An Experience Report of Improving Business Process Compliance Using Security Risk-Oriented Patterns

Mari-Liis Alaküla, Raimundas Matulevičius

An Experience Report of Improving Business Process Compliance using Security Risk-oriented Patterns

Mari-Liis Alaküla[1,2] and Raimundas Matulevičius[2]

[1] INSLY OÜ, Tallinn, Estonia
[2] Institute of Computer Science, University of Tartu, Tartu, Estonia
mariliis@gmx.com, rma@ut.ee

Abstract. Nowadays enterprises are searching the efficient compliance management method. Being compliant could potentially help capturing the most important information, using practice and existing process solutions; thus reducing the management effort and cost. When it comes to the security compliance management, it means treating and reducing the security risks to the acceptable level and employing the validated and cost effective security countermeasures. However, the typical question that small and medium enterprises face, is on how to achieve the security compliance in the efficient way. In this paper we report on our experience to use the security risk-oriented patterns to improve business processes of the insurance brokerage. The analysed case showed the major steps to apply the regulatory standard to check compliance, as well as the major procedures needed to improve the business process compliance. The lessons learnt highlight some method guidelines toward compliance management and suggest needed improvement directions for the application of the security risk-oriented patterns.

Keywords: Business process models and notations, standards and regulations, security modelling, security patterns.

1 Introduction

Business process management (BPM) is an instrument for enterprises to manage their activities in a holistic manner and to ensure consistent business outcomes that add value both to the enterprise and its customers [7]. This also means that the availability, integrity and confidentiality of valuable business assets (including data, processes, policies, etc.) need to be protected from intentional risks.

One way to achieve a certain security level within business processes is through compliance management. "*Compliance is a set of activities an enterprise does to ensure that its core business does not violate relevant regulations*" [10]. There exist a number of security regulations in terms of international and national standards (e.g., ISO/IEC 27001 [11], NIST SP 800-39 [15], Base III [4], IT-Grundschutz [12] and etc.); however the way to achieve business process compliance with the regulations remains rather labour intensive activity.

In this paper we analyse *how security patterns could help achieving business process compliance*. More specifically we consider how business processes

(represented in business process model and notation, a.k.a. BPMN) of some insurance company comply with the ISO/IEC 27001:2013 [11], standard before and after the security risk-oriented patterns (SRPs) [1] are applied and security constraints introduced to the business process. On one hand we have selected the ISO/IEC 27001:2013 standard because of its simplicity and popularity among enterprises; but we believe that other regulations or standards could be used instead. On the other hand we use the SRPs because they are expressed in BPMN and explicitly differentiate between the valuable assets, security risks, and risk countermeasures.

The lessons learnt are threefold. Firstly, we have observed that SRPs could contribute to the business process compliance. Secondly, we have learnt about the steps needed to pre-process business process models before applying SRPs. Finally, we have observed few SRP limitations, thus this results in the potential improvements to the SRP application process.

The remaining of the paper is structured as follows: in Section 2 we present the prerequisites of the case study. Section 3 discusses how compliance of the business process and application of the security risk-oriented patterns was performed. In Section 4 we survey a related work. Finally, in Section 5 we discuss the lessons learnt and present some future work.

2 Prerequisites

2.1 ISO/IEC 27001:2013

The ISO/IEC 27001:2013 standard is a specification for an information security management system [11]. It presents requirements for managing sensitive organisation's information by applying risk management, risk assessment and risk treatment means. The major parts of the standard include guidance on understanding context of organisation, leadership, planning, support, operation performance evaluation and improvement activities. Important part of the standard is its appendix, which provides a checklist of objectives and controls (although organisation could also choose other controls according to its preferences). The objectives and controls could be potentially combined to develop organisation's treatment plan to respond to security risks.

In this paper we consider how organisation's business processes could be estimated and improved to become compliant to the ISO/IEC objectives and controls listed in its appendix.

2.2 Security Risk-oriented Patterns

"A *security pattern* describes a particular *recurring security problem* that arises in a *specific security context* and presents a well-proven generic scheme for a *security solution*" [23]. Table 1 presents a list of security risk-oriented patterns (SRP) [1], developed using domain model [6] for information system security risk management (ISSRM). This domain model differentiates between three major concept groups –

asset-related concepts, *risk-related concepts* and *risk treatment-related concepts*. Thus, based on this structure each security risk-oriented pattern consists of the specific security context (expressed using the asset-related concepts), recurring security problem (analysed in terms of the security risk-related concepts) and suggests the security countermeasures (presented through the security risk-treatment concepts).

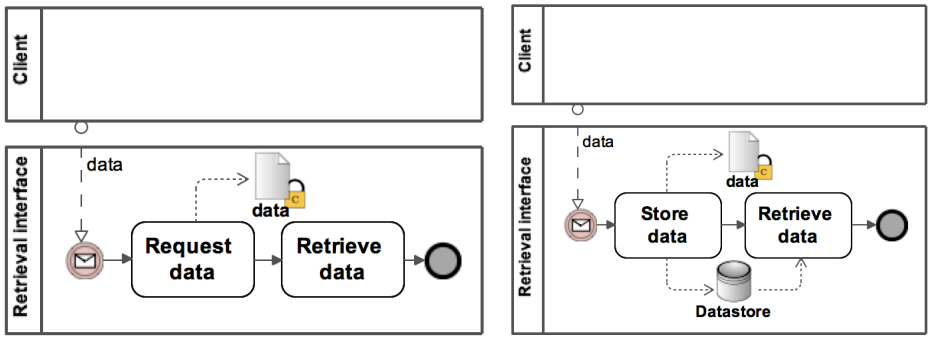
Table 1: Security Risk-oriented Patterns

Security Risk-oriented Pattern	**Description**
SRP.1 Securing data from unauthorized access	This pattern describes how to secure confidential data from unauthorized access by people or devices. The pattern is based on implementation of access control where (stakeholder or device) roles and data are classified to levels of trust and sensitivity.
SRP.2 Securing data that flow between the business entities.	This pattern addresses the electronic transmission of data between two entities, i.e., client (where data is submitted) and business (where data is used).
SRP.3 Securing business activity after data is submitted.	This pattern secures the business activity, which is carried out after data has been submitted, and where integrity and availability have to be ensured.
SRP.4 Securing business services against DoS attacks.	This pattern addresses the Denial of Service (DoS) attacks and their protection strategies. It helps to protect the business assets in order to guarantee its availability.
SRP.5 Securing data stored in/retrieved from the data store.	The main goal of this pattern is to prevent the leaking of confidential data from the enterprise's data store.

For example, *SRP.1 Securing data from unauthorized access* describes how to secure confidential data from access by unauthorised people or devices. In Fig. 1, a client requests data (a confidential business asset). In response to this request the data are retrieved (using the retrieval interface characterized as the IS asset) and provided to the user. The problem arises if the retrieval of the confidential data is allowed to any user (independently whether s/he is malicious or not) without checking his or her access permissions to the data. Such a risk event would lead to the disclosure of the confidential data; it might provoke that these data would be sent to the business competitors, thus, compromising the business itself. To reduce such risk, countermeasures to *check for the access rights* should be implemented.

Another example is *SRP.5 Securing data stored in/retrieved from the data store* (see Fig. 1). It ensures the data confidentiality stored at the data-store against insiders' attack (i.e., malicious administrators or malware that infects data-store). There exists a retrieval interface (i.e., IS asset), which helps clients (*i*) to store the client's confidential data (i.e., business asset) in the data-store and (*ii*) to retrieve them when needed. An attacker characterised as malicious insider is able to access the data-store and also retrieve data directly from it. If the retrieval interface (also including the queries to the database) is designed in a way that data are saved/retrieved in a plain-text format, the attacker could view the data, thus negating the data confidentiality. To reduce this security risk, one of the possible mechanisms is access control at the data-store level.

We will illustrate how *SRP.1* and *SRP.5* are applied to analyse some business process model in Section 3.



SRP.1 Securing data from unauthorized access (security context)

SRP.5 Securing data stored in/retrieved from the data store (security context)

Fig. 1. Security Risk-oriented patterns (illustrated in the latter discussion)

2.3 Description of Business Process Model

An information system, used in our context, was developed two years ago with the aim to cut labour costs of insurance brokerage by automating the business processes. By beginning of this study the system was already developed as the real-life application. But our first task was to model explicitly the business processes supported by the application. The created models were briefly reviewed by the project managers who confirmed the logics of the modelled processes.

In Fig. 2 we present an extract of the value chain where the main value, *offer*, is created as a result of consecutive steps. The process begins with *adding customer data* to the offer form, after which the *product* and *offer object* data are added, too. Product data describes the coverage information of various insurance services types (e.g., travel insurance or health insurance related excess amounts and deductibles), while object data defines the characteristics of the insurable body (e.g., a person or a vehicle). Next, *offer quotes* from different insurers are added to the offer form according to the product and object data. The last step is *acceptance of the offer*. The offer form is sent to the customer to his acceptance or decline. In case of acceptance, the customer chooses the relevant quote to purchase.

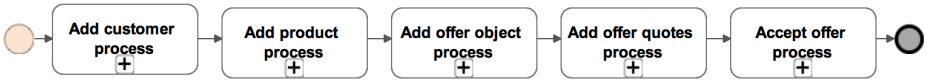


Fig. 2. Value Chain

In Fig. 3 we expand process of *Accept offer process*. The diagram includes three pools, presenting *Broker*, *Customer* (both human participants) and the *Insurance brokerage system* (a software system used by *Broker* and *Customer*). This insurance brokerage *system* is used to manage the *Offer* information in this example. Here the *Offer* is not described in detail in Fig. 3, but is characterized by *customer data*, *relevant quotes*, *offer status* and the *selected quote*. In order for this business process to be completed both *Broker* and *Customer* must collaborate while performing various

tasks: e.g., *Broker* prepares of the offer. After, the *Offer* is e-mailed to the *Customer*, *Broker* is able to checks Offer status (e.g., to be sure that *Offer* is emailed). The *Customer* could initiate the response, which indicates acceptance or rejection of the *Offer*. If response is not sent after some time, the *Offer* is cancelled.

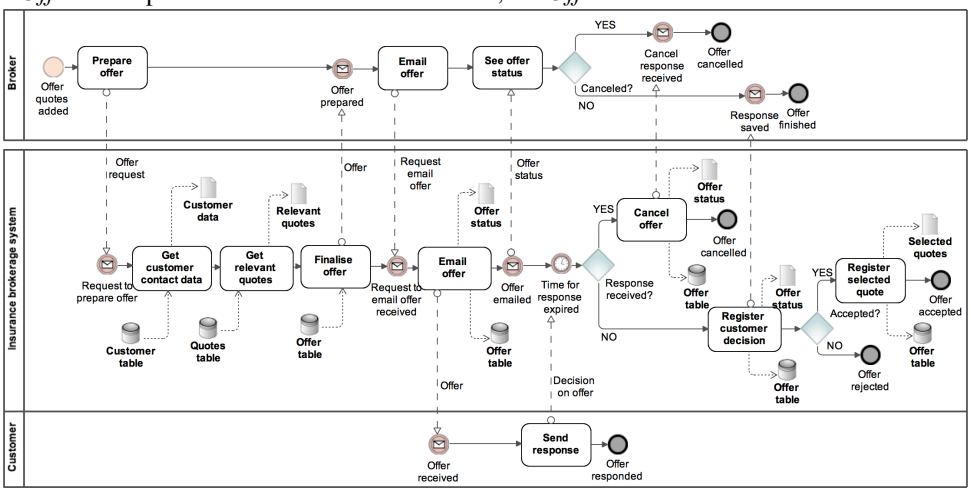


Fig. 3. Business Process Model of *Accept Offer Process*

3 Checking and Improving Business Process Compliance

The approach to check and improve business process compliance to the ISO 27001 standard is illustrated in Fig. 4. Firstly, we evaluated the level of compliance of the considered business process. We confronted the model to the ISO 27001:2013 standard. In Step 2 the security risk-oriented patterns are applied to derive security requirements and to introduce security constraints to the business process model. In the third step the business process compliance is checked again. Finally, in Step 4 we compare the compliance results of both compliance checks (Step 1 and Step 2) and draw conclusion on compliance change.

3.1 Evaluate Initial Model Compliance

Evaluation of the initial business process compliance consists of two steps: (*i*) instantiation of the standard to the considered problem, and (*ii*) checking how the business process visualised in Fig. 3 model complies the requirements described in the standard.

Instantiate standard. The ISO/IEC 27001:2013 standard describes a generic situation [14], which potentially could be adapted to various specific cases. For example, in Table 2 (columns 0 to 2) we list the *A.9.4.1 Information access restriction* control. Firstly, this control specifies at least two different concerns: one for access to

information and another for access to application systems. Secondly, it is important to understand what *information* is considered, and what is meant by the *application systems* in the given context. Following the case described in Section 2.3 we consider information, which is stored in the databases; this information consists of *Customer data*, *Relevant quotes*, *Offer status*, and *Selected quotes*. In our case the information system is *Insurance brokerage system*, which includes functions to manage the information; thus we need to consider the access to business processes such as *Get customer contact data*, *Get relevant quotes*, *Email offer*, *Cancel offer*, *Register customer decision*, and *Register selected quotes*. The refinement of the *A.9.4.1* control is presented in Table 2 as listed in columns 3 and 4.

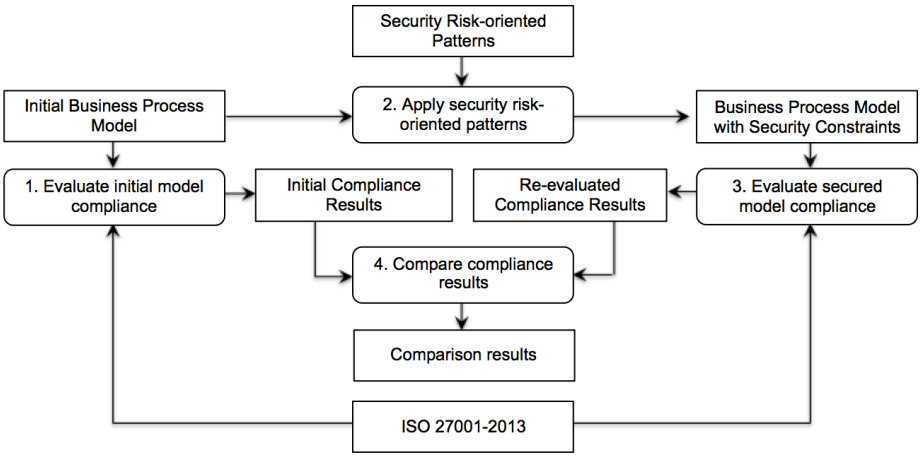


Fig. 4. Approach to Check and to Improve Compliance

Similarly, all standard controls need to be refined. For instance, *A.13.2.1* is another example. As illustrated in Table 2 it is refined to three requirements – regarding *policies*, *procedures* and *controls*.

Check compliance. Once the standard is initialised to the considered case, it becomes possible to analyse the business process compliance to the instantiated requirements. In our case we use a simple three-measure scale: "*Yes*" stands to indicate compliance; "*No*" – there is no compliance; and "*NR*" – the standard requirement is not relevant (NR) in the analysed case.

In Table 2, column 5, we present compliance assessment of business process. The business process model does not imply any access control policy; therefore requirements *A.9.4.1.i* and *A.9.4.1.ii* are given "No" score. Similarly, the model does not indicate any transfer policies or procedures, so *A.13.2.1.i* and *A.13.2.1.ii* also result in "No" score. Finally, as indicated in [3], the language used to visualise business process (namely, BPMN – business process model and notation) does not contain means to present controls; therefore *A.13.2.1.iii* is graded as "NR".

Table 2. Instantiating the ISO27001 Standard

Name of the control	Original standard		Instantiated standard		Compliance
	Number	Description	Number	Description	
0	1	2	3	4	5
Information access restriction	*A.9.4.1*	Access to *information* and *application system functions* shall be restricted in accordance with the access control policy.	*A.9.4.1.i*	Access to *Customer data*, *Relevant quotes*, *Offer status*, and *Selected quotes* shall be restricted in accordance with the access control policy.	No
			A.9.4.1.ii	Access to *Get customer contact data*, *Get relevant quotes*, *Email offer*, *Cancel offer*, *Register customer decision*, and *Register selected quotes* shall be restricted in accordance with the access control policy.	No
Information transfer policies and procedures	*A.13.2.1*	Formal transfer *policies*, *procedures* and *controls* shall be in place to protect the transfer of information through the use of all types of communication facilities.	*A.13.2.1.i*	Formal transfer *policies* shall be in place to protect the transfer of *Offer request*, *Offer*, *Request email offer*, *Offer status*, and *Decision on offer* through the use of all types of communication facilities.	No
			A.13.2.1.ii	Formal transfer *procedures* shall be in place to protect the transfer of *Offer request*, *Offer*, *Request email offer*, *Offer status*, and *Decision on offer* through the use of all types of communication facilities.	No
			A.13.2.1.iii	Formal transfer *controls* shall be in place to protect the transfer of *Offer request*, *Offer*, *Request email offer*, *Offer status*, and *Decision on offer* through the use of all types of communication facilities.	NR

3.2 Apply Security Risk-oriented Patterns

Application of security risk-oriented patterns consists of two steps: (*i*) security requirements derivation, and (*ii*) introduction of the security constraints to the business process model.

Security requirements derivation, as illustrated in [2], [13], consists of three steps. Firstly, one needs to *identify pattern occurrences*. The security context presentation of the security risk-oriented pattern (see Fig. 1) is used to analyse business process model and to identify potential occurrences of the pattern. We observe six occurrences of *SRP.1* and seven occurrences of *SRP.5* in Fig. 3.

Secondly, one needs to *extract security model* from the business process model. For instance, security model created when applying *SRP.1* is given in Fig. 5, and *SRP.5* - in Fig. 6. Extraction of security models for each pattern is performed followed pattern specific guidelines [2].

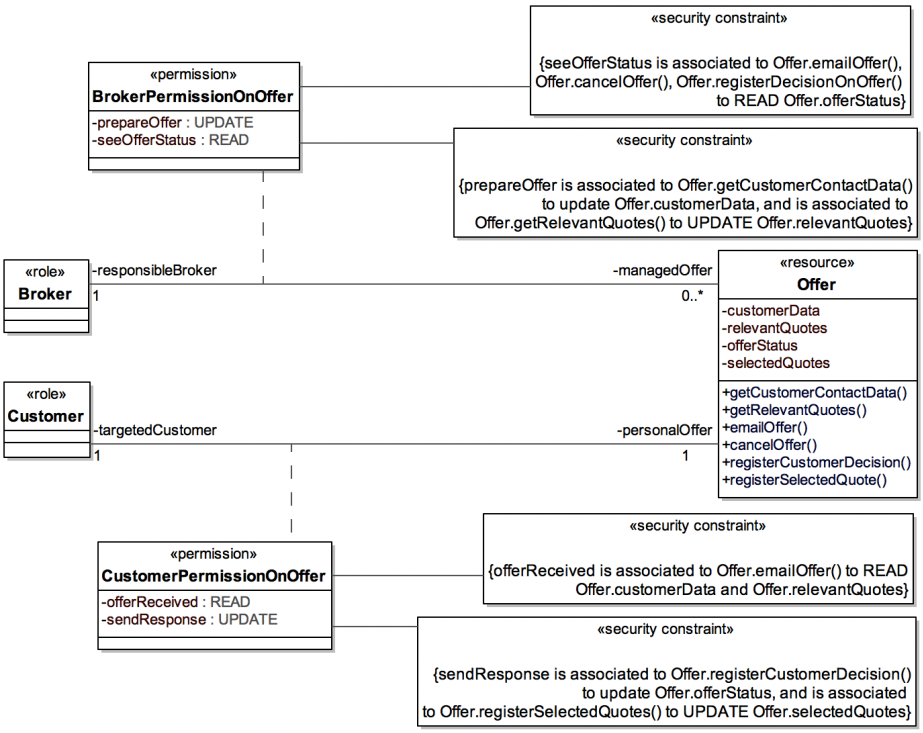


Fig. 5. Security model derived using *SRP.1*

For example, when applying *SRP.1*, one needs to (*i*) identify secured resource (e.g., *Offer*, determined by analysing the value chain, i.e., Fig. 2); (*ii*) identify roles (e.g., *Broker* and *Customer*); (*iii*) assign users (e.g., organisation's employees who play the identified roles); (*iv*) identify secured operations (e.g., *Get customer contact*

data, *Get relevant quotes*, *Email offer*, *Cancel offer*, *Register customer decision*, and *Register selected quotes*); and (*v*) assign permissions (e.g., *Broker permissions on Offer* and *Customer permissions on Offer*). These extracted data is used to create the security model (i.e., Fig. 5), which typically is graphical structure assigned to each pattern.

Finally, security requirements are derived from security models and explicitly documented. In Table 3 we list security requirements derived when applying *SRP.1* and *SRP.5*. These security requirements indicate that *Broker* and *Customer* have different permissions to the functionality of *Insurance brokerage system*, as well as different permissions to update and retrieve information to/from the data-stores (i.e., tables) used in the *Insurance brokerage system*.

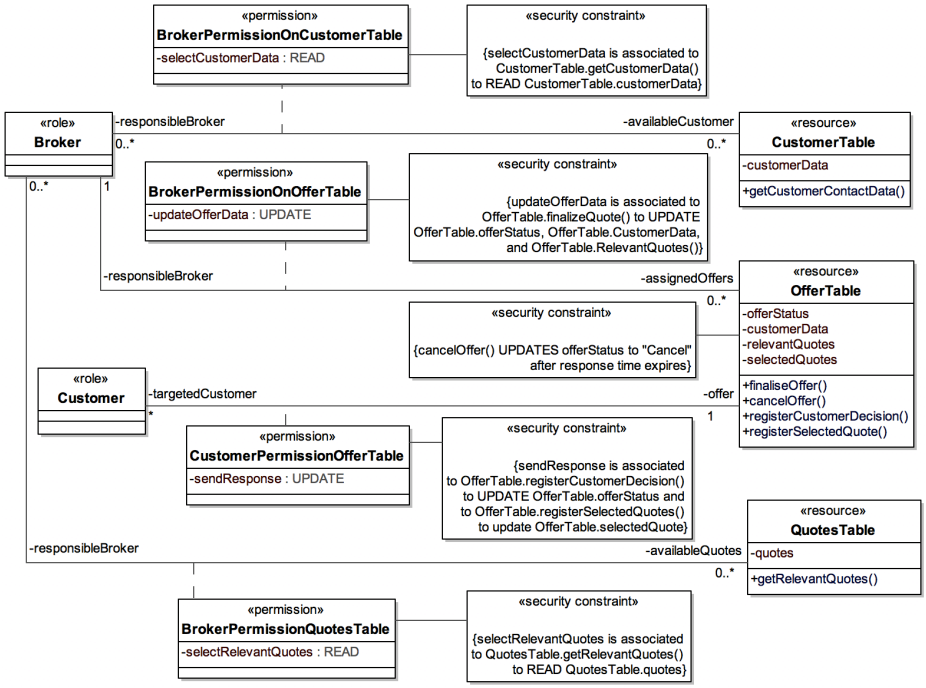


Fig. 6. Security model derived using *SRP.5*

Introduction of the security constraints to the business process model. Fig. 7 presents an extract of the business process model from Fig. 3. The security requirements derived in the previous steps are introduced as the security constraints to the business activities. This means that in order to execute the activity (e.g., *Get customer contact data*), it should be checked (*i*) whether the user assigned to the role *Broker* is trying to execute this activity (i.e., SReq.1.1.1) and guarantee that his role is *Broker* and is allowed to read *Customer data* from the *Customer table* (i.e., SReq5.1).

It is also important to note that both SReq.1.1.1 and SReq.5.1 should be respected in the given situation. This could be explained by the case, for example, to avoid the

unauthorised access of the *Customer table* (by the user or software, which does not have the role of *Broker*, i.e., violation of SReq5.1) while *Broker* is performing task *Get customer contact data*. In other words, the security requirements are introduced to the business process model and the *runtime* constraints, which must be respected when executing the business process.

Table 3. Derived Security Requirements

Requirement resulting from ***SRP.1*** application
SReq.1.1: Only *Broker* should ***update*** offer's *Customer data* and *Relevant quotes*. SReq.1.1.1: *Broker* should perform *Get customer contact data*. SReq.1.1.2: *Broker* should perform *Get relevant quotes*. SReq.1.2: Only *Broker* should ***read*** offer's *Offer status*. SReq.1.2.1: *Broker* should view *Offer status* after operation *Email offer*. SReq.1.2.2: *Broker* should view *Offer status* after operation *Cancel offer*. SReq.1.2.3: *Broker* should view *Offer status* after operation *Register customer decision*. SReq.1.3: Only *Customer* should ***read*** offer's *Customer data* and *Relevant quotes*. SReq.1.3.1: *Customer* should view *Customer data* and *Relevant quotes* after operation *Email offer*. SReq.1.4: Only *Customer* should ***update*** offer's *Offer status* and *Selected quotes*. SReq.1.4.1: By performing *Send response* task, *Customer* should invoke *Register customer decision*. SReq.1.4.2: By performing *Send response* task, *Customer* should invoke *Register selected quote* if *Offer status* is "Accepted".
Requirement resulting from ***SRP.5*** application
SReq.5.1: Only *Broker* should ***read*** *Customer data* from *Customer table*. SReq.5.2: Only *Broker* should ***read*** *Quotes* from *Quotes table*. SReq.5.3: Only *Broker* should ***update*** *Offer status*, *Customer data*, and *Relevant quotes* in *Offer table* with a single operation. SReq.5.4: Only *Customer* should invoke ***update*** of *Offer status* in *Offer table.*

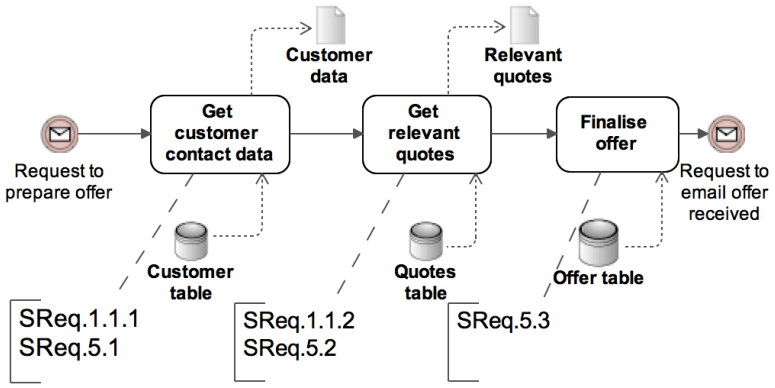


Fig. 7. Introduction of Security Constraints

3.3 Evaluate Secured Model Compliance and Compare Compliance Results

The instantiated standard and its requirements (see Section 3.1) are used to evaluate the secured business process. The evaluation is presented in Table 4, column 6. Hence, after applying the *SRP.1* and *SRP.5* we could observe that access control policy (in terms of the security models, security requirements, and security constraints introduced to the business process model) is defined both (*i*) to restrict access to the business tasks (in terms of standard – application system functions) and (*ii*) to restrict access to data/information kept in data-stores (in terms of standard – information). Thus we assign to *A.9.4.1.i* and *A.9.4.1.ii* "Yes" score.

Business model compliance to other standard requirement (e.g., *A.13.2.1*) remains the same as in the in initial assessment. However, it could be noted that application of *SRP.2* would potentially result in business process compliance to *A.13.2.1.i* and *A.13.2.1.ii* requirements. This illustration did not take the *SRP.2* application into account, but in our actual analysis we have performed the *SRP.2* (and other pattern) application to reach the business process compliance.

Table 4. Comparison of two Compliance Assessment Results

Instantiated standard		Initial Model Compliance	Secured Model Compliance
Number	Description		
3	4	5	6
A.9.4.1.i	Access to *Customer data*, *Relevant quotes*, *Offer status*, and *Selected quotes* shall be restricted in accordance with the access control policy.	No	**Yes**
A.9.4.1.ii	Access to *Get customer contact data*, *Get relevant quotes*, *Email offer*, *Cancel offer*, *Register customer decision*, and *Register selected quotes* shall be restricted in accordance with the access control policy.	No	**Yes**
A.13.2.1.i	Formal transfer *policies* shall be in place to protect the transfer of *Offer request*, *Offer*, *Request email offer*, *Offer status*, and *Decision on offer* through the use of all types of communication facilities.	No	No
A.13.2.1.ii	Formal transfer *procedures* shall be in place to protect the transfer of *Offer request*, *Offer*, *Request email offer*, *Offer status*, and *Decision on offer* through the use of all types of communication facilities.	No	No
A.13.2.1.iii	Formal transfer *controls* shall be in place to protect the transfer of *Offer request*, *Offer*, *Request email offer*, *Offer status*, and *Decision on offer* through the use of all types of communication facilities.	NR	NR

4 Related Work

Different aspects of business process compliance management are rather extensively reported in literature. For instance, Papazoglou in [16] and El Kharbili *et al* in [8] propose some business process compliance management frameworks. Ramezani *et al* considers how to separate compliance management and business process management activities [17]. Elsewhere in [18] some means to organize and select compliance rules are presented. Schumm *et al* propose to achieve process compliance through reusable units of compliant processes [24]. This at some extend resembles to the use of the (security risk-oriented) patterns to identify process fragments where the needed compliance regulations are determined.

In [19], Sadiq and Governatory propose a methodology for business process compliance management by process design. The major steps include control directory management, where regulations and directives are interpreted following the considered domain (we perform similar activities described in Section 3.1). Another important step is control modelling and process model enrichment (which highly correspond to security requirements derivation and security constraint introduction as discussed in Section 3.2).

There exist few studies that concern the business process compliance with respect to the access control regulations. For instance, an approach for compliance validation of secure service composition is described in [5]. Here validation of the access control and separation of duty concerns is managed using some automated tool support. In [22], application controls are used to enrich business process models. The work specifically focuses on preventive controls patterns, detective control patterns and required activity patterns. In our study we not only consider the access control (e.g., *SRP.1* and *SRP.5*), but we extent the analysis to other concerns, like secure communication (e.g., *SRP.2*), secure data input (e.g., *SRP.3*), and secure operation after data input (e.g., *SRP.4*).

An approach to extract security requirements and introduce security policies is reported in [20]. Authors are using actor-goal modelling approach to understand the stakeholder requirements through their goals, interactions, information and authorisations. The extracted requirements are introduced as security annotations (i.e., in terms of security countermeasures) to the business process model. In comparison to [20] we use the security risk-oriented patterns represented in the same modelling language as the business model. In [20] model compliance is performed at the model (i.e., graphical) level; in our case this still remains a future work.

5 Discussion and Future Work

In the paper we report on our experience to apply the SRPs to the insurance business processes in order to determine security requirements and improve process compliance with the selected security regulations. In this section we discuss observed limitations and lessons learnt. We also highlight some future work.

5.1 Limitations

Our work contains few limitations and threats to validity. We acknowledge that it includes some degree of subjectivity regarding (*i*) selecting regulation standard; (*ii*) created business process models and (*iii*) application and interpretation of the security risk-oriented patterns.

Firstly, ISO/IEC 27001:2013 is rather popular standard to which many enterprises tend to certify to. We do not believe that the process (e.g., see Fig. 2) would change much or result in too much different outcome if we had selected another regulation standard. However, applying other regulation standards could potentially be a future work of this study. Secondly, the first author of the paper is directly involved in the development of the system and supported processes. This helped us explicitly to identify the problem, to understand the particularities of the business process and to determine business activities, which should be automated using software systems. Thirdly, the second author of the paper is a co-author of SRPs [1], thus this helped us to apply the SRPs in the intended manner.

Another limitation is that we do not perform the formal compliance checking (i.e., "*a relationship between the formal representation of a business model and the formal representation of a relevant regulation*" [10]). We also did not have the goal to enrich the business process model with security-related activities (e.g., as discussed in [19]). Annotating business process model (e.g., Fig. 7) leaves the core business process representation separated from the security (i.e., compliance) details. However we acknowledge the importance of the formal compliance management and consider it as the future work.

The current report is limited to the application of two SRPs (namely *SPR.1* and *SRP.5*). However, other SRPs were also applied in the actual case (as mentioned in Section 3.3 discussing *SRP.2*) and showed their usefulness to contribute to the compliance of the business process.

5.2 Lessons Learnt

Firstly, the current work serves as a proof-of-concept showing that SRPs could systematically guide the compliance manager to achieve business process compliance with the selected regulations.

Secondly, we have learnt that the current security risk-oriented patterns [1] are rather limited to cover the complete list of security regulations. For instance, ISO/IEC 27001:2013 (and other standards) does not only concern the computerised information management (i.e., access control, cryptology, or information classification). It also deals with (physical) human resource security, media handling, physical and environmental security, equipment and other. Thus this leads to the necessity to develop new security risk, which potentially could be applied to compliance management at different enterprise level.

Thirdly, we have experienced that the heuristics of the SRP application should be improved. For instance, we have observed that it is important to perform some model pre-processing (by introducing *data stores*, *data object*, by explicitly clarifying *data flows* between the pools, etc.) before the SRPs could actually be used in the business

process models. One possible way to improve the SRP application is its specification using method engineering principles [9]. This work is already started in [21], however further validation is still needed.

Acknowledgements

This research is supported by the Estonian Research Council.
The paper of the Baltic-German University Liaison Office is also supported by the German Academic Exchange Service (DAAD) with funds from the Foreign Office of the Federal Republic Germany.

References

1. Ahmed, N., Matulevičius, R.: Securing Business Processes Using Security Risk-oriented Patterns. Computer Standards & Interfaces 36(4), 723–733 (2014)
2. Ahmed N., Matulevičius R.: Presentation and Validation of Method for Security Requirements Elicitation from Business Processes. In CAiSE Forum 2014, LNBIP 204, pp. 20–35, 2015.
3. Altuhhova O., Matulevičius R., Ahmed N.: An Extension of Business Process Model and Notification for Security Risk Management. International Journal of IS Modeling and Design (IJISMD), 4, pp. 93–113
4. Basel Committee on Banking Supervision, Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems, revised 2011, Bank for International Settlements Communications
5. Brucker S. D., Compagna L., Guilleminot P.: Compliance Validation of Secure Service Compositions, In Secure and Trustworthy Service Composition: The Aniketos Approach. LNCS 8900, 2014, pp 136-149
6. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Eng., pp. 289–306. Springer (2010)
7. Dumas M., La Rosa M., Mendling J., Reijers, H. A.: Fundamentals of Business Process Management pp. 1 (2013)
8. El Kharbili M., Stein S., Markovic I., Pulvermuller E., Towards a Framework for Semantic Business Process Compliance Management. In proceedings of GRCIS'08, 2008, pp 1-15.
9. Goldkuhl, G.; Lind, M. and U. Seigerroth (1998) Method integration: the need for a learning Perspective. . IEE Proceedings, Software (Special issue on Information System Methodologies), Vol. 145, Nr 4.
10. Governatori G., Shek S.: Rule Based Business Process Compliance. Proceedings of the RuleML2012@ECAI Challenge, 2012
11. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization, 2013.
12. IT-Grundschutz Catalogues. Bundesamt fu ̈r Sicherheit in der Informationstechnik (BSI), Bonn, 2013
13. Matulevičius R., Ahmed N.: Eliciting Security Requirements from the Business Processes Using Security Risk- Oriented Patterns. it - Information Technology, Vol. 55, No. 6, pp. 225–230

14. Neubauer, T., Ekelhart, A., Fenz, S.: Interactive Selection of ISO 27001 Controls under Multiple Objectives. 278, 2008, pp. 477-479 23rd International Information Security Conference IFIP – The International Federation for Information Processing (2008)
15. NIST Special Publication 800-39. Managing Information Security Risk – Organization, Mission, and Information System View. National Institute of Standards and Technology, Gaithersburg, 2011.
16. Papazoglou M. P., Making Business Processes Compliant to Standards & Regulations, In 15th IEEE International Enterprise Distributed Object Computing Conference (EDOC), 2011, pp. 3-13
17. Ramezani E., Fahland D., van der Werf J. M., Mattheis P.: Separating Compliance Management and Business Process Management, In: Business Process Management Workshops, LNBIP 100, 2012, pp 459-464
18. Ramezani E., Fahland D., van der Aalst W., Supporting Domain Experts to Select and Configure Precise Compliance Rules In: Business Process Management Workshops, LNBIP 171, 2014, pp 498-512
19. Sadiq S., Governatori G.: Managing Regulatory Compliance in Business Processes, In: Handbook on Business Process Management 2, International Handbooks on Information Systems 2015, pp 265-288
20. Salnitri M., Paja E., Giorgini P., Preserving Compliance with Security Requirements in Socio-Technical Systems, Cyber Security and Privacy, CCIS 470, Springer, 2014, pp 49-61
21. Sandkuhl K., Matulevičius R., Ahmed N., Kirikova M.: Refining Security Requirement Elicitation from Business Processes using Method Engineering, Accepted at the Workshop on Security and Compliance in Business Processes, 2015.
22. Schultz M., Enriching Process Models for Business Process Compliance Checking in ERP Environments, In: DESRIST 2013, LNCS 7939, 2013, pp. 120-135
23. Schumacher, M., Fernandez B., E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating Security and Systems Engineering. Wiley (2006)
24. Schumm D., Turetken O., Kokash N., Elgammal A., Leymann F., van den Heuvel W.-J.: Business Process Compliance through Reusable Units of Compliant Processes, In: Current Trends in Web Engineering, LNCS 6385, 2010, pp 325-337