties about implementing GDPR and the lack of awareness among companies. This happen because GDPR is a recent subject and concrete measures are not mentioned, appealing for implementing the requirements according to the level of risk that they have, for all the industries managing PD.

Plus, four studies argue that ISF (ISO 27001 or COBIT) may help organizations achieving the level of compliance desired by GDPR, since the ISF is not new and offers more concrete guidelines for implementing IS measures, reducing the risk of data breaches. However, none of these studies provide insights on how these ISF can do it.

As one can see in

Table 1, there is no related work investigating how can ISF help in GDPR compliance. Moreover, the few existent researches focus on the preparation without using ISF and are generic to all industries.

To sum up, there is studies pointing ISF as useful to help companies comply with GDPR, but no studies provide practical insights on how that can be done. Neither to the banking industry.

As one of the most regulated industries, Banking industry face several legal aspects to manage and protect their clients data (Betron, 2012; Irwin, 2018). With the appearance of GDPR Banks have now more compliance challenges to hold when using clients data and legal aspects to deal with in most phases of the personal data handling process (Gruschka, Mavroeidis, Vishi, & Jensen, 2019). The authors expect to collect some qualitative information about legal aspects/implications of GDPR adoption in banking industry along the research, but it is not the focus of the investigation. Instead, this research is broader in its nature and insights from several aspects are expected.

Therefore, this research intends to contribute with novel insights on how ISF can assist banks in GDPR adoption and compliance.

4. Research Methodology

This research applies the design science research (DSR) in order to design, build and evaluate how can current ISF help banks comply with GDPR. Since this research purposes to expand the limits of human capacities and organizations, to create the artefacts invoking the Design Science Research Methodology (DSRM) is the right choice (Hevner, March, Park, & Ram, 2004)(Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). Figure 1 presents the DSR process applied in this research.

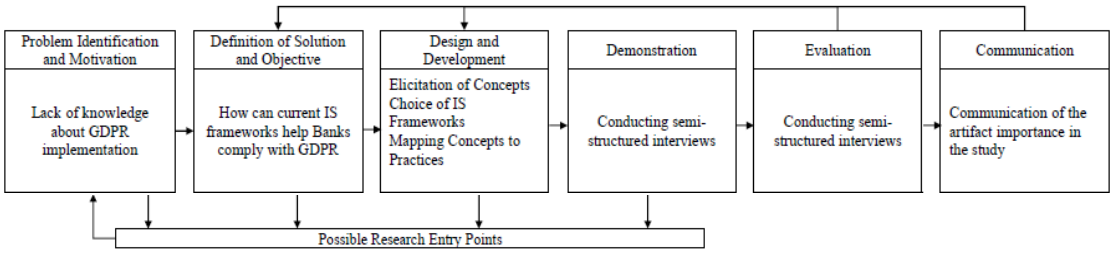
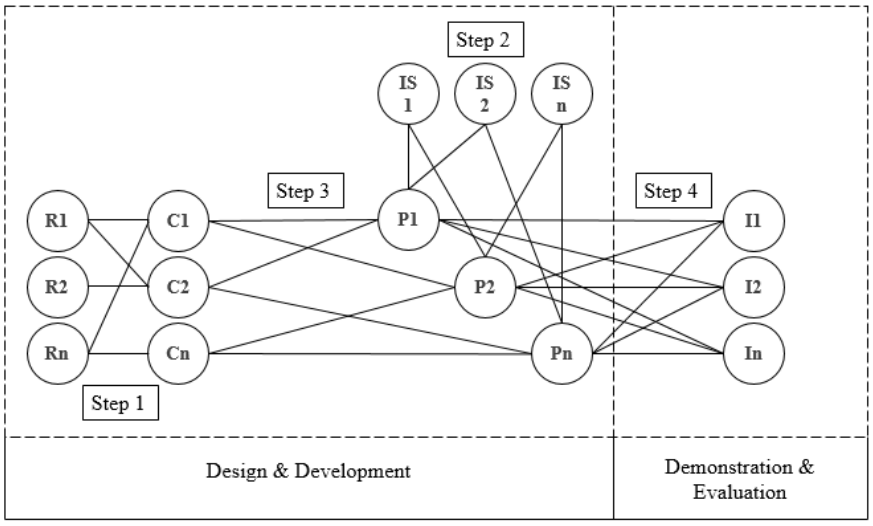


Figure 1 – DRS Process Model

The first two activities of this process have already been mentioned, in the respective chapters. In the design and development activity, is where all the design of the proposed artefact is performed. The demonstration and evaluation phase are where the authors prove that the artefact can be used in practice and where its validity is assured. By conducting semi-structured interviews, a validation of the work developed is done, as well as the demonstration that it can be applied in the banking industry, by collecting the practices proposed in the research and already used by the interviewees. The interviewees are experienced professionals in the areas of DP or IS and all of them work in the banking industry. Finally, in the communication, the authors submit the main findings to respectful journals of the area.

5. Design

This research aims to investigate how can ISF assist GDPR compliance in the banking industry. To pursue our goal and design the artefact, the authors have performed a set of steps. Figure 2 synthesizes the Design of the proposed artefact. Four steps were performed sequentially. The final step was used to demonstrate and evaluate the proposed artefact.



R – Requirement (Requirements from the GDPR, i.e., the articles); **C** – Concept (Concepts extracted from the requirements); **IS** - Information Security Frameworks (ISF that exists in the market); **P** – Practices (Practices or controls from the ISF); **I** – Interview (Presential interviews to obtain qualitative data to the research)

Figure 2 –Diagram of the Design

5.1 Step 1 – Elicitation of the List of Concepts

The first part of the design consisted in reading all the GDPR regulation (11 chapters and 99 articles) and from each of them extracting concepts that are related to the security of data, DP and rights of DS. It must be noted that articles related to DPA obligations, such as for example investigations carried out to data breaches, penalties that could be applied to organizations, etc, were not considered.

5.2 Step 2 – Choice of IS Frameworks

Several ISF exist, that despite not mandatory some could be certified to attest the compliance of the organizations with IS requirements. These frameworks offer a solid base to start implementing IS in the organizations, offering structures and practices not present in GDPR.

5.3 Step 3 – Mapping Concepts with Framework Practices

After complete Step 1 and Step 2 it was time to map the concepts with each ISF. For each elicited concept, one or more practices from the frameworks were selected when met the requirement of the concept. For each concept, that GDPR do not give any specific instruction on how to implement it, the authors sought for practices in ISF that could provide more precise instructions in order to achieve the appropriate level of compliance.

5.4 Step 4 - Conducting Semi-structured Interviews

This step aimed to demonstrate and evaluate the applicability of the artefact with experts in the area, i.e. that have experience in the banking industry and in GDPR. Therefore, the qualitative method interview was chosen to elicit qualitative information on the subject.

The goal of interviews is to collect data that cannot be obtained using quantitative methods, interviewing people that gives insight into the subject studied and their opinion (Hove & Anda, 2005).

Several types of interviews exist like structured interviews, semi-structured interviews and non-structured interviews (Seaman, 1999). This research used individual semi-structured interviews to obtain more information and validate the practices that are applied in the banking industry, the questions are open-ended, asking other information when necessary.

6. Development

The design of the artefact is described in the previous section. This section details each of the steps presented so the reader can better understand what and how the steps were performed.

6.1 Step 1 – Elicitation of the List of Concepts

The first part of the artefact consists in extracting from the GDPR articles/requirements all the concepts that are related to the security of data, DP and rights of DS. For instance, in Figure 3 one can see the following concepts: Lawfulness, Fairness and Transparency, Purpose Limitation, etc (EU Data Protection Regulation, 2016).

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

Figure 3 – Example of elicited concepts from article 5
Adapted from EU Data Protection Regulation (2016)

It should be noted that both the same concept can be elicited from more than one article and one article could have more than one concept.

Table 2 – Chapters of GDPR

Chapters with Concepts	Principles; Rights of the data subject; Controller and processor; Transfers of personal data to third countries or international organisations;
Chapters without Concepts	General provisions; Independent supervisory authorities; Cooperation and consistency; Remedies, liability and penalties; Provisions relating to specific processing situations; Delegated acts and implementing acts; Final provisions;

At the end of this step, 37 concepts were extracted from the 11 chapters (Table 2) and 99 articles that compose the GDPR. Some chapters were not considered since are not related to DPA obligations (for example, independent supervisory authorities or penalties that could be applied to the organizations and other subjects) and therefore are not directly related to the mandatory requirements of the organizations. Table 3 exemplifies a set of concepts collected from the article 5 (Figure 2).

Table 3 – Example of extracted concepts from GDPR

Concepts
Lawfulness, fairness and transparency
Data Minimisation
Inaccurate Data
Storage Limitation
….

6.2 Step 2 – Selected IS Frameworks

From the list of ISF existent in the market, the following four frameworks were chosen to ground the remaining steps of the research: ISO/IEC 27001:2013 (ISO/IEC, 2013), ISO 27552 (ISO/IEC DIS 27552, 2019), NIST SP 800-53 rev.4 (NIST, 2013) and COBIT 2019 Framework (COBIT, 2019).
ISO/IEC 27001:2013 appears to be the most used in the Europe by professionals and NIST SP 800-53 in the United States. COBIT is reference in IT Governance and was recently updated (2019). For last, ISO 27552 is a new framework, that is an extension of the ISO/IEC 27001:2013 and address the DPR and in especial the GDPR requirements.
Along this document the practices are the controls from ISO 27001, NIST SP 800-53 and ISO 27552 or the activities from COBIT.

6.3 Step 3 – Mapping Concepts with Framework Practices

In this step, individually, for each of the identified concepts, was performed a research of the practices presented in every ISF, in order to check if the practice can fulfil the level of compliance. The goal is from each of the concept, that do not give any specific instruction to implement them, find practices that give more precise instructions and can be applied to the banking industry to achieve the level of compliance. In case the practice fulfils the requirement of the concept, then it would add to the list.
Some practices were used more than one time because they can be used to comply with more than one concept, and as we will see in the next section, some may not be the indicated for the concept or may not be applied in the banking industry.
Not all the concepts could be mapped with at least one practice from each framework, since there are some subjects that the frameworks do not cover at 100 percent, such as for example the concept "Lawfulness, fairness and transparency", in the Table 4, that is not covered by the ISO/IEC 27001:2013.

Table 4 – Example of a concept with the practices

Article	Paragraph/ Line	Concept	ISO 27552	ISO 27001 :2013	COBIT 2019	NIST SP 800-53 v4
5	*1-A*	*Lawfulness, fairness and transparency*	*7.2.2-Identify lawful basis 8.2.2-Organization's purposes*	-	*EDM05.02-Direct stakeholder engagement, communication and reporting*	*AP-2-Purpose Specification*

Demonstration and Evaluation

After the development of the artefact, the authors searched for experts in banking industry and GDPR available to be interviewed. To choose the experts, first the authors looked to their personal contact list and then in the LinkedIn professional network. Overall, 17 experts and 11 banks were invited to participate in the study. At the end, a total of seven experts from six banks accepted to be interviewed. The interviews were conducted in person on the headquarters of six Portuguese banks, with a total of seven interviewees, from different departments, responsibilities and years of experience. All the selected interviewees have both knowledge in GDPR, DP and IS.
The requirements to participate in the study were:

- The expert should have participated in at least one GDPR project;
- The expert has professional experience in IS and/or DP.

The goal of the interviews is to demonstrate and evaluate the developed artefact. To conduct the interviews, a questionnaire was developed with the following structure. First, the header of

the questionnaire is composed by generic questions (Table 5), to certify the experience of the interviewee in the banking industry and GDPR. Then, a set of questions about the interviewee's organization was presented.
For each practice mapped to a concept, one question was formulated, to understand if the practice fulfils de concept, always in the banking industry. In each of these questions the interviewee could choose one of the following: Not Applicable (N/A), Partially Compliant (PC), Fully Compliant (FC).

Table 5 – Interviewee specific questions

Interviewee	
Years of experience	
Current Job Role	
Years of experience in banking industry	
What are your responsibilities?	
Months of experience in GDPR	
How many GDPR projects have you been involved	
Classify how much are you familiar with GDPR?	☐Excellent ☐Very Good ☐Good ☐Fair ☐Poor
Point out which of the following frameworks that you have experience	☐ISO 27001 ☐ISO 31000 ☐ISO 38500 ☐ISO 22301 ☐NIST SP 800-53 ☐COBIT ☐Other: _____

Then, the interviewees were asked if each of the elicited practices was being implemented at their organization (bank), with the following options: In Implementation (II), Implemented (I).
Plus, the analysed frameworks were not revealed to the interviewees until the end of the interview to avoid bias answers.

Table 6 lists an example of the first concept and mapped practices with the possible questions to be answered by the interviewees. In addition to these questions and when possible, additional information (qualitative) was gathered about the concepts and practices in the banking industry, as well as feedback about the implementation of the practices.

Table 6 – Concepts and practices question

Concepts and Practices	Level of Compliance				
Lawfulness, fairness and transparency	N/A	PC	FC	II	I
• Identify lawful basis					
• Organization's purposes					
• Direct stakeholder engagement, communication and reporting					
• Purpose Specification					

At the end of the interview (

Table 7), each interviewee was asked: if the listed concepts and practices were enough to a bank to comply with GDPR; if the implementation effort would be smaller; and if the interview was useful to increase their knowledge.

Table 7 – Last notes

Last notes	
In your experience, with these practices do you think that a company can be compliant with GDPR?	☐Yes ☐No
If not, what do you think is missing?	
With these practices, do you think that the effort of implementing GDPR can be less, comparatively to implement the GDPR without these guidelines?	☐Yes ☐No
Do you think this interview is useful?	☐Yes ☐No

In Table 8 it is possible to see an overview of interviewees, as well as their knowledge in GDPR and frameworks. Regarding the evaluation made by the interviewees about their knowledge of GDPR, it is normal to have dissonances between the experience (months) and the given evaluation, as it will depend on the feeling of each one and the degree of involvement of them in the projects, during this period of months.

Table 8 – Interviewees comparation

Interview	Years of Experience	Role	Years of experience in banking industry	Months experience in GDPR	Number of GDPR projects	How much are familiar with GDPR (*)	Frameworks in which they have experience	Interview duration
I.1	*8*	*IT Auditor*	*8*	*12*	*1*	*Good*	*ISO27001;ISO31000; ISO22301;COBIT;NIST Cybersecurity Framework*	*1:30*
I.2	*13*	*IT Auditor*	*13*	*12*	*1*	*Good*	*ISO27001;NIST SP 800-53;COBIT;ITIL*	*1:00*
I.3	*15*	*Senior Manager of IS/IT*	*12*	*26*	*2*	*Very Good*	*ISO27001;ISO31000; ISO22301*	*1:30*
I.4	*14*	*DPO*	*12*	*10*	*1*	*Very Good*	*ISO27001;COBIT*	*1:30*
I.5	*25*	*CISO*	*19*	*30*	*2*	*Good*	*ISO27001;ISO31000; ISO38500;ISO22301; COBIT;ISO20000; ISO9001;ISO14000*	*2:00*
I.6	*26*	*DPO*	*26*	*30*	*1*	*Very Good*	*ISO 27001;NIST SP 800-53;ISO 27005*	*2:00*
I.7	*33*	*Responsible of Risk and Security of IS/IT*	*30*	*30*	*1*	*Good*	*ISO27001;ISO22301; COBIT*	*2:30*

*Scale = Excellent; Very Good; Good; Fair; Poor;

From the banks that participated in this study, half have more than 500 employees, as shown in Figure 4. Plus, all banks are present in Portugal and four of them have international presence.

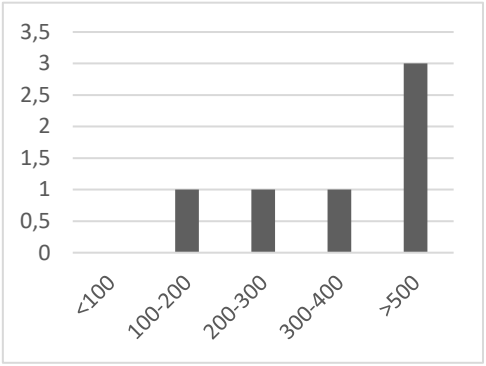


Figure 4 – Number of employees

The interviewees said that all the banks follow/perform a framework or best practice. The most used framework among the interviewed banks is ISO 27001, with the justification that is the ISF of reference in Europe. The second most used framework is COBIT, related to IT governance and IS, this framework is widely used by IT auditors as a reference for the processes to be audited in the banking industry.
Figure 5 shows the distribution of used frameworks in the banks. This list is not restricted only to ISF.

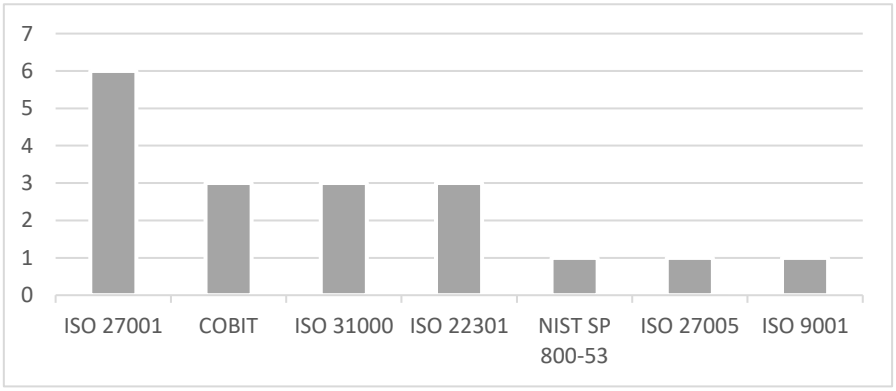


Figure 5 – Frameworks followed/performed in the banks

As can be seen, most of the banks are of a considerable size, with a strong international presence, which requires compliance with more laws than those required in Portugal. Plus, all the banks already follow at least one ISF. For instance, ISO 27001 is followed (partly) by all the interviewed banks. Moreover, there is a strong concern in this industry to compliance with this type of laws, in order to avoid reputational damage.
All the interviewees agreed that all the presented concepts are correct, and no further concepts were proposed as missing. Interviewees also agreed that all concepts are required to be in place. However, interviewees argued that some exceptions exist for this industry since GDPR sometimes overlap other existing laws of the sector.
At the end of each interview a set of questions were performed so interviewees could assess the content and usefulness of the proposal.
As can be seen in Table 9, all the interviewees considered that they can be compliant with these practices. Regarding the effort required to implement GDPR, all interviewees said that the effort decrease, except for one interviewee, arguing that it will always depend on the approach of each bank, and if there is no ISF already to be followed, the effort would be the same. The usefulness of the proposal was validated by all the interviewees.

Table 9 – Final set of questions

	Can you be compliant with these practices?	Would the effort of GDPR implementation decrease by implementing these practices?	Is this research useful?
I.1	*Yes*	*Yes*	*Yes*
I.2	*Yes*	*Yes*	*Yes*
I.3	*Yes*	*Yes*	*Yes*
I.4	*Yes*	*No*	*Yes*
I.5	*Yes*	*Yes*	*Yes*
I.6	*Yes*	*Yes*	*Yes*
I.11	*Yes*	*Yes*	*Yes*

Analysis and discussion of results

Due to the existence of different answers to the same question, this section discusses and analyses our results.

Analysis of the results

In order to separate practices into three groups (Not Applicable, Partially Compliance and Fully Compliance), a formula was created to obtain a score per practice, with the following assumptions:

- Score of each practice = (Sum of answers with N/A * 0) + (Sum of answer with PC * 1) + (Sum of answers with FC * 2)
- N/A = 0
- PC = 1
- FC = 2

For example, in Figure 6, the practice "Identity lawful basis", have 12 on score, based on this calculation (0*0) + (2*1) + (5*2) = 12.

Framework	Concepts and Practices	Level of Compliance					Score
	Lawfulness, fairness and transparency	N/A	PC	FC	II	I	
ISO 27552	Identify lawful basis		2	5	1	5	12
ISO 27552	Organization's purposes		4	3		6	10
COBIT 2019	Direct stakeholder engagement, communication and reporting		4	3	6		10
NIST SP 800-53 Rev.4	Purpose Specification		3	4	1	5	11

Figure 6 – Concept and Practices with score

To differentiate the practices that are fully compliant with the concept, partially compliant or not applicable, a range of values was created, as can be seen in Table 10 based on the score formula.

Table 10 – Score Matrix

Level of Compliance	Score range	Color
N/A – Not Applicable	*0 – 7.99*	
PC – Partially Compliance	*8 – 11.99*	
FC – Fully Compliance	*12 – 14*	

After applying the previous formula in all practices, 13 out of 37 concepts have practices that are fully compliant. This means that 35% of the concepts have at least one practice that address the entire concept in the banking industry. Table 11 lists the concepts that have at least one practice that fulfil all the requirement, with the related practice(s).

Table 11 – Concepts with practices fully compliant

Concept	Practice
Lawfulness, fairness and transparency	*Identify lawful basis*
Storage Limitation	*Support data archiving and retention*
	Data Retention and Disposal
Accountability	*Policies for information security*
	Information security roles and responsibilities
Right of access by the data subject	*Individual Access*
Right to rectification	*Access, correction and/or erasure*
	Evaluate and update or retire information
Notification obligation regarding rectification or erasure of personal data or restriction of processing	*PII controllers' obligations and third parties*
Right to data portability	*Providing copy of PII processed*
Right to object	*Provide mechanism to object to PII processing*
Notification of a personal data breach to the supervisory authority	*Responsibilities and procedures*
Data Protection Impact Assessment	*Privacy impact assessment*
Designation of the data protection officer	*Acquire and maintain adequate and appropriate staffing*
	Governance and Privacy Program
Tasks of the data protection officer	*Establish roles and responsibilities*
	Governance and Privacy Program
General principle for transfers	*Information Sharing with Third Parties*

On the Table 12 there are the concepts that have practices with less or equal seven in their score. The information gathered during the interviews was enough to justify this low score, and most of it is due to the specifications of the industry. The next section presents the discussion and findings.

Discussion on Findings

For the “Security of Personal Data” and “Security of Processing” concept, the opinion is that none of the existing practices is 100% compliant. However, the presented set of practices are the required to be compliant in the banking industry.
Regarding the concept “Storage Limitation”, six of the interviewees agreed that is very difficult to implement due to the existence of old systems and many dependencies between them. Plus,

this inhibits the banks to delete the information after the retention period, the solution is rebuilding the systems/applications, which are currently developed in technologies already obsolete.
Regarding "data portability", all the interviewees agreed that despite having the fully compliant practice, it is urgent to create a form for data portability between banks, like what is already widely used in telecommunications companies. For instance, to transfer data to third parties, bank may be required to transfer PD to other countries and must comply with Foreign Account Tax Compliance Act (FATCA), which requires the sending of PD about the US citizens.
All practices that refer to automated decisions have a low score, because in the banking industry there are no automated decisions, there is some process automation that is evolving fast (Santos, Pereira, & Vasconcelos, 2019), but the final decision is made by humans. For example, it is impossible to automatically decide if a mortgage loan can be decided based only in automated decision (at this moment).
Regarding the concept "Information to be provided where PD have not been obtained from the data subject", unlike other industries, when banks collect data, they can only obtain them from their regulator, for effects of money laundering and terrorist financing or other debtors blacklist. In this case the DS cannot ask for rectification or erasure because there are other laws/regulations that overlap the GDPR. If this information is incorrect, the DS must prove the home institution, responsible for the incorrect data, and never directly to the bank.
The practice "Review effectiveness of business process controls" is not necessary because it is very abstract and redundant, as there are more complete practices outlined for the concept.
The practices of the concept "Communication of a personal data breach to the data subject" had a low score because they are not in the context of this concept. In reporting the incident to the DS it is not necessary to say what is being done to mitigate the problem, only to the regulator.

Table 12 – Concepts with practices not applicable

Concept	**Practice**
Information to be provided where personal data are collected from the data subject	*Automated decision making*
Information to be provided where personal data have not been obtained from the data subject	*Provide mechanism to modify or withdraw consent* *Provide mechanism to object to processing* *Providing copy of PII processed* *Automated decision making* *System of Records Notices and Privacy Act Statements*
Right of access by the data subject	*Automated decision making* *Identify basis for international PII transfer* *Direct stakeholder engagement, communication and reporting*
Right to object	*Providing information to PII principals*
Automated individual decision-making, including profiling	*Establish data profiling methodologies, processes and tools* *Data Mining Protection*
Regularly Testing, Assessing and Evaluating	*Review effectiveness of business process controls*
Communication of a personal data breach to the data subject	*Response to information security incidents* *Define classification schemes for incidents and service requests*

As can be seen in Table 13, the average practices score per concept points that most of them are in the partially compliance range. This is in line with interviewees comments, who said that

in banking industry most practices complement each other to comply with the concept. The overall average of the concepts is 9.7, which is among the "partially compliance" range. There are 2 concepts that have a score below 8. As explained earlier most of the practices do not apply in banking industry, although the concepts are necessary. These results reinforce interviewee's comments regarding the practices, with the exception of those removed (Table 12), that complement each other thus obtaining a list of good practices from the main ISF that help in GDPR implementation.

Table 13 – Practice score level per concept

Concept	**Practice score level**
Lawfulness, fairness and transparency	*10.75*
Data Minimisation	*10*
Inaccurate Data	*9,8*
Storage Limitation	*11*
Security of Personal Data	*9,46*
Accountability	*9,92*
Transparent information, communication and modalities for the exercise of the rights of the data subject	*10,16*
Information to be provided where personal data are collected from the data subject	*9,11*
Information to be provided where personal data have not been obtained from the data subject	*7,22*
Right of access by the data subject	*9*
Right to rectification	*11,33*
Right to erasure ('right to be forgotten')	*8,75*
Right to restriction of processing	*10,4*
Notification obligation regarding rectification or erasure of personal data or restriction of processing	*10,5*
Right to data portability	*10*
Right to object	*9,2*
Automated individual decision-making, including profiling	*7,75*
Data Protection Policies	*10*
Codes of Conduct	*10,2*
Data Protection by Design	*9,12*
Data Protection by Default	*9*
Processor	*9,6*
Records of Processing Activities	*9,69*
Security of processing	*9,7*
Pseudonymisation	*9,14*
Encryption of Personal Data	*9,42*
Confidentiality, Integrity, Availability and Resilience	*10,11*
Restore the Availability	*10,25*
Regularly Testing, Assessing and Evaluating	*8,71*
Approved Certification	*9*
Notification of a personal data breach to the supervisory authority	*10,71*
Communication of a personal data breach to the data subject	*8,85*
Data Protection Impact Assessment	*9,87*
Designation of the data protection officer	*11,5*
Tasks of the data protection officer	*11*
Certification	*8,5*
General principle for transfers	*10,66*

Conclusion

This research aimed to explore how can current ISF help banks comply with GDPR. The main GDPR concepts (requirements) on this field were elicited and then mapped with the practices of the chosen ISF. Forwardly, semi-structured interviews were conducted with experts working in the banking industry.

At the end, several conclusions can be withdrawn about the specificities of the banking industry, ISF and the GDPR implementation. According to our findings, one may argue that an ISF is a good starting point to implement GDPR and get more specific instructions, on how to implement controls to mitigate the IS and DP risk that the organizations are exposed.

In terms of particularities in the banking industry, the main findings are:

- When PD have not been obtained from the DS, the DS cannot deny the consent;
- There are not completely automated decisions;
- Storage limitation is very difficult to implement, even though is mandatory and applicable in this industry;
- There is no template for data portability between banks;
- Other laws can overlap GDPR, like FATCA, money laundering and terrorist financing, etc;
- With the use of ISF the banks can develop certifications of compliance, for example if they implement the entire controls of ISO 27001, because the GDPR expressly provides that adherence to approved certifications to demonstrate compliance.

In general, the interviewees are satisfied with the proposal due to the ability to improve the GDPR implementation and reduce the level of effort. Plus, with these practices they can have a more solid view of what to do, to comply with GDPR.

Plus, there is not a single ISF that has practices for all concepts. This is due to several factors such as:

- Only ISO 27552 has been developed to comply with GDPR;
- The NIST SP 800-53 is very technical and oriented to IS and DP;
- ISO 27001 was last updated in 2013, when DP was not yet a hot topic;
- COBIT is very focused on governance and management of IT, although it was updated in 2019 and added new controls to IS.

However, the ISF used in this research complement each other. Considering this research goal one may argue that it is possible for an ISF assist in the implementation of GDPR, achieving the compliance and thereby decrease the level of effort required.

In conclusion, the research question, “How can current ISF help banks comply with GDPR” was answered positively, even if more than one ISF may be required.

This research took contributions by exploring an area that was not proper explored, improving the body of knowledge on how can banks implement GDPR using ISF.

Some limitations exist. This research grounds its demonstration and evaluation on the knowledge of the interviewees and their organization context. Moreover, the interviewees were performed with experts that work in Portugal. More interviews should be performed in the future. This would also be interesting with interviewees from other countries. Despite being a rigid industry, regional and cultural differences may influence the implementation of these domains (Pereira & da Silva, 2012). Plus, legal aspects and implications of GDPR adoption deserve to be further investigated in such a critical industry. Other techniques (Case Study, Delphi, survey, etc) can also be used to cross results and find new insights.

References

Agarwal, S. (2016). Towards dealing with GDPR uncertainty. In *11th IFIP Summer School on Privacy and Identity Management* (pp. 1–7). Karlstad, Sweden.

Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance* . https://doi.org/10.1108/DPRG-01-2019-0007

Ayala-Rivera, V., & Pasquale, L. (2018). The grace period has ended: An approach to operationalize GDPR requirements. In *Proceedings - 2018 IEEE 26th International Requirements Engineering Conference, RE 2018*. https://doi.org/10.1109/RE.2018.00023

Betron, M. (2012). The state of anti-fraud and AML measures in the banking industry. *Computer Fraud & Security*, *2012*(5), 5–7. https://doi.org/https://doi.org/10.1016/S1361-3723(12)70039-8

Cardoso-Cachopo, A., & Oliveira, A. L. (2003). An Empirical Comparison of Text Categorization Methods. In *Proceedings of SPIRE-03, 10th International Symposium on String Processing and Information Retrieval* (pp. 183–196). https://doi.org/10.1007/b14038

COBIT. (2019). *Governance and Management*. *Governance and Management Objectives*. https://doi.org/10.1201/b13869-7

Council, O. F. T. H. E. (1995). DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995, (L).

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2017.09.001

Díaz Díaz, B., García-Ramos, R., & García Olalla, M. (2020). Does regulating remuneration affect the market value of European Union banks? Large versus small/medium sized banks. *Regulation & Governance*, *14*(1), 150–164. https://doi.org/10.1111/rego.12175

EU Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Freitas, M. da C., & Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*. https://doi.org/10.20897/jisem/3941

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2019). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. In *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*. https://doi.org/10.1109/BigData.2018.8622621

Heimes, R. (2016). Global InfoSec and Breach Standards. *IEEE Security and Privacy*. https://doi.org/10.1109/MSP.2016.90

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

https://doi.org/10.2307/25148625

Hove, S. E., & Anda, B. (2005). Experiences from conducting semi-structured interviews in empirical software engineering research. In *Proceedings - International Software Metrics Symposium*. https://doi.org/10.1109/METRICS.2005.24

Irwin, L. (2018). How banks should prepare for the GDPR. Retrieved April 9, 2020, from https://www.itgovernance.eu/blog/en/how-banks-should-prepare-for-the-gdpr

ISO/IEC DIS 27552. (2019). DRAFT INTERNATIONAL STANDARD ISO / IEC DIS 27552 Security techniques — Extension to ISO / IEC 27001 and ISO / IEC 27002 for privacy information management — Requirements and guidelines, *2018*.

ISO/IEC, I. O. for S. E. C. (2013). Iso/Iec 27001: 2013. *Information Technology Standard*.

Krempel, E., & Beyerer, J. (2018). The EU general data protection regulation and its effects on designing assistive environments. In *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3197768.3201567

Krystlik, J. (2018). With GDPR , preparation is everything. *Computer Fraud & Security Bulletin*, *2017*(6), 5–8. https://doi.org/10.1016/S1361-3723(17)30050-7

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. In *Iberian Conference on Information Systems and Technologies, CISTI*. https://doi.org/10.23919/CISTI.2019.8760937

Lopes, I. M., Guarda, T., & Oliveira, P. (2020). General Data Protection Regulation in Health Clinics. *Journal of Medical Systems*, *44*(2), 53. https://doi.org/10.1007/s10916-020-1521-0

Lucic, D., Boban, M., & Mileta, D. (2018). An impact of general data protection regulation on a smart city concept. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings*. https://doi.org/10.23919/MIPRO.2018.8400074

Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., … Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2017.03.013

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2013.03.010

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers*, *21*(6), 1307–1324. https://doi.org/10.1007/s10796-019-09974-2

NIST. (2013). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. *NIST SP-800-53 Ar4*. https://doi.org/10.6028/NIST.SP.800-53Ar4

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). <Design Science Research Methodology 2008.pdf>. *Published in Journal of Management Information Systems*, *24*(3), 45–78. https://doi.org/10.2753/MIS0742-1222240302

Pereira, R., & da Silva, M. (2012). IT Governance Implementation: The Determinant Factors. *Communications of the IBIMA*, 1–16. https://doi.org/10.5171/2012.970363

Philip, R. K. (2019). General Data Protection Regulation (GDPR) and paediatric medical practice in Ireland: a personal reflection. *Irish Journal of Medical Science*. https://doi.org/10.1007/s11845-018-1857-3

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*, *137*(8), 575–582. https://doi.org/10.1007/s00439-018-1919-7

Portugal, C. N. de C. (2019). REFERÊNCIA PARA A, 0–160.

Radvanovsky, R., & Brodsky, J. (2013). *Handbook of SCADA/control systems security*. *Handbook of SCADA/Control Systems Security*. https://doi.org/10.1201/b13869

Randolph, I. (2020). Exploring the ethical implications of business analytics with a business ethics canvas. *European Journal of Operational Research*, *281*(3), 491–501. https://doi.org/10.1016/J.EJOR.2019.04.036

Santos, F., Pereira, R., & Vasconcelos, J. (2019). Toward robotic process automation implementation: an end-to-end perspective. *Business Process Management Journal*, *ahead-of-p*(ahead-of-print). https://doi.org/10.1108/BPMJ-12-2018-0380

Seaman, C. B. (1999). Qualitative Methods in Empirical Studies of Software Engineering, *25*(4), 557–572.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.09.063

Sydekum, R., & Networks, F. (2018). Can consumers bank on financial services being secure with GDPR ?, 11–13. https://doi.org/10.1016/S1361-3723(18)30054-X

Tankard, C., & Pathways, D. (2016). What the GDPR means for. *Network Security*, *2016*(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2017.05.015

Wilson, S. (2018). A framework for security technology cohesion in the era of the GDPR. *Computer Fraud & Security Bulletin*, *2018*(12), 8–11. https://doi.org/10.1016/S1361-3723(18)30119-2