Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model

Completed research paper

A paper presented at ACIS 2020, written by UTS and Data Zoo

Abstract

The protection of information assets requires interdisciplinary approach and cross-functional capabilities. In recent times, information security and privacy compliance continue to be a complicated task due to increasing regulatory restrictions, changing legislations and public awareness. The newly published information security and privacy standard ISO/IEC 27701:2019 provides support for organisations looking to put in place systems to support compliance with global data privacy requirements. However, there is little known about how does this standard map to other regulatory requirements in different jurisdictions specifically the globally relevant General Data Protection Regulation (GDPR). Hence, this research aims to answer an important research question: **whether and how the ISO/IEC 27701:2019 framework represents an opportunity for the GDPR compliance?** This research provides a review and mapping of ISO/IEC 27701:2019 and GDPR by using an integrated requirement engineering model as a kernel theory. The results of this research will assist organisations contemplating to meet their compliance needs. It will also help academics and practitioners interested in integrating the ISO/IEC 27701:2019 and GDPR for developing relevant compliance frameworks and tools.

Keywords: Information Security, Privacy, Compliance, GDPR, ISO27701:2019

Acknowledgements

This research is funded by the Australian Govt. Research Training Program (RTP). Views expressed herein are however not necessarily representative of the views held by the funders. We are also thankful to Data Zoo and team for their continued support for this research.

1. Introduction

Information security is one of the biggest concerns due to increasing attacks on businesses (World Economic Forum 2018) and thus pose a substantial risk to international stability. The security of personally identifiable information (PII) is one of the basic human rights of the information owner. Around the world, laws to protect such rights already exist, or are being implemented and strengthened in an ecosystem where the processing of data is being globalised and concerns about the management of PII is rising. The European Union's GDPR (EU GDPR 2018) is possibly the better-known data protection regulation (Anwar et al. 2018), although, many other countries, such as Korea, the Philippines and China, are also introducing data protection laws. Designing a system to meet with different compliance requirements poses one of the greatest challenges for individuals and organisations operating in a global multi-national environment. How can organisations keep up with the necessary business agility needs and be able to protect themselves at the very same time? Identifying this crucial need for a general set of requirements to manage the security of PII, irrespective of explicit legal or regulatory requirements, the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) developed the recent ISO/IEC 27701:2019 (ISO 2019) standard to offer much needed guidance. ISO/IEC 27701:2019 provides a framework for supporting organisations to establish personal data protection and privacy compliance with multiple legislations in a varying regulatory environment. The differences in data privacy laws across the globe were recognized as barriers to the organisations operating in international market (Bougiakiotis 2019). A universally acceptable GDPR certification (Anwar et al. 2018) around all regions and industry verticals is vital to manage the risk and consequently reduce impediments to trade among business partners. Nevertheless, it is challenging to fulfill GDPR compliance requirements for huge volume of information and provide its end to end traceability. Meanwhile, ISO/IEC 27701:2019 is envisioned to be a ground-breaking standard for privacy so as to ensure that all organisations, small or big, operating in different jurisdictions, and doing business in different industry verticals, can efficiently shield and manage the personal information they hold. The interoperable standard is expected to help organisations in following the path towards GDPR compliance. However, it is unclear whether to implement ISO/IEC27701:2019, GDPR or both for fulfilling global compliance needs.

This research is part of a large action design research (Sein et al. 2011) project, which is focused on adaptive decentralised digital identity ecosystem for our industry partner IDZ (coded name). Due to their international nature of business, a coherent and consistent assurance method is needed to demonstrate that IDZ complies with relevant laws and regulations. Hence, to adapt to an evolving regulatory landscape, IDZ wants to expand their existing ISO 27001 based information security management system (ISMS) by implementing ISO/IEC 27701:2019 based privacy information management system (PIMS). However, before this implementation, IDZ wants to make sure that this move towards information security and privacy will help IDZ in attaining GDPR compliance. Through academic research, it has been found that literature is scarce on information about how ISO/IEC 27701:2019 adheres with most widely accepted privacy and data protection regulations such as GDPR (Anwar et al. 2018). Hence, this research is an effort to fill this small and important gap by analysing the overlaps and gaps of ISO/IEC 27701:2019 and GDPR for developing an integrated set of compliance requirements. The integrated requirement engineering model (Gill and Bunker 2013) is used as a kernel theory to systematically review and map the requirements from ISO/IEC27701:2019 and GDPR. Therefore, this research addresses following research question: **whether and how the ISO/IEC 27701:2019 framework represents an opportunity for the GDPR compliance?**

This paper is structured as follows. Firstly, it discusses the research background and problem. Secondly, it discusses the action design research method. Thirdly it discusses the mapping of ISO/IEC27701:2019 and GDPR using the integrated requirement engineering model. Finally, it discusses results before concluding with options for further research.

2. Background

Several organisations are facing the challenging task of embedding privacy into their policies and procedures to ensure long-term compliance. In that regard, ISO/IEC 27701:2019 has been published as an extension to ISO 27001 to incorporate the privacy-specific matters as an integral part of the PIMS.

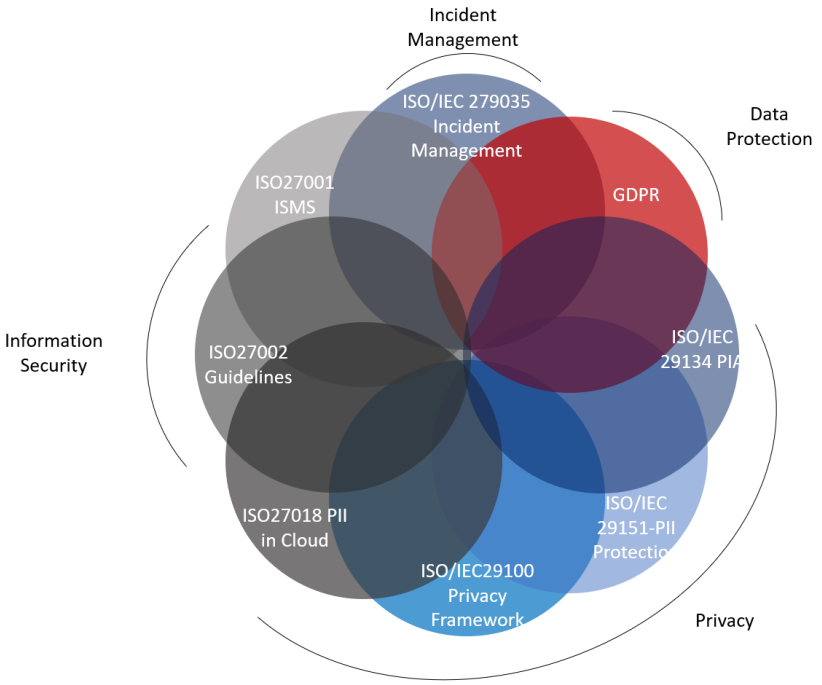

Figure 1: The Building Blocks of ISO/IEC 27701:2019 adapted from (Shaikh 2020)

According to ISO, the PIMS is an ISMS dedicated to privacy protection (ISO/IEC 27701 2019). The EU's GDPR came into effect in May 2018, and despite that, there is still no certification standard for it. ISO/IEC 27701:2019 came into effect in August 2019 and is expected to support GDPR compliance. Since ISO/IEC 27701:2019 is relatively a new standard, not much guidance is available on how it can support in attaining GDPR compliance.

A report by Keepabl research (Keepabl 2020) states that adoption figures are not high for 27001 in the context of driving GDPR compliance. This does not suggest that ISO/IEC 27701:2019 will enjoy widespread adoption. In August 2019, Corporate Compliance Insights (Forman 2019) published Coalfire's David Forman's musings over the possible implications of the newly published extension to ISO27001. His thoughts were set on the privacy extension pertaining to and supporting the GDPR. Tzolov (Tzolov 2019) has presented ISO/IEC 27701:2019 as a model for establishment of PIMS. RedMond (RedMond 2019) conducted a comparison of ISO27001, ISO27002 and ISO/IEC 27701:2019 at a high level. However, he did not discuss about the details of clauses, differences, and overlaps. Forman (Forman 2019) has noted that the previous ISO 27001 was more comparable to the service organisation control reporting suite. With the new privacy extension by ISO/IEC 27701:2019, it seems to become the GDPR certification standard to help businesses. Therefore, it is expected that this standard will assist in developing better systems to achieve GDPR compliance, validation, and stronger marketing value.

The French Data Protection Authority (the"CNIL") issued a press release (CNIL 2020) emphasising the significance of the ISO/IEC 27701:2019 standard towards the security of PII. The CNIL stresses that the ISO/IEC 27701:2019 standard is a truly global standard. Siganto (Siganto 2020) has analysed how useful ISO/IEC 27701:2019 can be in ensuring compliance against global regulatory requirements.

Although, the immediacy of the standard with GDPR is highlighted in a dedicated annex that charts each clause of the standard with the respective GDPR article, there is lack of guidance regarding explicit requirements. Most of the articles mentioned above provide their own point of view on expectation from ISO/IEC 27701:2019, none of them map the standard's privacy requirements with any other global privacy regulation. To fill this gap, this research is conducted to review and map the privacy compliance requirements by ISO/IEC 27701:2019 and GDPR. The reason for choosing GDPR for this comparison is that it is assumed to be one of the most generalised and comprehensive regulation that seems to cover privacy requirements of multiple jurisdictions (Anwar et al. 2018). The results of this research will help organisations in establishing, implementing, maintaining, and continuously improving their privacy compliance requirements and programs. Further the review and mapping done in this research will develop an understanding of the ISO/IEC 27701:2019 standard that will help organisations in conducting business at an international level and help in attaining consistent PII protection. ISO/IEC 27701:2019 builds on a multitude of other standards and regulations, which are shown in figure 1. The focus of this article is ISO/IEC 27701:2019 and its mapping to GDPR.

3. Action Design Research Method

This research forms an important part of our large action design research (Sein et al. 2011) project, which is performed in partnership with industry partner IDZ. The idea was formulated by IDZ which was further refined by reviewing the relevant literature. IDZ is processing PII and operating in different jurisdictions which implies that it must comply with individual country regulations. Ensuring compliance with multiple regulations is a costly and tedious task. Hence, IDZ wants to adopt an approach based on international best practice that must be capable of adapting to other regimes and not impose requirements that hinge on specific legislation. Therefore, before designing the intended ecosystem, IDZ wants to ensure that their processes and practices are compliant to global privacy regulations such as GDPR. For this purpose, IDZ intends to expand their existing ISO27001 ISMS by implementing ISO/IEC 27701:2019 PIMS. However, they are unsure on whether this will ensure GDPR compliance or not. This problem was formulated by IDZ for which they engaged University researchers to map ISO/IEC 27701:2019 with GDPR and devise an integrated set of requirements from both. The principles of practice-based research and theory-ingrained artefact were employed at this stage. The build, intervene and evaluate stage is carried out as an iterative process in IDZ environment. ISO 27701 and GDPR mapping was developed and evaluated through intervention for IDZ's context. Review workshops were conducted to evaluate the proposed artifact. This stage is guided by the principles of reciprocal shaping, mutually influential roles, and authentic and concurrent evaluation. Reflection and learning is a continuous stage. The principal of guided emergence enabled this mapping to be applicable to contexts other than IDZ. The final stage of ADR methodology is formalisation of learning and draws on the principal of generalized outcomes. This overall research project started in Nov 2018 and is expected to complete in Nov 2020. Figure 2 describes the action design research project spanning over two years.

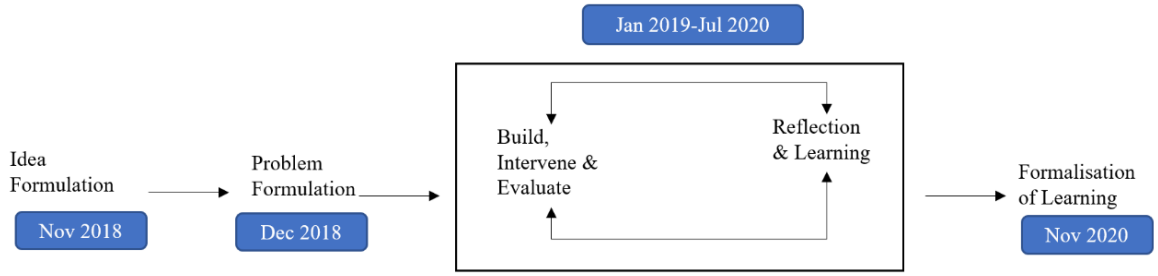

Figure 2: Action Design Research Project Timeline

4. ISO27701-GDPR Integrated Compliance Requirements Model

This research uses integrated requirement engineering model (Gill and Bunker 2013) as a theoretical lens to review and map compliance requirements from ISO/IEC 27701:2019 and GDPR for developing an integrated set of compliance requirements (See Figure 3). As a first step, clauses and articles are selected from ISO/IEC 27701:2019 and GDPR in alignment with IDZ's compliance goals (See Table 1). Next, ISO/IEC 27701:2019 is mapped to GDPR to find out gaps and overlaps between the two (See Table 2, Table 3). Finally, in the light of mapping done in step two, clauses from ISO/IEC 27701:2019 and articles from GDPR are integrated to develop a set of compliance requirement.

4.1. Selection of controls in alignment with organisational goals

The overall goal of IDZ is to ensure GDPR compliance to strengthen their position in international market. To fulfill this goal, IDZ defined information security and privacy specific goals as detailed in table 1. The relevant clauses from ISO/IEC 27701:2019 and articles from GDPR are selected against the compliance goals. However, IDZ is not sure whether the two frameworks have common requirements to fulfill IDZ compliance goals. Hence, the next step is to highlight the gaps and overlaps between the compliance requirements from ISO/IEC27701:2019 and GDPR.

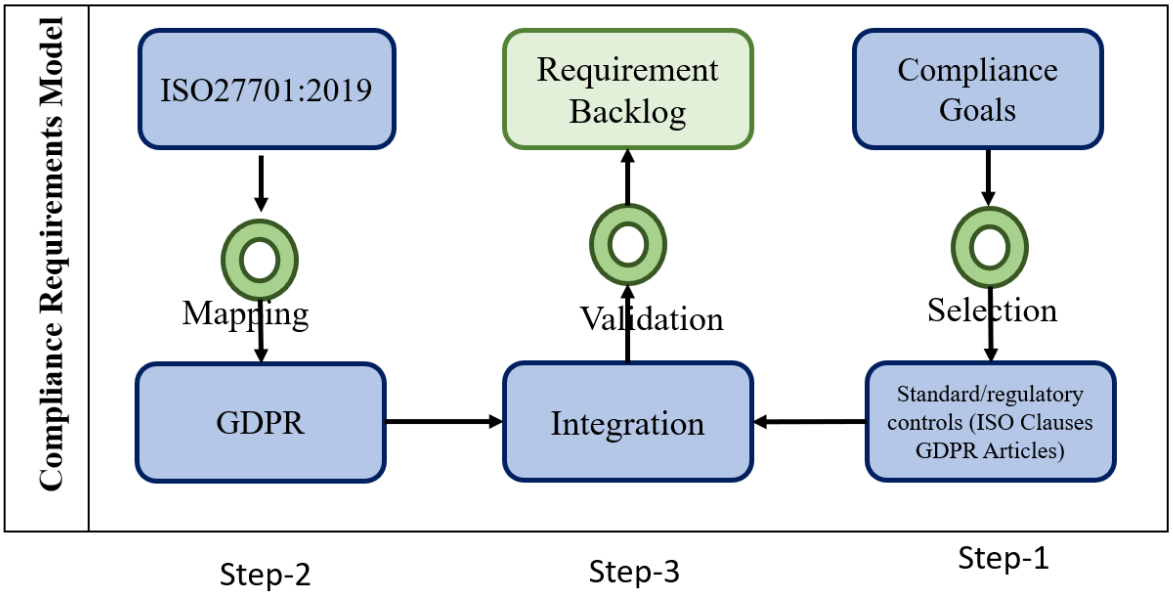

Figure 3: Integrated Compliance Requirement Model adapted from (Gill and Bunker 2013)

4.2. ISO/IEC 27701:2019-GDPR Mapping

The mapping of ISO 27701:2019 and GDPR was done to highlight the gaps and overlaps between the two as follows:

4.2.1. ISO/IEC 27701:2019-GDPR Gaps

The approach suggested by the ISO/IEC 27701:2019 standard on data protection differs in many ways from the one enshrined in the GDPR (See Table 2). To start with, ISO makes data protection dependent on information security while, in the GDPR, information security remains a component of data protection. GDPR does not mention privacy but it refers to data protection as a general principal. On the other hand, to ensure privacy, the ISO/IEC 27701:2019 promotes a full risk-based approach offering to identify and reduce information security risks applying to IT assets managing and storing PII. However, the GDPR occasionally relies on a risk-based approach to address broader risks on data subjects' rights and freedoms. GDPR is rather a right based approach. In addition, the schemes based on ISO/IEC 27701:2019 certify the conformity to a management system but the GDPR excludes certification of management systems from the scope of GDPR

approved certification. ISO's standards are private and protected by strict copyright while the GDPR requires certification requirements to be approved by a supervisory authority and made publicly and easily accessible. GDPR has a broader scope and covers different types of data. The data protected by ISO/IEC 27001 and ISO/IEC 27701:2019 includes datasets structured in IT assets while the GDPR also applies to unstructured datasets, for example standalone word processing files, spreadsheets and files stored in cabinets. Additionally, the GDPR does not only apply to digitised data processing but also to the processing and storing of personal data on physical media (e.g. paper-based records).

IDZ Goal	ISO/IEC 27701:2019 Control	GDPR Article
To understand the organisational context, stakeholder's needs, and expectations	5.2.1	24, 25, 28, 32, 40, 41, 42
To identify the stakeholders needs and expectations	5.2.2	31, 35, 36
To identify IDZ's role as a PII controller, PII processor or joint PII controller	7.2.6, 7.2.7,7.2.8, 7.3.2, 7.3.3, 7.3.5, 7.3.7, 7.3.8, 7.4.9, 8.2.5, 8.3.1, 8.4.2,8.5.1, 8.5.3, 8.5.4, 8.5.6, 8.5.7, 8.5.8	5,28,26, 24, 30, 11, 13, 14, 15, 18, 20,21,44,45,46,47,49
To determine the scope of information security management system, information security risk assessment and risk treatment	5.2.3, 5.2.4, 5.4.1.2, 5.4.1.3	32
To understand information security roles and responsibilities, develop information security policies, create awareness and training, manage information, handle media, and manage security incidents	6.3.1.1, 6.3.2.1, 6.4.2.2, 6.5.3.1, 6.8.2.7, 6.9.3.1, 6.9.4.1, 6.9.4.2, 6.10.2.1, 6.10.2.4, 6.13.1.1, 6.13.1.5,	27, 28, 33, 34,37, 38, 39
To conduct privacy impact assessment	7.2.5	35, 36
To identify applicable legislation and compliance requirements	6.15.1.1, 6.15.2.3	5,28,30,32

The GDPR does not solely protect confidentiality, integrity, and availability of information as the ISO defines information security (ISO 27000 :2018 Subclause 3.28). It also aims to prevent and address the "likelihood and severity (of the risks) for the rights and freedoms of natural persons". (Article 5.1 (f) GDPR). It is important to note that ISO/IEC 27701:2019 is a standard, which is optional and good to have for organisations whereas companies processing EU citizen's data are obligated to fulfill GDPR requirements. Also, the ISO/IEC 27701:2019 standard defines its own requirements with its own terminology though, the content and terminology of the standard does not fully align with the GDPR's provisions. The ISO/IEC 27701:2019 standard proposes such a management system that is consistent with other management system standards published by ISO. On the other hand, the GDPR does not Table 1. IDZ Compliance Goals offer a management system following ISO's definition. The GDPR establishes a legal framework defining principles and requirements that do not aim to be directly auditable. The GDPR does not aim to provide ready-to-use guidelines helping to reach compliance with the framework's requirements.

One such instance to analyse is the data breach management rules in ISO/IEC 27701:2019 and the mandatory data breach notification obligations (article 33) in GDPR. The standard's security data breach management rules map with the GDPR data breach requirement however, the standard does not include a particular 72-hour notification as required by the regulation. Another major gap between

the two is that the implementation of the PIMS does not need certification, even though it may possibly be a target to get external acknowledgment for the work conducted in the privacy space. In this regard, it is much likely that ISO/IEC 27701:2019 may serve as the foundational step for a prospective GDPR certification system. Furthermore, the certifiable terminology is perceived differently in ISO/IEC 27701:2019. As an example, although the standard's certification is supported by ISO, which is a renowned entity in entire certification panorama, it does not have the official endorsement of GDPR Article 42. This implies that the certifications cannot be considered as a comprehensive way to ensure "compliance" with Article 42 obligations unless it is acknowledged by one of the supervisory entities (Puce 2020).

Using the gaps identified in table 2, the practitioners can now carefully select controls from ISO/IEC 27701:2019 for sustained GDPR compliance. The next step is identification of overlaps between ISO/IEC 27701 and GDPR.

ISO 27701:2019	GDPR
Focuses on privacy	Focuses on data protection
Risk based approach to ensure privacy of personal information	Right-based approach to address broader risks on data subjects' rights and freedoms.
Documentation is private and protected by strict copyrights	Publicly and easily available
Focus on datasets structured in IT assets, on digital media	Also applies to un-structured data on digital as well as physical media
Collection, confidentiality, integrity and availability	probability and seriousness (of the risks) for the rights and freedoms of natural persons.'
A management system	A legal framework
Optional requirements	Mandatory principles and requirements
Terminology: PII Principal, PII controller, PII Processor	Terminology: Data Subject, Data Controller, Data Processor
Regional	International
ISO backed certification	Certification Article 43
Breach notification with no 72 hours limitation	Breach notification with 72-hour requirement

Table 2. Gaps in ISO27701:2019 and GDPR

4.2.2. ISO/IEC 27701:2019-GDPR Overlaps

The previous section highlighted the gaps between ISO/IEC27701:2019 and GDPR. In this section, overlaps between the two have been analysed. The gaps and overlaps, identified as a result of this mapping, will be integrated with controls selected against organisation goals. Hence this mapping will be used as an input for regulatory compliance requirements modelling. Instead of differences (See Table 2) in the details of requirements, the two frameworks overlap at many points. Table 3 shows the overlap between the requirements from the standard and the regulation, that can be integrated to support GDPR compliance. Clauses 1 to 3 of the ISO/IEC 27701:2019 cover the scope, lawful references, conditions, and definitions. Clause 4 comprises the common PIMS obligations in accordance with ISO 27001 and ISO 27002. The exact PIMS requirements and related information is set out from clause 5 onwards. The mapping of ISO/IEC 27701:2019 against GDPR (ISO/IEC27701:2019 Annex D) indicates that the coverage for Articles 5 to 49 of the GDPR has been provided in ISO/IEC27701:2019, with the omission of Article 43, which is discussed in previous section as a gap (Table 2). The reason for including article 5 to 49 of GDPR in Annex D of ISO/IEC 27701:2019 is that, after article 49 the later part, 50 and beyond, is about how you should handle GDPR from management perspective, except for few articles (art 83 (fines), art 86 (access t0 public documents), art 87(handling of national identity) and art 88 (employment context)).

The overlaps highlighted in table 3 suggest that benefits of employing the ISO/IEC 27701:2019 can be significant even though there are minor gaps with GDPR requirements. This standard can increase user confidence and trust through the inclusion of structured and well-defined privacy procedures and controls, that can result in more stable and trustworthy privacy protection. While the GDPR does not specifically mention adopting ISO/IEC 27701:2019 as a pathway to support compliance, many organisations already recognise ISO/IEC 27701:2019 as the global benchmark for privacy (Keepabl 2020). Nevertheless, ISO/IEC 27701:2019 certification will not meet the GDPR's requirements for a certification scheme. Regardless of the timescales for internationally recognised accredited certification, demonstrating conformity with ISO/IEC 27701:2019 is likely to become a popular approach to managing data protection and privacy. Next step is integration of requirements from ISO /IEC 27701:2019 and GDPR.

ISO27701 Clause	**GDPR Article**	**Notes**
Clause 5: PIMS specific requirements related to ISO/IEC27001	**Art 24:** Responsibility of Controller, **Art 25:** Data protection by design and default, **Art 28:** Processor, **Art 32:** Security of processing, **Art 40:** Codes of conduct, **Art 41:** Approved code of conduct, **Art 42:** Certification, **Art 31:** Cooperation with the supervisory authority**, Art 35:** Data protection impact assessment, **Art 36:** Prior consultation, **Art 32:** Security of processing	As part of the context of the organisation, needs and expectations of stakeholders and risk assessment , both ISO27701 and GDPR require companies to determine their role as a processor and/or controller and consider the impact of internal and external factors such as privacy specific regulations and contractual requirements.
Clause 6: PIMS specific guidance related to ISO/IEC27002	**Art 5:** Principles relating to processing of personal data, **Art 24:** Responsibility of the controller, **Art 25:** Data protection by design and default, **Art 27:** Representatives of controllers or processors not established in the Union, **Art 28:** Processor, **Art 30:** Records of processing activities, **Art 32:** Security of processing, **Art 33:** Notification of a personal data breach to the supervisory authority, **Art 34:** Communication of a personal data breach to the data subject, **Art 37:** Designation of the data	ISO27701 provides guidance and GDPR specifies requirements with an emphasis on roles and responsibilities regarding processions of personal data, data classification, acceptable use policy, access management, suppliers' relationships and incident reporting

	protection officer, **Art 38:** Position of the data protection officer, **Art 39:** Tasks of the data protection officer	
Clause 7: Additional ISO/IEC 27002 guidance for PII Controllers	**Art 5:** Principles relating to processing of personal data, **Art 6:** Lawfulness of processing, **Art 7:** Conditions for consent, **Art 8:** Conditions applicable to child's consent in relation to information society services, **Art 9:** Processing of special categories of personal data, **Art 10:** Processing of personal data relating to criminal convictions and offences, **Art 11:** Processing which does not require identification, **Art 12:** Transparent information, communication and modalities for the exercise of the rights of the data subject, **Art 13:** Information to be provided where personal data are collected from the data subject, **Art 14:** Information to be provided where personal data have not been obtained from the data subject**, Art 15:** Right of access by the data subject, **Art 16:** Right to rectification, **Art 17:** Right to erasure ('right to be forgotten'), **Art 18:** Right to erasure ('right to be forgotten'), **Art 19:** Notification obligation regarding rectification or erasure of personal data or restriction of processing, **Art 20:** Right to data portability, **Art 21:** Right to object, **Art 22:** Automated individual decision-making, including profiling, **Art 24:** Responsibility of the controller, **Art 25:** Data protection by design and by default, **Art 26:** Joint Controllers, **Art 28:** Processor, **Art 30:** Records of processing activities, **Art 32:** Security of processing, **Art 35:** Data protection impact assessment, **Art 36:** Prior consultation, **Art 44:** General principle for transfers, **Art 45:** Transfers on the basis of an adequacy decision, **Art 46:** Transfers subject to appropriate safeguards, **Art 47:** Binding corporate rules, **Art 48:** Transfers or disclosures not authorised by Union law, **Art 49:** Derogations for specific situations	ISO27701 provides guidance and controls in Annex A and GDPR specifies requirements on processing of personal data, consent, withdrawals, access, transfer, disclosure, privacy impact assessment, contracts with data processors, roles and responsibilities for joint controllers.
Clause 8: Additional ISO/IEC 27002 guidance for PII processors	**Art 5:** Principles relating to processing of personal data, **Art 7:** Conditions for consent, **Art 15:** Right of access by the data subject, **Art 17:** Right to erasure ('right to be forgotten'), **Art 28:** Processor, **Art 29:** Processing under the authority of the controller or processor**, Art 30:** Records of processing activities, **Art 32:** Security of processing, **Art 44:** General principle for transfers, **Art 46:** Transfers subject to appropriate safeguards, Art 48: Transfers or disclosures not authorised by Union law, Art 49: Derogations for specific situations	ISO27701 provides guidance and controls in Annex B and GDPR specifies requirements on agreed data processing and organisation's role as data processor to assist with customer obligations and data transfer/disclosure to address jurisdictional transfers.

Table 3. Overlaps between ISO27701:2019 and GDPR

4.2.3. ISO/IEC 27701:2019-GDPR Requirements Integration

There are significant overlaps between the ISO/IEC 27701:2019 and GDPR (See table 3) however, the ISO/IEC 27701:2019 defines its own requirements that sometimes differ from their counterparts in the GDPR. For example, the requirements concerning data processors (ISO/IEC 27701:2019 subclause 7.2.6) remain optional in the ISO's standard whereas in GDPR it is compulsory for processor (Article 28). ISO exempts a candidate entity from applying the safeguards (privacy controls) aimed at securing the relationships with processors as long as this exclusion is justified in the 'statement of applicability' required by the risk-based methodology(ISO/IEC 27701:2019 Subclause 6.1.3b). The ISO standard does not specify any delay to notify a data breach (Subclause 6.13.3.) to the supervisory authorities (GDPR Article 33.1). It neither requires to directly connect with the information owners possibly impacted by the incident, when the breach is "likely to result in a high risk to the rights and freedoms of natural persons" (GDPR Article 34). At the opposite, the data controller or processor is free (Subclause 7.2.6) to perform a privacy impact assessment every time it judges this procedure useful or necessary to evaluate the risk carried out by the data processing.

In the light of gaps and overlaps identified in the previous step, there are two integration points a) overlaps between the requirements from standard and the regulation suggest that common requirements need to be implemented only once with no adjustment. b) Gaps represent the uniqueness and partial match between the requirements from the standard and regulation. This gap is used to implement a unified requirement that satisfies both the standard and the regulation. One such example is the partial mismatch in breach notification requirement (ISO/IEC 27701:2019 subclass 6.13.3, GDPR Article 33.1). In order for the privacy practitioners to prove that the organisation has employed a management system that accomplishes this specific GDPR condition, they must demonstrate that the organisation either has a uniform process in place that would notify the privacy regulator within 72 hours of breach confirmation or has a process to determine if the breach is covered by the GDPR and, if so, trigger the notification within the required timeframe. Hence the two requirements were integrated into one unified requirement by adding 72 hours notification requirement to subclause 6.13.3. The unified requirements were further validated against IDZ compliance goals through management review meetings.

5. Discussion and Implications

Our industry partner, IDZ wants to ensure compliance with globally relevant GDPR. Before implementation of ISO/IEC 27701:2019, IDZ wanted to find out the gaps (See Table 2) and overlaps (See Table 3) between ISO/IEC 27701:2019 and GDPR to develop an integrated set compliance requirements that can fulfill IDZ's compliance goals (See Table 1). The goal is to identify how ISO/IEC 27701:2019 can help IDZ reconcile privacy requirements from GDPR. The standard is relatively new, and literature is scarce on this topic. Thus, we conducted this research by performing content analysis using integrated requirement engineering model (Gill and Bunker 2013), to address this important research question: whether and how the ISO/IEC 27701:2019 framework represents an opportunity for the GDPR compliance? The results of this research highlight the differing approaches promoted by the two frameworks in the form of gaps and the requirements where ISO27701 provides an opportunity for GDPR compliance.

ISO/IEC 27701:2019 is a broadly applicable standard and a globally accepted framework that can offer valuable support for integrating privacy compliance into key risk management routines (DeBos 2020). Many national authorities (such as the CNIL) participated in the development of the standard. However, other techniques of crowd sourcing could have also been used for developing the specific challenge and end user-centric standard (e.g. Gill and Bunker 2012). Further, for implementation, it is important to ask, what are the adherences between the ISO 27701 content and the GDPR content? Regarding the fundamental principles of the GDPR (consent, rights, legality, etc.), the new standard develops a set of requirements covering all the GDPR topics (See

Table 3). Clause 5 to clause 8 of the standard covers all major topics included in GDPR such as guidance for data processors, and data controllers, policies, roles, responsibilities, incident management and privacy impact assessment. However, as the standard is intended to be international, it remains by nature less precise than the GDPR on some topics (i.e. no precision of the deadline to be respected for notifying the authority) (See Table 2). An example of how the standard differs from GDPR is the conditions on data breach management in ISO/IEC 27701:2019 and the breach notification requirements (article 33) in GDPR. Even though, the standard's controls mostly map to the GDPR breach management requirements (Table 3), the standard does not include an exact 72-hour notification as noted in GDPR. The mapping done in this research suggest that, despite gaps (Table 2), this standard will be of tremendous assistance to businesses in creating privacy schemes that will assure compliance with several requirements from the GDPR. For organisations considering to implement globally accepted controls and a recognised framework, the new standard could be an effective starting point towards evolution and growth of privacy processes. However, it is imperative to note that an ISO/IEC 27701:2019 certification is not synonymous with GDPR compliance. Indeed, the main purpose of the standard is to establish worldwide principles and rules around privacy in a common language. It is, therefore, the responsibility of academics and privacy practitioners to carefully map and integrate requirements to understand what adjustments need to be made to comply with applicable regulations and standards.

Although, Annex D of ISO/IEC 27701:2019 is informative in nature, the challenge in using ISO/IEC 27701:2019 Annex D, is the need to continually consult ISO/IEC 27701:2019 documentation and GDPR text as the reader is instructed to specific clause and article in these two frameworks. Moreover, the mapping provided in official documentation of ISO/IEC 27701:2019 is only using the numbers which is quite time consuming and not easy to understand. Hence, this research is an effort to help organisations in understanding the mapping between ISO/IEC 27701:2019 and GDPR as input to developing compliance requirements modelling. However, it is still left to the privacy professionals using ISO/IEC 27701:2019 to verify regulatory compliance against privacy regulations applicable to their specific context and compliance goals. This research has following implications:

This research is an important endeavour in presenting a structured process (See Fig 3) for extracting requirements from different standards/regulations and developing an integrated set of compliance requirements backlog.

It is aimed to save time and reduce duplicate effort that is required to refer back and forth to the specific documentation to know the context and details of the controls mapped in Annex D of the standard. It would be handy and time saving for organisations to have a more explicit and clear naming and reverse mapping (GDPR to ISO).

The significant overlap between ISO/IEC 27701:2019 and GDPR highlighted in this article presents a compelling case to review the ISO/IEC 27701:2019 standard and GDPR regulation for developing a unified compliance requirements model and tools.

The proposed requirements model can help developers to develop internationally compliant software systems involving contemporary agile frameworks (Bou Ghantous and Gill 2017) both in the local and global distributed environments (Alzoubi et al. 2015)

6. Conclusion

This paper intended to evaluate the comparison and linking of newly emerged ISO/IEC 27701:2019 standard and GDPR regulation. The main contribution of this research is the gaps (Table 2) and overlaps (Table 3) between the specifications of ISO/IEC 27701:2019 and GDPR, which has not been discussed before. Furthermore, the process of extracting compliance requirements (Fig 3) from different standards and regulations is also presented in this research. The mapping of ISO/IEC

27701:2019 clauses with GDPR articles studied in this research, provides a detailed view of unique as well as overlapping requirements. The analysis conducted in this research shows that, ISO/IEC 27701:2019 is an international standard, it is not GDPR specific, nor does it represent a GDPR certification tool as defined in article 42 of the regulation. Nevertheless, it embodies the state of the art in terms of privacy protection and its adoption, which may allow organisations to improve their privacy posture and adopt an effective approach towards personal data protection. The results of this research will enable academics, policy makers and auditors to better understand the gaps and overlaps between ISO/IEC 27701:2019 and GDPR and hence develop compliant systems as appropriate to their specific context.

6. References

"ISO 27701 & GDPR: Adoption Issues Ahead",. 2020. Keepabl TM, (available at. https://keepabl.com/news/iso-27001-data-protection-research/; retrieved August 10, 2020).

"ISO/IEC 27701:2019",. 2020. ISO, (available at https://www.iso.org/standard/71670.html; retrieved August 13, 2020).

Alzoubi, Y.I., Gill, A.Q. and Al-Ani, A., 2015. Distributed Agile Development Communication: An Agile Architecture Driven Framework. JSW, 10(6), pp.681-694.

Anwar, M., Gill, A., and Beydoun, G. 2018. "A review of information privacy laws and standards for secure digital ecosystems", in ACIS, 2018, Sydney, Australia.

Bou Ghantous, G. and Gill, A., 2017. DevOps: Concepts, practices, tools, benefits and challenges. PACIS2017.

Bougiakiotis, E. 2019. "The Layered Links Model: An Alternative Approach to International Privacy Regulation", SSRN Electronic Journal (doi: 10.2139/ssrn.3464380).

CNIL. 2020. "CNIL Stresses Importance of ISO 27701 for Global Data Protection Compliance | Privacy & Information Security Law Blog", Privacy & Information Security Law Blog, (available at https://www.huntonprivacyblog.com/2020/04/06/cnil-stresses-importance-of-iso-27701-for-global-data-protection-compliance/; retrieved August 08, 2020).

DeBos, T. 2020. "How ISO 27701 could be a new framework for sustained GDPR compliance", Ey.com, (available at https://www.ey.com/en_au/consulting/how-iso-27701-could-be-a-new-framework-for-sustained-gdpr-compliance; retrieved August 06, 2020).

EU. 2018, “General Data Protection Regulation”, https://gdpr-info.eu , Retrieved: August 05, 2020.

Foreman, D. 2020. "ISO 27701: Will it Be the New GDPR Certification? | Corporate Compliance Insights", Corporate Compliance Insights, (available at https://www.corporatecomplianceinsights.com/iso-27701-gdpr-certification/; retrieved August 20, 2020).

Gill, A., and Bunker, D. 2013. "SaaS Requirements Engineering for Agile Development", IGI Global, Italy (2013)

Gill, A.Q. and Bunker, D., 2012. Crowd sourcing challenges assessment index for disaster management. In 18th Americas Conference on Information Systems 2012, AMCIS 2012.

IBM Security. 2019. "Cos of a Data Breach", Michigan,USA: IBM Security, pp. 1-74 (available at https://www.ibm.com/security/data-breach).

ISO., 2020. "ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection", ISO, (available at https://www.iso.org/committee/45306.html; retrieved August 12, 2020).

Puce, J.,2020. “Is ISO 27701 a silver bullet for GDPR compliance?”, (available at https://www.linkedin.com/pulse/iso-27701-silver-bullet-gdpr-compliance-juris-puce/?articleId=6613479113191632896).

Redmond, M. 2020. "ISO/IEC 27552*:The Answer to Data Privacy? - PECB Insights", PECB Insights, (available at https://insights.pecb.com/iso-27552-answer-data-privacy/; retrieved August 11, 2020).

Sein, M., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R.: Action Design Research, Management Information Systems Quarterly (35:1), pp. 37-56 (2011)

Shaikh, M. 2020. "INTRODUCTION TO ISO27701- PRIVACY INFORMATION MANAGEMENT SYSTEMS | Muneeb Imran Shaikh | Experts Exchange", Experts-exchange.com, (available at https://www.experts-exchange.com/articles/34491/INTRODUCTION-TO-ISO27701-PRIVACY-INFORMATION-MANAGEMENT-SYSTEMS-Muneeb-Imran-Shaikh.html; retrieved August 13, 2020).

Siganto, J. 2020. "ISO 27701 Privacy Management System: How useful is it? - Privacy108 | Australian Data Privacy & Security Consulting", Privacy108 | Australian Data Privacy & Security Consulting, (available at https://privacy108.com.au/insights/iso-27701/; retrieved August 11, 2020).

Tzolov, T. 2019. "ISO 27552 as a Model for Establishment Personal Information Management Systems", in 2019 International Conference on Information Technologies (InfoTech), Bulgaria: IEEE.

World Economic Forum. 2020. "Executive Summary", The Global Risks Report 2018, (available at http://reports.weforum.org/global-risks-2018/executive-summary/; retrieved August 05, 2020).