Regulatory Rules for Security Requirements of Financial Information Systems: Attempt to Formalize

Shouki A. Ebad¹

Received: 16 March 2017 / Accepted: 27 June 2017 / Published online: 25 July 2017
© Springer International Publishing AG 2017

Abstract As a result of the economic growth and increasing technology usage, financial systems are becoming pervasive and automate customer processes and data. These systems, like other systems that are governed by law, are required to comply with governmental regulations. However, this requirement is not easy to implement because of the challenge that comes from domain-specific definitions and the ambiguities that exist in laws. Moreover, mining financial data requires a combination of domain and technical knowledge plus an understanding of how the financial markets are manipulated. Thus, there is a business need to formalize security texts, extract rules, and then enforce them throughout the supply chain. Most of the approaches that have tried to achieve this need were validated on healthcare systems. Using a case study from Saudi Arabia, we applied a well-known approach proposed by Breaux and Antón on a quite different domain, Saudi stock exchange (Tadawul). Security in Saudi Arabia is an issue because of the high-income Saudi economy. Without such validation on non-healthcare domains, it is premature to automate Breaux and Antón approach which is currently performed manually. We also used readability analysis of Tadawul's regulations based on proven metrics. As a result, we extracted and formalized two rights, eight obligations, eighteen constraints, and seven rules. From readability view, Tadawul's regulations considerably need reading skills. Our analysis can help standards organizations, requirements engineers, systems administrators, and policy makers by ensuring that their systems conform to law.

Keywords Software requirement engineering · Information systems, security · Saudi stock exchange · Formalization · Readability

✉ Shouki A. Ebad
shouki.abbad@nbu.edu.sa

¹ Faculty of Computing and IT, Northern Border University, Rafha, Saudi Arabia

1 Introduction

In general, better utilization of technology can improve the quality of life for many citizens in the developing countries. However, one of the specific challenges facing scholars is to take into account the wide range of different contexts that regulations and policies appear in (Bada and Madon 2006). Although there have been several strategies to development, still economic growth is a dominant perspective of development since the Second World War (Zheng 2009). Accordingly, the outcome of development is measured by gross national product or per capita income. The perspective of economic growth and increasing technology usage have pushed financial information systems (FISs) to become pervasive and automate customer processes and data. FISs are often business-critical systems because if they fail to deliver their services as expected then serious problems and significant economic losses may result (Sommerville 2015). Such systems have become the targets of security attacks due to the popularity of their online transactions that require sharing financial data (Bada and Madon 2006).

In addition, poor infrastructure in the less-developed countries has led attackers to have both the incentive and the ability to inflict significant harm to technology users (Ben-David et al. 2011). Emerging economies suffer economically proportionally more than developed ones from security attacks or cybercrimes (Ben-David et al. 2011). The costs of recovery from attackers form a much higher percentage of GDP for developing countries than for developed nations (Baker 2014). Research on this subject has encouragingly moved beyond the boundary of an organizational level of analysis to explore much wider societal and technical issues. This has also led security to be a central concern in financial systems and a hotspot in research (Cheng and Atlee 2007; Ben-David et al. 2011; Zafar et al. 2012; Osei-Bryson and Vogel 2014). Such systems, which are increasingly social too, should then be developed not only to address business goals or stakeholder needs but to address security and privacy issues because the boundary between sensitive and non-sensitive personal information is still blurring (Breux 2014). The impact of announcements of cyberattack on the stock market of publicly traded companies has been examined by Campbell et al. (2003). Moreover, security articles in financial systems are difficult for users to interpret, and their ambiguities and complexity make it difficult for software engineers to use them as a guide for designing and implementing these systems (Breux et al. 2006). The consequences of failing to comply with these regulations not only may lead to the disclosure of customer confidential information, which could be damaging to their reputations and finances, but also can cause tremendous economic loss and reputation damage for financial providers (Wu et al. 2012; Ebad et al. 2016). Thus, building a legally compliant system is an engineering problem and is recognized as a significant issue, especially in systems governed by law (Massey et al. 2010; Maxwell et al. 2012). This challenge comes from ambiguities and domain-specific definitions found in governmental rules (Breux et al. 2006; Otto and Antón 2007).

Security regulations of Tadawul, Saudi Arabian stock exchange, contain ambiguities that are intended by policy makers to be reinterpreted as business

practices evolve and as the abilities to comply with regulations change over time. For instance, Article 7-2, states that “They (i.e., Tadawul’s personnel) should also take all reasonable precautions for properly switching off their computers”; the word “reasonable” is intentionally ambiguous, as it is unclear exactly which precautions are considered reasonable. This ambiguity comes from English words that cannot be removed from the legal requirements and can be mapped to different logical interpretations by software engineers; it can only be interpreted in the context of organizational practices, goods, and services (Breux 2009). Because financial data have many forms such as stocks, mutual funds, commodities, and futures contracts, mining such data requires a combination of domain and technical knowledge plus an understanding of how the financial markets work and are manipulated (Boetticher 2006). Accordingly, there is a pressing need for methods to automatically formalize security texts, extract regulations, and enforce them throughout the supply chain. A well-known approach for such an analysis is the approach proposed by Breux and Antón (2008). Up to our knowledge, most of the available works that formalize and extract rules and regulations use healthcare as a case study. In this study, we applied the Breux and Antón’s approach to the security articles in the code of conduct of Tadawul. The approach is used here to extract formal descriptions of the Saudi rules that govern stakeholder actions from the regulations of Tadawul. In addition, due to economic and political complexities in Arab states, when conducting research, one cannot easily apply the same business models in these regions as those used in Western countries (Jakobsen 2013).

This paper is an early, novel attempt to apply concepts of the Breux and Antón approach to security requirements of non-healthcare regulations in an emerging economy, Saudi Arabia. This provides a conceptual lens to address the issues of formalizing process in the context of financial security requirements; which can contribute to improving security issues in such FISs. This validation is expected to assist system administrators and policy makers as well as requirements engineers. This article is structured as follows: Sect. 2 describes the related work. In Sect. 3, we present our methodology in detail. Section 4 presents the required background that forms the basis for the Breux and Antón approach. In Sect. 5 we present and discuss the results of our implementation. Section 6 describes the readability analysis on Tadawul’s statements. We discuss the study’s limitation in Sect. 7. Finally, Sect. 8 summarizes the article and offers some directions for future work in this area.

2 Related Work

In this section we, in chronological order, describe the previous works on formalizing the regulations. Breux et al. (2006) analyzed the U.S. Health Insurance Portability and Accountability Act (HIPAA) rules as a set of natural language statements as rights, constraints, or obligations; after that, they extended their work in (Breux and Antón 2008) by presenting a method to handle the cross-references appearing in the HIPAA text. Wu et al. (2012) proposed a framework to facilitate compliance analysis between healthcare systems and legal rules. Massey et al. (2010) discussed how requirements engineers can evaluate security software

requirements for compliance with the relevant aspects of law in the form of a particular legal text. Specifically, they demonstrated their study of the iTrust¹ requirements with respect to the HIPAA rules. May et al. (2006) transformed legal text into a format that uses the commands in a presented semantic structure to express policies. Once the legal rules had been expressed, they used the SPIN model checker² to reason about the consistency of the generated rules, and they determined differences between the 2000 and 2003 versions of the HIPAA Rules. To map legal requirements for sensitive information to a set of technical security requirements, Jensen et al. (2009) elicited security requirements from legislation applicable to the healthcare domain. They are written to support reuse and provide traceability to the legislation from which they were derived. They used the European Data Protection Directive, and then listed and referred to the Norwegian legislation used in their work as example of a national implementation of the Directive. Jorshari et al. (2011) presented a process, which supports the extraction of requirements from relevant laws and legislation and their mapping to system security requirements. The approach follows the Hohfeld legal taxonomy (Hohfeld 1913) and nature language patterns (Breux and Antón 2008) to model and analyze legal text and Secure Tropos to extract and analyze security requirements (Mouratidis 2004); a smart card-based system was used as a case study to evaluate usefulness of the proposed approach. Kargl et al. (2008) analyzed the security and privacy requirements of pervasive eHealth monitoring systems (PEMS) which use wireless sensor networks. Based on their experience developing their eHealth system, ReMoteCare, they devised a model of such systems which they use to discuss threats and attacks, address security requirements, and give guidelines for security mechanisms. Ebad et al. (2016) applied the Breux and Antón approach beyond U.S healthcare by demonstrating its validity in an analysis of Saudi healthcare privacy regulations, in Saudi Arabia. Practical attempts—namely, tools and techniques—to the task of natural-language processing of regulatory texts are considered by others (Brodie et al. 2006; Kiyavitskaya et al. 2007; Stamey and Rossi 2009).

In conclusion, formalizing and analyzing security requirements of financial legal texts have not attracted the attention of sufficient researchers with regard to that of healthcare regulations or the development of practical tools. Most attempts have focused on healthcare regulations (Bada and Madon 2006; Breux et al. 2006; May et al. 2006; Kargl et al. 2008; Massey et al. 2010; Wu et al. 2012; Ebad et al. 2016). For this, there is a need to further validate Breux and Antón methodology, heuristics, and patterns within the context of financial regulations and aviation standards to determine its applicability beyond healthcare.

This paper applies Breux and Antón approach to formalize laws and regulations and to support the elicitation of security requirements of a financial system to demonstrate the applicability of the approach beyond healthcare. Without such validation, it is premature to automate Breux and Antón approach that which is currently performed manually. According to Beckers (2012), the U.S. has no central data protection law, but separate privacy laws such as those of finance, healthcare,

¹ <http://sourceforge.net/projects/itrust/>.

² <http://spinroot.com/spin/whatispin.html>.

and children. The same happens with Saudi Arabia, the Code of Conduct for the Personnel of Saudi Stock Exchange Company (Tadawul) is for financial information, and the Ethics of the Medical Profession is for medical information (Ebad et al. 2016). However, criminal violations of health regulations in the U.S. (i.e., HIPAA) can involve violations of other laws (Massey et al. 2010). To date, this does not happen in the case of less-developed countries like Saudi Arabia. Although adoption of these guidelines in less-developed countries is positive because any kind of regulations is better than nothing, it is not enough unless these guidelines are implemented by any given software system. Our study contributes to this direction.

3 Research Strategy

Case study is an empirical research strategy suitable for investigating contemporary phenomena that cannot be addressed through controlled experiments; it is commonly used in areas like political sciences, public administration, and social work (Yin 2013). Recently, the term “case study” has appeared in the title of IT research papers (Runeson and Höst 2009). Our motivation for using case study methodology arises primarily from previous studies that have validated the Breau and Antón approach using only healthcare documents. Moreover, we want to know how security requirements of a financial system successfully formalized. Compared with other research strategies, e.g., survey, histories, and analysis of archival financial records, the case study would be more suitable to answer for such a how question because it might examine how FISs could implement their legal regulations to achieve the necessary security. Herein, we apply the approach beyond healthcare by demonstrating its validity in analysis formalization of Saudi stock exchange security articles. Investigator triangulation was addressed by carefully documentation for the study’s procedures while conducting the case study. In addition, the author is experienced in analysis of such requirements on different contexts (Ebad et al. 2016). Contradictions, which limit reliability, and limitations, which limit external validity, are sought in Sect. 6, addressed and documented to the maximum extent possible. The units of analysis in our case study are the natural language characteristics including words, phrases, sentences, passages, items, subsections, sections, and articles in Tadawul’s code of conduct. We assume that the reader is familiar with the above characteristics of case study strategy such as units of analysis, triangulation, and analysis of archival records. Interested readers can consult (Yin 2013) for further information.

3.1 Saudi Stock Exchange (Tadawul)

Our case study in this research is from Saudi Arabia which is the largest oil producer, oil exporter, and oil proven reserves possessor worldwide. It also has almost 20 percent of the world’s proven reserves and has a leading role in OPEC so that its economy is considered the largest in the Middle Eastern region (Merdad 2012). Saudi Arabia is categorized as a high-income economy and is the only Arab country to be part of the G-20 major economies.

On the 19th of March 2007, the Council of Ministers in Saudi Arabia approved the formation of the Saudi Stock Exchange (Tadawul) Company. This was in accordance with Article-20 of the Capital Market Law establishing Tadawul as a joint stock company.³ Tadawul is the only stock exchange in Saudi Arabia and the largest in the Middle Eastern region. Furthermore, Tadawul lists 156 firms as of September 2, 2012. In August 2010, the Capital Market Authority Council approved the code of conduct that is consistent with best professional practices that can be harmonized with the distinctive characteristic of Tadawul in order to have a highly ethical and professional working atmosphere for its Personnel. Tadawul shall ensure that its Personnel is committed to abide by the terms of the code of conduct to sustain its credibility, efficiency, and competence of its business and activities and to maintain its reputation in the capital market (Soldatkin and Astrasheuskaya 2011). Although the code of conduct consists of 16 articles, we focused in this research on the article related to information security, articles 6, 7, and 16. Because the main idea of Article 9 is already existing in Article 6, we ignore it from our focus. Tadawul's code of conduct is available in the official website of Tadawul. We put the considered articles in the Appendix.

4 Concepts of the Breaux and Antón Approach

The Breaux and Antón approach that we validate in this paper was conducted in the spirit of Grounded Theory (GT), in which phenomenon is analyzed to develop an understanding of the present state of a specific subject of interest. GT is derived from data that have been gathered and analyzed systematically (Glaser and Strauss 1967). In particular, observations from a data set are relevant to that data set; the key points are marked within a text of interest marked with several codes. The codes are grouped into similar concepts to make them more workable. From these concepts, categories are formed, which are the basis for creating a theory. Therefore, our work herein is not based on hypothesis or a distinct theory that we hope to accept or reject. The results of this kind of analysis are expected to provide additional benefits to financial policy makers, requirements engineers, and information systems developers, especially in emerging economies, by providing more objective criteria for assessing Tadawul practices.

With the Breaux and Antón approach, the following three-step process should be repeated to extract rules:

1. Identify a statement written in natural language that expresses rights, permissions, or obligations.
2. Apply semantic parameterization to the statement to derive semantic models for the actors, actions, and objects of each statement.
3. Derive rules with preconditions and effects built from the temporal constraints that are related to the semantic models.

³ Tadawul's website is <http://www.tadawul.com.sa>.

More details of the Breaux and Antón approach are not included here. We, therefore, assume that the reader is familiar with the basic concepts including: constraint, right, obligation, semantic parameterization, property types (subject, action, object, target, purpose), and rule tables (reference of rule, initial record of rule, extended record of rule), as well as the Grounded Theory (GT). Otherwise, interested readers can consult (Breaux and Antón 2008; Breaux 2009) for a comprehensive review of such details.

5 Analysis of Results

Applying the semantic parameterization process to the code of conduct of Tadawul yielded encodings for two rights, eight obligations, eighteen constraints, and seven rules. To characterize rights, obligations, and constraints, some patterns have been noticed. They consist of a sequence of words and parts of speech such as verbs and adjectives. The patterns for encoding rights and obligations identify an actor, action, and relationship to other objects or activities. Furthermore, the patterns for encoding rules may contain constraints on personnel rights and obligations. Table 1 shows the two, eight, and ten natural language patterns that were identified to encode rights, obligations, and constraints in the code of conducts, respectively.

The predicates produced by the semantic parameterization process distinguish properties, for example: the action, subject, and object of an activity. To deny/allow and parameterize rules related with information access, rule tables are designed.

Based on patterns shown in Table 1, we extracted the following two rights, eight obligations, and eighteen constraints:

R₁: Tadawul shall have the right to pursue any legal proceedings.

R₂: Tadawul's Compliance Committee shall be the authority with which the application of the terms of code of conduct.

O₁: Personnel and Tadawul's CEO are prohibited from practicing other work.

O₂: Personnel are prohibited from offering consultation.

O₃: Personnel shall not disclose any confidential information.

Table 1 Patterns

	ID	Pattern
Rights	R ₁ , R ₂	<actor> shall <verb> ...
Obligations	O ₁ , O ₂	<actor> is/are <adjective> ...
	O ₃ , O ₄ , O ₅ , O ₇ , O ₈	<actor> shall/shall not <verb> ...
	O ₆	<actor> must not <verb> ...
	C ₃ , C ₅ , C ₆ , C ₇ , C ₁₄ , C ₁₆	<actor> is/are <adjective> ...
Constraints	C ₄	<actor> should <verb> ...
	C ₁ , C ₂ , C ₈ , C ₉ , C ₁₀ , C ₁₇ , C ₁₈	<actor> shall <verb/adjective> ...
	C ₁₁ , C ₁₂ , C ₁₃ , C ₁₅	< actor> must/must not <verb> ...

The patterns identified to encode rights, obligations, and constraints in the code of conduct of Tadawul

O₄: Personnel shall take all necessary precautions to secure confidential information.

O₅: Personnel shall comply with specific policies at the end of service.

O₆: Personnel must not demand any information not-relating to their work.

O₇: Tadawul shall maintain the confidentiality of the information.

O₈: Tadawul's Compliance Committee shall keep all disclosed information.

C₁: Tadawul shall have the right to pursue any legal proceedings.

C₂: Tadawul's Compliance Committee shall be the authority with which the application of the terms of code of conduct.

C₃: Work is outside Tadawul.

C₄: Personnel should obtain Tadawul's written approval.

C₅: Personnel are prohibited from practicing work.

C₆: Personnel are prohibited from offering consultation.

C₇: Tadawul's CEO is prohibited from practicing work.

C₈: Personnel shall disclose confidential information.

C₉: Disclosing information shall be officially.

C₁₀: Personnel shall take all necessary precautions to secure confidential information

C₁₁: Personnel must refrain from disclosing confidential information.

C₁₂: Personnel must stop using confidential information.

C₁₃: Personnel must comply with the code of Law Practice.

C₁₄: Personnel are at the end of service.

C₁₅: Personnel must not demand any information.

C₁₆: Information is relating to work.

C₁₇: Tadawul shall maintain the confidentiality of the information.

C₁₈: Tadawul's Compliance Committee shall keep all disclosed information.

All of these rights, obligations, and constraints are transformed into the seven rules shown in Table 2. For further illustration, the fourth column, i.e., the statement level is added, which merely rephrases the constraints using an if-else statement.

For a single rule, there are one or more entities that could be queried. This entity is the value of the subject, target, object, or action. Therefore, we consider all of the expected values for the subject, target, object, and action.

Table 2 List of rules

Rule#	Right/obligation	Constraints on rule	Statement level
1	Right (R ₁)	$\neg C_{13} \wedge C_1$	If not C ₁₃ , then C ₁
2	Right (R ₂)	C ₂	Clause (always true)
3	Obligation (O ₁)	$C_3 \wedge (C_5 \vee C_7)$	If C ₃ , then C ₅ or C ₇
4	Obligation (O ₂)	$\neg C_4 \wedge C_6$	If not C ₄ , then C ₆
5	Obligation (O ₃)	C ₈ $\wedge$ C ₉	If C ₈ , then C ₉
6	Obligation (O ₄ , O ₆ , O ₇ , O ₈)	$O_{4,6,7,8}: C_{16} \wedge (C_{10} \vee C_{17} \vee C_{18} \vee C_{15})$	If C ₁₆ , then C ₁₀ or C ₁₅ or C ₁₇ or C ₁₈
7	Obligation (O ₅)	$C_{14} \wedge (C_{11} \vee C_{12} \vee C_{13})$	If C ₁₄ , then C ₁₁ or C ₁₂ or C ₁₃

A description of the rules extracted from the code of conduct of Tadawul; the (Statement Level) column converts the (Constraints on Rule) column into if-else syntax

Consider Rule 2, for instance, with the constraint C_2 , where C_2 says “Tadawul’s Compliance Committee shall be the authority with which the application of the terms of code of conduct”. We can query two different entities, namely, the subject and object, as follows:

- The Tadawul’s Compliance Committee (subject) can be queried regarding who might be the authority with which the application of the terms of code of conduct.
- The terms of code of conduct (object) can be queried regarding to which Tadawul’s Compliance Committee might be the authority with.

For every rule, we created three tables (1) reference of rule which describes the rule and its reference, (2) initial record of rule which sorts the properties, and (3) extended record of rule which states the required query and its answer in the Value and Property columns, respectively. The goal of tables is to expose details that will support software engineers design access control systems. Due to space limitation, we merge the three tables of each rule into one.

Rule 1 (in Table 2), which represents right R_1 , is formalized through Table 3. Rule 2 (in Table 2), which represents right R_2 , is formalized through Table 4. Rules 3, 4, and 5 (all in Table 2), which represent the obligations O_1 , O_2 , and O_3 , are

Table 3 Rule 1 tables

Reference of rule: $R_1: \neg C_{13} \wedge C_1$		
Reference	7-6	
R_1	Tadawul shall have the right to pursue any legal proceedings.	
C_1	Tadawul shall have the right to pursue any legal proceedings.	
C_{13}	Personnel must comply with the code of law practice	
Initial record of rule		
1	Subject	Tadawul
2	Object	Legal proceedings
3	Subject	Personnel
4	Object	Code of law practice
Extended record of rule		
Paragraph	Property	Value
7-6	Subject	Who shall have the right to pursue any legal proceedings (C_1)
7-6	Subject	Who must comply with the code of law practice (C_{13})
7-6	Object	Which Tadawul shall have the right to pursue on (C_1)
7-6	Object	Which personnel must comply with (C_{13})

It shows the considered tables of Rule 1 (i.e., Right R_1): (1) Reference of rule, (2) Initial record of rule, and (3) Extended record of rule

Table 4 Rule 2 tables

Reference of rule: R ₂ : C ₂		
Reference	16	
R ₂	Tadawul's Compliance Committee shall be the authority with which the application of the terms of code of conduct	
C ₂	Tadawul's Compliance Committee shall be the authority with which the application of the terms of code of conduct	
Initial record of rule		
1	Subject	Tadawul's Compliance Committee
2	Object	Terms of code of conduct
Extended record of rule		
Paragraph	Property	Value
16	Subject	Who shall be the authority with which the application of the terms of code of conduct (C ₃)
16	Object	Which Tadawul's Compliance Committee shall be the authority with (C ₃)

It shows the considered tables of rule 2 (i.e., Right R_2): (1) Reference of Rule, (2) Initial record of rule, and (3) Extended record of rule

Table 5 Rule 3 tables

Reference of rule: $O_1: C_3 \wedge (C_5 \vee C_7)$		
Reference	6-1,2	
O_1	Personnel and Tadawul's CEO are prohibited from practicing other work	
C_3	Work is outside Tadawul	
C_5	Personnel are prohibited from practicing work	
C_7	Tadawul's CEO is prohibited from practicing work	
Initial record of rule		
1	Subject	Personnel or Tadawul's CEO
2	Object	Work
Extended record of rule		
Paragraph	Property	Value
6-1,2	Subject	Who is prohibited from practicing other work (C_5, C_7)
6-1,2	Object	Which personnel or CEO is prohibited from (C_5, C_7)

It shows the considered tables of Rule 3 (i.e., Obligation O_1): (1) Reference of rule, (2) Initial record of rule, and (3) Extended record of rule

formalized through Tables 5, 6, and 7 respectively. Rule 6 (in Table 2), which represents obligations O_4 , O_6 , O_7 , and O_8 are formalized through Table 8. Finally, Rule 7 (in Table 2), which represents obligation O_5 , is formalized through Table 9.

Table 6 Rule 4 tables

Reference of rule: $O_2: \neg C_4 \wedge C_6$		
Reference	6-1	
O_2	Personnel are prohibited from offering consultation	
C_4	Personnel should obtain Tadawul’s written approval	
C_6	Personnel are prohibited from offering consultation	
Initial record of rule		
1	Subject	Personnel
2	Object	Consultation
3	Object	Tadawul’s written approval
4	Action	Obtain
Extended record of rule		
Paragraph	Property	Value
6-1	Subject	Who is prohibited from offering consultation (C_6)
6-1	Object	Which personnel should obtain Tadawul’s written approval (C_4)
6-1	Object	Which personnel is prohibited from (C_6)
6-1	Action	What the personnel should do to offer consultation (C_4)

It shows the considered tables of Rule 4 (i.e., Obligation O_2): (1) Reference of Rule, (2) Initial record of rule, and (3) Extended record of rule

With the above rule tables, it is easier for software requirement engineers to address the ambiguity in each requirement of the Saudi stock exchange security articles. Unlike natural languages, these tables use the first-order predicate logic (FOPL) as a formal method to provide interpretation so that whether an expression is legal can be precisely determined. The other good point is related to existence of ‘shall’ statements in the Tadawul text; for example, in articles: 6-2, 7-1, 7-2, 7-5, and 16, such statements define what the system shall do (Sommerville 2015). In systems requirements engineering, the use of these statements is encouraged; as this implies a directive to express what is obligatory. By contrast, ‘shall not’ statements define system behavior that is unacceptable. These ‘shall not’ statements cannot be implemented directly but have to be decomposed into more specific ‘shall’ statements. For example, Article 7-1 (‘Personnel shall not disclose, announce or declare any such information to any other party’). This ‘shall not’ statement is decomposed into two ‘shall’ statements: ‘Personnel shall disclose confidential information’ and ‘Disclosing information shall be officially’. Table 7 shows this decomposition. Implementation of the ‘shall and ‘shall not’ statements might make the responsibility of professionals and ethics on machines or software rather than people.

With the above analysis, policy makers in Saudi Arabia can have insights in the semantic relationships that create the meaning of their policy. Accordingly, they can

Table 7 Rule 5 tables

Reference of rule: O_3 : $C_8 \wedge C_9$		
Reference	7-1	
O_3	Personnel shall not disclose any confidential information	
C_8	Personnel shall disclose confidential information	
C_9	Disclosing information shall be officially	
Initial record of rule		
1	Subject	Personnel
2	Object	Information
3	Action	To disclose
Extended record of rule		
Paragraph	Property	Value
7-1	Subject	Who shall disclose any confidential information (C_8)
7-1	Object	Which personnel shall disclose (C_8)
7-1	Action	What the personnel shall do with confidential information (C_8, C_9)

It shows the considered tables of Rule 5 (i.e., Obligation O_3): (1) Reference of Rule, (2) Initial record of rule, and (3) Extended record of rule

recommend mechanisms to resolve conflicts and ambiguity, resulting in higher quality policy statements that better conform to the Tadawul's requirements.

6 Readability Analysis

Tadawul's personnel are increasingly becoming more interested in knowing how to secure their information. Therefore, it is useful to assess security regulations in a way that tests their readability. Although the Tadawul provides useful examples, the examples are not exhaustive and it is up to the financial firm to make a subjective judgment with regard to readability. A more objective measure entails considering the reading skills of the target people, as well as conducting a readability analysis of the statements to know whether they are clear enough to be understood. The most widelyused method is to employ a statistical, standardized readability metric that allows an objective evaluation. The Flesch Reading Ease Score (FRES) is a metric usually used both to evaluate school texts as well as legal documents (Flesch 1949). It gives an approximate score for the difficulty of a text. The Flesch metrics have been commonly accepted benchmarks for decades. It rates texts on a 100-point scale, where a higher score indicates to a simpler text. FRES computation depends on two sub-metrics (a) the average sentence length (b) the average number of syllables per word. Short words and sentences are easier to read and, therefore, produce a higher FRES. The Flesch Grade Level (FGL) determines the U.S. grade-school equivalency level of a text and is also based on the previous two sub-metrics. The metrics can be computed as follows:

Table 8 Rule 6 tablesReference of rule: $O_{4,6,7,8}: C_{16} \wedge (C_{10} \vee C_{15} \vee C_{17} \vee C_{18})$

Reference	7-2, 7-4
O_4	Personnel shall take all necessary precautions to secure confidential information.
O_6	Personnel must not demand any information not-relating to their work
O_7	Tadawul shall maintain the confidentiality of the information
O_8	Tadawul's Compliance Committee shall keep all disclosed information
C_{10}	Personnel shall take all necessary precautions to secure confidential information.
C_{15}	Personnel must not demand any information
C_{16}	Information is related to personnel work
C_{17}	Tadawul shall maintain the confidentiality of the information
C_{18}	Tadawul's Compliance Committee shall keep all disclosed information

Initial record of rule

1	Subject	Personnel
2	Object	Information
3	Action	Take or demand
5	Purpose	To prevent any leakage of confidential or internal information.

Extended record of rule

Paragraph	Property	Value
7-2	Subject	Who shall take all necessary precautions to secure information (C_{10})
7-4	Subject	Who must not demand any information (C_{15})
7-5	Subject	Who shall maintain the information (C_{17})
16	Subject	Who shall keep all information (C_{18})
7-2	Object	Which personnel shall take all necessary precautions to secure (C_{10})
7-5	Object	Which Tadawul shall maintain (C_{17})
16	Object	Which Tadawul's Compliance Committee shall keep (C_{18})
7-4	Object	What must not the personnel be demanded (C_{15})
7-2	Action	What the personnel shall do to secure information (C_{10})
7-4	Action	What the personnel must not do with information (C_{15})

It shows the considered tables of Rule 6 (i.e., Obligation $O_{4,6,7,8}$): (1) Reference of rule, (2) Initial record of rule, and (3) Extended record of rule

$$FRES = 206.835 - 84.6 \times \frac{\text{total syllables}}{\text{total words}} - 1.015 \times \frac{\text{total words}}{\text{total sentences}} \quad (1)$$

$$FGL = (0.39 \times \text{Average sentence length(in words)}) + (11.8 \times \text{Average number of syllables per word}) - 15.59 \quad (2)$$

According to Flesch (1979), FRES scores can be interpreted as shown in Table 10:

Table 9 Rule 7 tables

Reference of rule: $O_5: C_{14} \wedge (C_{11} \vee C_{12} \vee C_{13})$		
<hr/>		
Reference	7-3	
O_5	Personnel shall comply with specific policies at the end of service	
C_{11}	Personnel must refrain from disclosing confidential information	
C_{12}	Personnel must stop using confidential information	
C_{13}	Personnel must comply with the code of Law Practice	
C_{14}	Personnel are at the end of service	
<hr/>		
Initial record of rule		
<hr/>		
1	Subject	Personnel
2	Object	Disclosing or using information
3	Object	Code of law practice
4	Action	Comply
5	Purpose	To keep the internal information confidential after the personnel end of service
<hr/>		
Extended record of rule		
<hr/>		
Paragraph	Property	Value
<hr/>		
7-3-1	Subject	Who must refrain from disclosing information at the end of service (C_{11})
7-3-1	Subject	Who must stop using confidential information at the end of service (C_{12})
7-3-2	Subject	Who must comply with the code of Law Practice in respect of legal cases or litigation (C_{13})
7-3-1	Object	Which the personnel must refrain from disclosing or using. (C_{11})
7-3-2	Object	Which the personnel must comply with. (C_{13})
7-3-2	Action	What the personnel must do with the code of Law Practice (C_{13})

It shows the considered tables of Rule 7 (i.e., obligation O_5): (1) Reference of Rule, (2) Initial record of rule, and (3) Extended record of rule

Table 10 Interpretation of FRES scores

Score	School level	Notes
90.0–100.0	5th grade	Very easy to read
80.0–90.0	6th grade	Easy to read
70.0–80.0	7th grade	Fairly easy to read
60.0–70.0	8th and 9th grade	Plain English
50.0–60.0	10th to 12th grade	Fairly difficult to read
30.0–50.0	College	Difficult to read
0.0–30.0	College graduate	Very difficult to read

These tests are bundled with several word processing programs and services. We used Microsoft Office Word, a well-known word processing, to find the FRES and FGL scores. Accordingly, it is found the FRES score to be 16.6, which is interpreted as ‘Very difficult to read and best understood by university graduates’. We ignored

Fig. 1 Some statistics about the current state of ICT sector in Saudi Arabia (Communications and IT Commission 2014)

the FGL score because it is specialized for the U.S. grade level. The resultant score differs from that of financial regulations in developed countries. For example, the average FRES and FGL of financial policies of seven U.S. banks were 33.1 and 14.1, respectively, which were interpreted as ‘Difficult to read and best understood by university’ (Antón et al. 2004). The education level statistics for the adult U.S. population of Internet users was employed rather than that of the general population. In contrast, Tadawul’s readability score is low, though the high usage and government subsidization for technology in Saudi Arabia (Ebad 2016). Figure 1 shows some statistics that state that 95% of the Saudi organizations including governmental establishments, corporates, and educational institutes use computers (i.e., PCs, laptops, and tablets), and 64% of them use e-services (e.g., e-government, e-learning, e-banking, e-payment, and online shopping) (Communications and IT Commission 2014). A potential explanation for this low score might not strongly relate to the usage of technology but links to the regulations’ language. These regulations were written with the natural language of the Tadawul’s personnel (i.e., Arabic) which is the official language of the Saudi Stock Exchange. The English version that we studied herein is the official translation of the Arabic text. Accordingly, if there is a misunderstanding for any Tadawul’s regulation, the Arabic text would be considered. Unfortunately, we cannot calculate the above readability scores with Arabic text. Up to the best knowledge, this feature is not supported by the considered programs or tools. In general, shorter Tadawul’s regulations (e.g., Article 7-3-3) do not give additional information, but on average, they are no easier to read than their longer counterparts (e.g., Article 7-1).

7 Limitations and Contradictions

Transformation of the legal text into logical elements still is a problem that must be addressed by researchers attempting to apply automated reasoning to data usage. Full automation in our context is not easy because the logical consequences in FOPL are semi-decidable⁴ (Crick 2009). Full automation can only be applied to a decidable subset of FOPL using logic programming systems such as Prolog. The

⁴ In semi-decidable systems, there is no effective procedure that, given sentences A and B, always correctly decides whether A logically implies B.

automation problem is a limitation that we noticed in the Breaux and Antón approach, which has not been validated mathematically using existing software tools. In general, transformation of the legal text into logical elements is still a problem that must be addressed by researchers attempting to apply automated reasoning to data usage. As we mentioned in Sect. 2, it is premature to automate the Breaux and Antón approach which is currently performed manually unless we are able to apply it beyond healthcare context which is made in this research. The other limitation comes from the use of English words that may lead to vagueness with other words, for example “shall” word (in Article 6-2, 7-1, 7-2, 7-5, and 16) and “must” word (in Article 7-3-1, 7-3-2, 7-4) as both words require a sense of commitment. Any contradiction could bind the study’s reliability (Yin 2013). In particular, we only identify trivial contradictions by observing negation in semantic models, as in the case of R_1 , O_2 , and O_{4b} . To reinforce our study’s reliability, investigator triangulation has been considered as we mentioned in Sect. 3. We can also provide copies of materials used in our study for other researchers interested in repeating it.

8 Conclusion and Future Work

This paper has engaged with the debate on formalizing security requirements found at a financial information system in Saudi Arabia, by applying concepts of Breaux and Antón approach as a conceptual basis. The approach mainly depends on a semantic parameterization process that converts natural language descriptions into first-order predicate logic. To this end, we formalize the articles related with personnel information security from the code of conduct of Saudi stock exchange (Tadawul) in Saudi Arabia, the largest oil producer worldwide. Security in Saudi Arabia is an issue because of the high-income Saudi economy. We also used readability analysis of Tadawul’s regulations based on standard metrics. As a result of the case study, we extract two rights, eight obligations, eighteen constraints, seven rules, and several rule tables. Additionally, most of Tadawul’s security regulations considerably need more reading skills than just usage of the ICT services. Still, technology is relatively new and legislators are slow to agree with standards. To our knowledge, this work is an early, novel attempt to comprehensively formalize an entire text from financial regulations. The results of our formalization are expected to benefit regulators, legislators, policy makers, and information system administrators/developers by focusing their attention on those natural language policy semantics that are implementable in software systems. Moreover, the paper has reported that the Breaux and Antón approach is generalizable to different domains/countries. It is not simple for software engineers to ensure that their systems are compliant with all new legal requirements without stifling innovation. In future plans, more work is needed to address the automation process mentioned in the previous section using a hypothetical example of a legal document. This, which is in-progress, would be done by developing an automatic Breaux and Antón approach-based tool.

Appendix A: Code of Conduct

Code of Conduct for The Personnel of Saudi Stock Exchange Company (Tadawul) approved by virtue of the Resolution of the Capital Market Authority Council No. 3-20-2010 Dated 27/8/1431 H. Corresponding to 8/8/2010 G.

Article One: Foreword

The Saudi Stock Exchange Company (Tadawul) is committed to have its Personnel bound to a code of conduct that is consistent with best professional practices that can be harmonized with the distinctive characteristic of Tadawul in order to have a highly ethical and professional working atmosphere for its Personnel. Tadawul shall ensure that its Personnel is committed to abide by the terms of the code of conduct to sustain its credibility, efficiency, and competence of its business and activities and to maintain its reputation in the capital market.

Article Two: Definitions

1. The Terms: terms of the code of conduct for the Personnel of Tadawul.
2. Tadawul: the Saudi Stock Exchange Company incorporated by virtue of the Royal Decree N.(M/15) dated 1/3/1428 H.
3. Personnel: staff, consultants and staff under specified or unspecified terms of contracts or any of the staff working directly or indirectly at Tadawul, including staff who are working as part-timers or pursuant to sub-contracts.
4. Protective Measures: to maintain confidentiality and safekeeping of the internal information which may be accessed by Personnel in connection with the performance of their work as well as those policies that aimed to ensure that such information will not be accessible except to those authorized personnel and not disclosed to any other persons.
5. Conflict of Interests: any impact on Tadawul's interests, status, rights, business, decisions or reputation, with the material or moral interests of any of its staff, whether direct or indirect, current or future, or resulting from personal or commercial relationships.
6. The Relevant Parties: natural or juristic persons who have a direct or indirect relationship with Tadawul, including professional, financial, and commercial relationships. This includes listed companies or those seeking to be listed in the Capital Market, advisers, financial analysts, consultants, members, suppliers, contractors, clients, or staff of any of the aforementioned parties or investors in the Capital Market.
7. Confidential or Internal Information: any piece of information, data, number, statistic to which the public has no access that any of Tadawul's personnel may have access to by virtue of the nature of his/her work or in any other capacity, whether such piece of information, data, number or statistic is written, oral, electronic or otherwise, whether financial, administrative,

commercial, marketing, technical or any other information connected with Tadawul or with any of its Personnel, clients or contractors or connected with the Capital Market in general.

8. Minors: persons below eighteen years of age pursuant to the Hijra Calendar
9. Compliance Section: department or section of Compliance at Tadawul, pursuant to the powers granted herein by these Terms.
10. The Committee: The Audit Committee at Tadawul pursuant to the powers granted thereto by these Terms.
11. The Chairman: Chairman of Tadawul's Board or Vice-Chairman in case of Chairman's absence or in case of Chairman's delegation of powers to the Vice-Chairman.

Accessed Person: a person who has access to Confidential or Internal Information that is not accessible to the public, either through; a business relationship, or through any other capacity whatsoever, whether directly or indirectly.

Article Six: Working for Other Parties

1. Personnel are prohibited from practicing any other profession or business outside Tadawul, including the occupation of posts or functions in any company or with the government, public or private entities. Personnel are also prohibited from offering consultation to any other parties except after obtaining Tadawul's written approval.
2. Tadawul's CEO shall be prohibited from performing any other government or private work.

Article Seven: Confidentiality of Information

1. Personnel undertake at all times to comply with all Protective Measures that protect against the infiltration of information and to fully protect and safe keep Confidential or Internal Information and shall not disclose, announce or declare any such information to any other party unless it is officially or legally requested or prompted by the interest and nature of business of Tadawul.
2. Personnel shall take all necessary precautions to prevent any leakage of confidential or Internal Information. This includes making sure that they are not conspicuously displayed at the work area where others can have access thereto. They should also take all reasonable precautions for properly switching off their computers and safeguarding their user names and passwords and take precautions when sending or receiving information, whether through their computer or fax or any other means and not to take out any document whether hard copy or electronic copy of a confidential nature outside the head office of Tadawul.
3. At the end of their service, Personnel shall comply with the following:

1. They must refrain from disclosing and stop using any Confidential or Internal Information or any documents that are in his/her possession and shall return them to the management. In any event, returning any such documents or information or their destruction thereof shall not exempt Personnel from any obligation to maintain the non-disclosure of Confidential or Internal Information even after the end of the contractual relationship with Tadawul.
2. They must comply with the Code of Law Practice in respect of legal cases or litigation.
3. Personnel must not demand any information that has no relation to their work.
4. Tadawul shall maintain the confidentiality of the information pertaining to its personnel.
5. In addition to the administrative penalties which Tadawul is entitled to impose as a result of any breach to compliance with confidentiality obligation, Tadawul shall have the right to pursue any other legal proceedings/remedies as it may deem to be appropriate against any of its Personnel in the event of their breach to any of their obligations provided herein including claiming from him/her any loss or compensation resulted from such breach of confidentiality.

Article Nine: Prohibition of Disclosure of Internal Information

Personnel are prohibited from disclosing any internal information to any party whatsoever.

Article Sixteen: Responsibility

Tadawul's Compliance Section or the Committee—each according to the powers granted thereof, under these Terms, shall be the authority with which the application of the Terms of code of conduct is vested, and which shall keep all disclosed information. Each of the Compliance Section and the Committee pursuant to the powers granted to them, shall identify all violations to these Terms and reply to any queries connected therewith.

References

- Antón AI, Earp JB, Bolchini D, He Q, Jensen C, Stufflebeam W (2004) The lack of clarity in financial privacy policies and the need for standardization. *IEEE Secur Priv* 2(2):36–45
- Bada AO, Madon S (2006) Enhancing human resource development through information and communications technology [Editorial]. *Inf Technol Dev* 12(3):179–183

- Baker EW (2014) A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan. *Inf Technol Dev* 20(2):122–139
- Beckers K (2012) Comparing privacy requirements engineering approaches. In: The 7th international conference on availability, reliability, and security, Prague, pp 574–581
- Ben-David Y, Hasan S, Pal J, Vallentin M, Panjwani S, Brewer E (2011) Computing security in the developing world. In: the 5th ACM workshop on networked systems for developing regions, ACM Press, New York, pp 39–44
- Boetticher GD (2006) Teaching financial data mining using stocks and futures contracts. *J Syst Cybern Inf* 3(3):26–32
- Breaux T (2014) Privacy requirements in an age of increase sharing. *IEEE Softw* 31(5):24–27
- Breaux TD, Antón AI (2008) Analyzing regulatory rules for privacy and security requirements. *IEEE Trans Softw Eng* 34:5–20
- Breaux TD, Vail MW, Antón AI (2006) Towards regulatory compliance: extracting rights and obligations to align requirements with regulation. In: the 14th IEEE international requirements engineering conference, Los Alamitos, CA, pp 49–58
- Breaux TD (2009) Legal requirements acquisition for the specification of legally compliant information systems. Dissertation. North Carolina State University, Raleigh (NC), US
- Brodie CA, Karat C, Karat J (2006) An empirical study of natural language parsing of privacy policy rules using the SPARCLE policy workbench. In: Symposium on usable privacy and security, Pittsburgh. ACM Press, New York
- Campbell K, Gordon L, Loeb M, Zhou L (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J Comput Secur* 11:431–448
- Cheng BHC, Atlee JM (2007) Research directions in requirements engineering. In: Conference on future of software engineering, Los Alamitos, CA, pp 285–303
- Communications and IT Commission (2014) Establishment report (corporate, government and education) ICT survey results. <http://www.citc.gov.sa/English/Reportsandstudies/Studies/Documents/IT021E-PublicReportForEstab.pdf>. Accessed 21 June 2017
- Crick T (2009) Superoptimisation: provably optimal code generation using answer set programming. Dissertation. University of Bath, UK
- Ebad SA, Jaha ES, Al-Qadhi MA (2016) Analyzing privacy requirements: a case study of healthcare in Saudi Arabia. *Inf Health Soc Care* 41(1):47–63
- Ebad SA (2016) Influencing factors for IT software project failures in developing countries—a critical literature survey. *J Softw* 11(11):1145–1153
- Flesch R (1949) The art of readable writing. Harper & Row Publishers, New York
- Flesch R (1979) How to write plain English: a book for lawyers and consumers. Harpercollins, New York
- Glaser BC, Strauss AL (1967) The discovery of grounded theory. Aldine Publishing, Chicago
- Hohfeld WN (1913) Some fundamental legal conceptions as applied in judicial reasoning. *Yale Law J* 23(1):16–59
- Jakobsen S (2013) MENA and Egypt are like an upside down Europe Arab News. <http://www.arabnews.com/news/462245>. Accessed 21 June 2017
- Jensen J, Tøndel IA, Andresen H (2009) Reusable security requirements for healthcare applications. In: The international conference on availability, reliability and security, Fukuoka, Japan, pp 380–385
- Jorshari FZ, Mouratidis H, Islam S (2011) Extracting security requirements from relevant laws and regulations. In: The 6th international conference on research challenges in information science, Valencia, Spain
- Kargl F, Lawrence L, Fischer M, Lim YY (2008) Security, privacy and legal issues in pervasive eHealth monitoring systems. In: the 7th international conference on mobile business, Barcelona
- Kiyavitskaya N, Zeni N, Breaux TD, Antón AI, Cordy JR, Mich L, Mylopoulos J (2007) Extracting rights and obligations from regulations: toward a tool-supported process. In: The 22nd IEEE/ACM international conference on automated software engineering, Atlanta, GA, US
- Massey AI, Otto PN, Hayward LJ, Antón AI (2010) Evaluating existing security and privacy requirements for legal compliance. *J Requir Eng* 15:119–137
- Maxwell JC, Antón AI, Swire P, Riaz M, McCraw CM (2012) A legal cross-references taxonomy for reasoning about compliance requirements. *J Requir Eng* 17:99–115
- May MJ, Gunter CA, Lee I (2006) Privacy APIs: access control techniques to analyze and verify legal privacy policies. In: the 19th IEEE workshop on computer security foundations, Los Alamitos, CA

- Merdad HJ (2012) Two essays in Islamic finance and investment. Dissertation. University of New Orleans, New Orleans, Louisiana, US
- Mouratidis H (2004) A security oriented approach in the development of multiagent systems: applied to the management of the health and social care needs of older people in England. Dissertation. University of Sheffield, UK
- Osei-Bryson KM, Vogel D (2014) Special issue on cyber-security for development [Editorial]. *Inf Technol Dev* 20(2):93–95
- Otto PN, Antón AI (2007) Addressing legal requirements in requirements engineering. In: The 15th IEEE international requirements engineering conference, Delhi. Los Alamitos, CA
- Runeson P, Höst M (2009) Guidelines for conducting and reporting case study research in software engineering. *Empir Softw Eng* 14(2):131–164
- Soldatkin V, Astrasheuskaya N (2011) Saudi Arabia to overtake Russia as top oil producer-IEA, Reuters. Retrieved from: <http://www.reuters.com/article/russia-energy-ia-idUSL6E7M93XT20111109>. Accessed 21 June 2017
- Sommerville I (2015) Software engineering, 10th edn. Pearson Education Limited, London
- Stamey JW, Rossi RA (2009) Automatically identifying relations in privacy policies. In: the 27th ACM international conference on design of communication, Bloomington, New York, US
- Wu R, Ahn G-J, Hu H (2012) Towards HIPAA-compliant healthcare systems. In: The 2nd ACM SIGHT international health informatics symposium, Miami. New York
- Yin RK (2013) Case study research: design and methods, 5th edn. Sage Publications, USA
- Zafar H, Ko MS, Osei-Bryson KM (2012) Financial impact of information security breaches on breached firms and their non-breached competitors. *Inf Resour Manag J* 25(1):21–37
- Zheng Y (2009) Different spaces for e-development: what can we learn from the capability approach? *Inf Technol Dev* 15(2):66–82