Towards Continuous Information Security Audit

Dmitrijs Kozlovs, Kristine Cjaputa, Marite Kirikova

Riga Technical University, Latvia
{dmitrijs.kozlovs, kristine.cjaputa, marite.kirikova}@rtu.lv

Abstract. Requirement engineering calls for continuous possibility to check whether latest changes of significant requirements are met by the target systems. This review is important because the environment of the system, if impacted by changes, may lead to new exposures. Current paper reports on knowledge gained during the attempt to move towards continuous security audit by extending one business process based security requirements identification method with the elements from audit area and the automated business process analysis method for identifying the points for the attention of audit.

Keywords: SREBP, information security audit, security patterns identification.

1 Introduction

Security requirements gain importance for different types of business and public institutions in the nowadays environment, where practically anything is linked by certain relations [1, 2]. One of the major problems of this area is that statement of requirements starts at the business level and not always general security intensions are properly transformed down to an operational level. By concentrating, in particular, to information security issues, we tried to find ways how to solve this problem at the business process level. The business process level was chosen because it has close relationships to both - higher strategic levels and to the information technology infrastructure. The choice of the level was validated using business processes of middle-sized enterprise based in Latvia.

Security requirements identification approach that focuses on information flows in business processes was used for information security audit at the business level. Security Requirements Elicitation from Business Processes approach (SREBP) [3], which utilizes 5 security patterns, was chosen as a base approach, because the patterns explicitly focus on particular information flows in the process. However, SREBP approach uses manual pattern identification, which is a complex and time consuming process even for SME. Therefore, we attempted to find a way for searching the patterns of interest in the business process automatically.

The paper is organized as follows. In Section 2 we briefly describe how the SREBP approach was used for auditing purposes. In Section 3 we discuss the method that, to some extent, helps to identify security patterns automatically. In Section 4 brief conclusions are provided.

2 Information Security Audit at Business Process Level

According to Glossary of Terms introduced by Information Systems Audit and Control Association (ISACA) [2], Information Security encompasses protection of information within the boundary of a company against disclosure to unauthorized users, improper modification, and the fact of being unavailable, when required. Hereby the three main information security concepts are indicated:

- Confidentiality – takes into consideration the aspect of restrictions on disclosure, protection of privacy.
- Integrity – tackles protection of information against unauthorized changes, also destructive damages to information, preserving non repudiation and authenticity of information.
- Availability – ensures reliable and timely access to information, in the terms of business continuity.

These three concepts are utilized by SREBP approach that was developed by Naved Ahmed and Raimundas Matulevicius from Institute of Computer Science, Tartu University, Estonia, and afterwards the approach was further elaborated in the international project of Tartu University (Estonia), Riga Technical University (Latvia) and University of Rostock (Germany) [3,4,5]. The approach bridges the needs and knowledge of business process analysts and security engineers by transforming the security objectives into security requirements, whereas attracting security engineering and business analysts, in order to determine and lower down the intentional harm to valuable assets. Therefore, the key issue of the approach is to identify the security criteria and elicit security requirements from a business process model.

SREBP approach deals with limitations of the systematic requirement engineering for addressing security in business processes. Use of the approach encompasses two phases determining five contextual areas for deriving security requirements: access control, communication channel, input interface, network infrastructure, and data store [3,4,5]:

- Identification of business assets (information assets) and their security objectives
- Elicitation of security requirements from business process models

The approach focuses on such information security aspects as confidentiality, integrity, and availability, as well as three conceptual groups of security concept (asset related, risk related, and risk treatment related). As a result the following five patterns are utilized [3,4,5]:

- SPR1 – deals with confidential data by multilevel security approach
- SRP2 – copes with data transferred between business entities
- SRP3 – enables data validation methods during input in business process
- SRP4 – ensures service availability for business assets (information assets) in case of service denial attack
- SRP5 – tackles data privacy aspects against insiders

The use of SREBP approach prescribes the following activities to be performed regarding the processes:

- Identify the business assets
- Identify the key security objectives – confidentiality, integrity, availability
- Identify SREBP patterns to a definite contextual area

- Extract SREBP patterns
- Apply security requirement derivation from security model [3]
- Assess and analyze risks by identification of risk, risk cause – event, impact, vulnerability, threat, threat agent, and attack method
- Treat risks and proceed with security requirements – categorize risk treatment, select control, specify security requirement
- Add security requirements to business process model graphically

The above-mentioned contextual areas are deemed to include the additional information security criteria like identification, authentication, authorization, non-repudiation, cryptography, auditability.

Based on the information explicated above, the main results that can be expected from SREBP approach are linking business assets to security criteria, then identifying whether certain patterns can be applied, and afterwards proceeding with information security requirements for the certain business activity or several activities within the scope of the definite business process. The approach is more oriented for the use of providing security requirements to the company and as guidelines in the initial phases of information security audit or within the scope of agreed-upon-procedures, therefore not covering the full scope of the information security audit.

For the purposes of identifying requirements from the perspective of Information Security Audit towards SREBP or any other approach that could be used for information security audit of information flows, we considered expedient to base the requirements on one of the most important document that is used in any audit – the Audit Plan [6,7,8,9,10,11,12,13,14].

By analyzing main constituents of the audit plan, we found 37 requirements for information security audit, and grouped them as it is shown in Table 1. The first column of the table reflects the audit requirements, the second column shows the numbers of those requirements that can be met by SREBP approach. The fit ratio regarding number of requirements from information security audit met by SREBP approach was quite low (27%) (last column in Table 2).

We developed the method that, to some extent, can close the indicated gaps derived from requirements of information security audit. The knowledge from OCTAVE Allegro methodology [15], Global Audit Methodology by Big4 Audit Companies [6, 8, 9, 13], Entity Level Control Risk Matrix [16, 17, 18], and Information Demand Patterns [19] were utilized. This knowledge is fused in the main artefact of the designed method (extension for SREB application in information security audit) - Table 3. Table 3 for information security audit of information flows in business processes should be applicable to any activity that is identified within the business process (or sub-process) and involves creation, processing, retaining, transforming, loading, or any other action done to an information asset. The designed Table 3. can be applied to any activity, regardless its type, industry, timing, and executors involved.

The following audit techniques were used for design of Table 3 for purposes of Information Security Audit of Information Flows in Business Processes: visual inspection, observations, analysis of files, technical examination, data analysis, and written questionnaires.

Table 1. Information Security Audit plan

Audit Plan Requirement	Fits
1. Requirements derived from Planning and Risk Identification: 1.1. Complete Entity Level Control Preliminary Risk Assessment Matrix, in order to ensure evaluation of 1.1.1. Control preliminary assessment of the process 1.1.2. Changes and reorganization done to the process 1.1.3. Complexity of the process 1.1.4. Impact on other processes 1.1.5. Cost level 1.1.6. External or third party impact 1.1.7. Time since previous audit 1.1.8. Management concern assessment 1.1.9. Fraud indications 1.1.10. Impact on further decision making 1.1.11. Employee (data custodian/information custodian) experience and qualification 1.1.12. Social responsibility and public interest 1.2. Ensure ability to design the audit program activities that are aligned with information security management systems intended outcomes and strategic direction of the organization, 1.3. Ensure proper documentation of the results gained during information security audit 1.4. Be applicable within definite boundaries of information security management system, 1.5. Be capable to identify external and internal vulnerabilities 1.6. Be capable to check the integration of information security management system requirements in organization’s processes	1.2, 1.3, 1.4, 1.5, 1.6.
2. Requirements derived from Strategy and Risk Assessment 2.1. Map existing business process, mark data input and output, identify information flows/ identify data sources, processing points and end points (information flow) 2.2. Identify information security risk owners 2.3. Use information flows to identify information assets 2.4. Identify information demand patterns 2.5. Apply information security criteria towards activities that involve information flows 2.6. For activities that involve information flows, identify potential risks, risk impact and risk likelihood 2.7. Summarize the risk assessment for an activity that involves information flows 2.8. Support information security risk acceptance criteria state (whether risk is accepted, transferred or mitigated 2.9. Prioritizes analysed risk for treatment based on risk assessment plan the strategy of the audit – whether to rely on controls or not, by applying substantive procedures for information security audit 2.10. Prepare a list of information that would help to plan the audit activities 2.11. Specify whether any information, user activity logs are to be observed	2.1, 2.2, 2.3, 2.5.
3. Requirements derived from Execution of Audit Activities 3.1. Determine match of controls with security assertions	

Audit Plan Requirement	Fits
3.2. Based on business process mapping state whether appropriate controls are designed to cover the risks in the concept of security objectives 3.3. Based on business process mapping check whether appropriate controls are effective to cover the risks in the concept of security objectives 3.4. Define whether additional procedures are required	
4. Requirements derived from Conclusion and reporting 4.1. Merge all identified issues 4.2. Compare the indicated issues with risk tolerance 4.3. Prepare suggestions and improvements Identify if any changes occurred after audit	4.1.
5. Requirements derived from Follow up 5.1. Mark whether the recommendation towards information security are implemented	

Table 2. Fit Gap Analysis

Requirement Section	Number of Requirements	Number of Fits	Number of Gaps	Fit %
Planning and risk identification	17	5	12	29%
Strategy and risk assessment	11	4	7	36%
Execution	4	0	4	0%
Conclusion and Reporting	4	1	3	25%
Follow Up	1	0	1	0
Total:	**37**	**10**	**27**	**27%**

Thus, based on Table 3, the execution of the designed method involves the following parts (phases) that are placed in a sequence:

1. Mapping the business process (sub-process) using an appropriate notation at the entity and process level.
2. Completing Entity Level Control Risk Preliminary Assessment matrix at the entity and process level [16,17,18].
3. Applying SREBP approach at the activity level, in terms of business asset (information asset) identification and relating it to security requirement elicitation (for purposes of identifying security criteria), - omitting the security patterns at this stage, because the identification of patterns is better applied after the activities related to definite information assets are processed in Table 3.
4. Proceeding to complete Table 3.

The designed Table 3. starts with identification of **General** part with the following rationale:

1. Entity level controls preliminary assessment result based on the self-assessment. The Company can indicate the process that is considered as critical to the Company. The values of Entity Level Control Preliminary Assessment are low, moderate or high, based on the number of assigned points. The identification of the critical process gives substance for selecting the sub-process for deeper analysis. It is advised to select moderate or high risk.
2. Process – the process should be named for the purposes of proper audit documentation.

3. Sub-process – the sub process should be named for the purposes of proper audit documentation.
4. Activity – the activity should be named for the purposes of proper audit documentation.

Table 3. Designed Extension to SREBP approach for the purposes IT Security Audit of Information Flows in Business Processes

No.	**Activities**
1	**General**
1.1	Entity Level Control Preliminary assessment
1.2	Process
1.3	Sub process
1.4	Activity
2	**Data and Information**
2.1	Information Asset
2.2	Information Asset Owner
2.3	Information Asset Custodians
2.4	Apply Assertions/Security Criteria
2.5	Vulnerabilities related to Information Asset
3	**Risk Assessment for Information Asset**
3.1	What can go Wrong
3.2	Risk Impact
3.3	Risk Occurrence
3.4	Level of Risk
4	**Analysis of Significant Risks (non tolerable)**
4.1	List of Recommended Controls at Place
4.2	Control Effectiveness
4.2.1	List of Recommended Test of Controls
4.2.2	Effective Control vs Security Criteria
4.3	Controls not at place or not effective
4.3.1	List of Recommended Substantive Procedures
4.3.2	Security criteria vs. Substantive Procedures
4.4	Summary of Results
5	**Conclusion on Protection of Information Asset**
6	**Suggestions for Improvements**

Table 3 is continued with **Data and Information** part with the following rationale:

1. Information asset – is identified for the purposes of understanding what should be protected and for the purposes of creating a summary on all further activities that are linked to this information asset, if it is involved in several activities within the scope of a business process or sub process.

2. Information asset owner – is identified for the purposes of creating a summary on all further activities that are linked to this information asset owner, if s/he is involved in several activities within the scope of a business process or sub-process for checking of segregation of duties.
3. Information asset custodian(-s) – is identified for the purposes of creating a summary of all further activities that are linked to this information asset custodian, if s/he is involved in several activities within the scope of a business process or sub-process for checking of segregation of duties. Also, this is used for identification of information demand patterns.
4. Apply assertions/ security criteria – is used as a list, where the related security criteria should be check-marked, in order to understand what kind of security criteria should be applied to this definite information. The basis of selection of the security criteria should be derived from the Information Security policies and procedures that are developed, approved and implemented by the Company.
5. Vulnerabilities related to information asset – are indicated according to the security criteria prescribed to the information asset, the most significant vulnerabilities are marked as potential threats.

Table 3 is continued with **Risk Assessment of Information Asset** part with the following rationale:

1. What can go wrong – lists the potential threats, that can be transformed into risks and recorded as risks towards the protection of information asset.
2. Risk impact – is assessed as low (insignificant affect), moderate (not significant affect) or high (significant affect) in regards to potential harm that could be done by realization of threats.
3. Risk occurrence – is assessed as low (rarely or never possible), moderate (possible, but not periodic), or high (possible or periodic).
4. Level of risk – is assessed as low, moderate, or high, based on the combination of risk impact and risk occurrence (low impact and low occurrence, low impact and medium occurrence, medium impact and low occurrence results in low level of risk; low impact and high occurrence, medium impact and medium occurrence, high impact and low occurrence result in medium level of risk; medium impact and high occurrence, high impact and medium occurrence, high impact and high occurrence result in high risk level [20]).

Table 3 is continued with **Analysis of Significant Risk (non-tolerable)** part that deals only with moderate or high level risks with the following rationale:

1. List of recommended controls at place – should determine which controls are at place for the specific information asset.
2. Control effectiveness – should suggest a predefined list of test of controls for specific information asset and evaluate whether the control reaches the security criteria of protection of the information assets.
3. Controls not at place or not effective – should be completed if only controls are not at place or not effective by suggesting a list of recommended substantive procedures and afterwards verify whether there are no indications of the information asset being vulnerable to the risks indicated that are derived from security criteria.
4. Summary of results – indicates key findings.

Table 3 is continued with **Conclusion on Protection of Information Asset** that should give a conclusion whether the information asset is protected or not (whether security requirements for the protection of the information asset are met). The last part of the Table 3 should list **suggestions** on key findings or opportunities for potential improvement of security of definite information asset**.**

3. Support for (Semi-) Automatic Identification of Security Patterns

The changes in business processes assume changes application of security measures for information assets. To gain scalability and avoid manual time consuming execution, Table 3. could be partly filled on the basis of security patterns [3]. As manual pattern identification is very time consuming, we tried to automate this process by using the transformation of business process mapped in BPMN to XML format, then comparing XML code of each process to the XML code of known process patterns (see Figure 1).

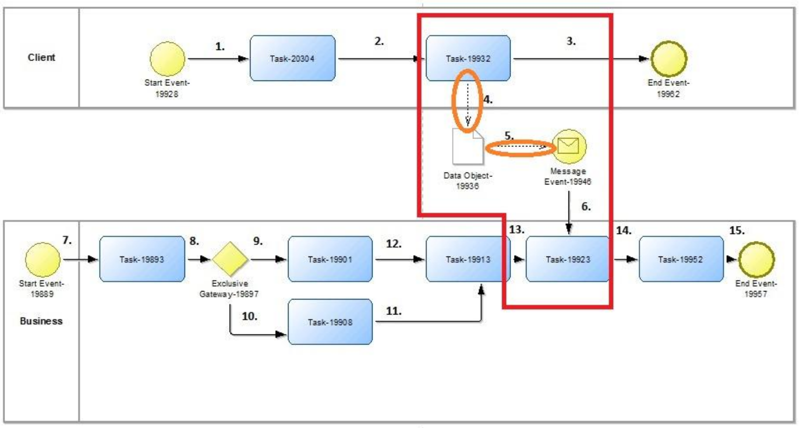

Fig. 1. Potential pattern SRP1 detected with Altova DiffDog

The method has the following main steps:

1. In order to make comparison of the business process and the pattern, the XML files of the business process should be made.
2. The XML file should be checked whether the business process has connectors with type “Data Association”. If the business process has no connector with type “Data Association, then the elements of this business process do not contain the elements of the pattern. If the connectors with the type “Data Association” are identified, the analysis should be continued.

4. Look through the “Instances” and their classes in the business process. If exactly the same “Instances” as in one of the pattern are found, there is a possibility to have the pattern in the business process. When all “Instances” for one pattern are identified in the business process, the connections between the elements in the

business process must be identified. The sequence between instances has to be taken into consideration as it is different for each pattern. If the connectors in the XML file match, then the pattern is identified. The connectors should match with exactly the same pattern, whose instances were identified. For example, the sequence of the elements in the pattern SRP1 is listed below:

- “From” Instance “Task A” with the class “Task”
- Connected with “Data association”
- “To” Instance “Data object B” with the class “Data object”
- From Instance “Data object B” with the class “Data object”
- Connected with connector with type “Data association”
- “To” Instance “Message event C” with the class “Start event”
- “From” Instance “Message event C” with the class “Start event”
- Connected with connector with type “Subsequent”
- “To” Instance “Task D” with the class “Task”

6. If the pattern SRP 3 or SRP 5 are identified, the similarities with the business process elements are found, the pattern can be used for ensuring security in the business process. If the pattern that consists of the business process elements from one of the patterns SRP 1, SRP 2 or SRP 4, then additional information is needed from the users’ side:
   a. If the user needs authorization to access the data – it is pattern SRP 4.
   b. If the user has to submit data, it is pattern SRP2.

For identified security patterns the security requirements can be derived according to the SREBP approach, which prescribes potential measures for each security pattern.

4. Conclusions

In this paper we shared our knowledge that we gained by trying to find a way how to establish methods for continuous security requirements engineering. We took as a basis one of security requirement methods SREBP and extended it towards the audit of information assets and towards automatic detection of security patterns. Applicability of both extensions was validated on the procedure descriptions of advanced Latvian middle-sized enterprise. To apply the audit successfully, further IT developments are needed for supporting tools that could give a possibility to save time during the audit procedure. The patterns derivation using XML code is possible, but for two of five patterns expert involvement is still needed.

Acknowledgment: The research presented here is done in part under the grant agreement Nr.10-4/VPP-4/11.

References

1. Schmitt, C., Liggesmeyer, P.: Getting Grip on Security Requirements Elicitation by Structuring and Reusing Security Requirements Sources. In: Complex Systems Informatics

and Modeling Quarterly, CSIMQ, 2015, No. 3, pp. 15–34. ISSN 2255-9922. Available from: http://dx.doi.org/10.7250/csimq.2015-3.02

2. Information Systems Audit and Control Association, Glossary of Terms, 2015 [cited Nov 2015]. Available at: http://www.isaca.org/Pages/Glossary.aspx
3. Ahmed, N., Matulievičius, R.: A Taxonomy for Assessing Security in Business Process Modelling. In: Research Challenges in Information Science (RCIS), IEEE Seventh International Conference, pp. 1-10 (2013)
4. Ahmed, N., Matulievičius, R.: Eliciting Security Requirements from the Business Processes Using Security Risk-oriented Patterns, it - Information Technology, vol. 55, Issue 6, pp. 225–230 (2013)
5. German Federal Office for Information Security, Information Security Audit (IS Audit): A guideline for IS audits based on IT-Grundshutz, Bonn, 38 p (2008)
6. Information Systems Audit and Control Association. Auditing Global Compliance of Data Protection Mechanisms. In: ISACA Journal Volume 6 "Emerging and Evolving IT Risk", pp. 46-49 (2011)
7. Ahmed, N., Matulievičius, R.: Securing business processes using security risk-oriented patterns, Elsevier B.V., Computer Standards and Interfaces vol. 36, Issue 4, pp. 723–733 (2013)
8. Information Systems Audit and Control Association, In: IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals [cited– Mar 29 2015] (2010). Available at: http://www.isaca.org/Knowledge - Center/Standards/Documents/IT-Audit-Assurance-Guidance-1March2010.pdf
9. ISO, Information technology — Security techniques — Information security risk management, 27005, 68 p (2011)
10. ISO, Information technology– Security Techniques– Information Security Management Systems– Requirements, 27001 2nd edition, 23 p (2013)
11. IT Compliance Institute, Information Security: Practical Guidance on How to prepare for successful audits, [cited Dec 2015]. Available at: http://download.101com.com/pub/itci/Files/ITCi_ITACL-InfoSec_0612_finalweb.pdf
12. IT Governance Institute, Control Objectives for Information and related Technology 4.1, 213 p (2007)
13. National Archives, Identifying Information Assets and Business Requirements, [cited Dec 2015]. Available at: http://www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf
14. Taubenberger, S., & Jurjens, J.: IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements, [cited Sept 2015] 10 p (2008). Available at: http://ceur-ws.org/Vol-413/paper16.pdf
15. Caralli, R.A., Stevens, J.F., Young, L.R., William, R., Wilson: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Software Engineering Institute, Hanscom, CMU/SEI-2007-TR-012 ESC-TR-2007-012, 154 p (2007)
16. ISO/IEC, Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements, 325 p (2005)
17. ISO/IEC, Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, 233 p (2012)
18. Verdina, G.: Iekšējās Kontroles Sistēmas Pilnveidošanas iespējas Studiju Programmas Īstenošanas procesā, PhD doctoral thesis, University of Latvia, Riga, Latvia, 252 p (2012)
19. Sandkuhl, K.: Information Demand Patterns: Capturing Organizational Knowledge about Information Flow, PATTERNS 2011: The Third International Conferences on Pervasive Patterns and Applications, 6 p (2011)
20. Nørgaard, H., Kühn, T.: EY Danmark, Presentation: Risikobaseret tilgang til revision (Use of Risk Based Concepts for Financial Statement Assurance), Copenhagen, 55 p (2013)