1-1-2010

Supporting Compliance through Enhancing Internal Control Systems by Conceptual Business Process Security Modeling

Moritz Riesner
University of Regensburg, moritz.riesner@wiwi.uni-regensburg.de

Günther Pernul
University of Regensburg, guenther.pernul@wiwi.uni-regensburg.de

Supporting Compliance through Enhancing Internal Control Systems by Conceptual Business Process Security Modeling

Moritz Riesner, Günther Pernul
Department of Information Systems
University of Regensburg
Regensburg, Germany
Email: {moritz.riesner | guenther.pernul}@wiwi.uni-regensburg.de

Abstract

The importance of Business Process Modeling (BPM) particularly in sensitive areas combined with the rising impact of legislative requirements on IT operations results in a need to conceptually represent security semantics in BPM. We define critical security semantics that need to be incorporated in BPM to aid documentation of security needs and support compliant behavior of security systems. We analyze ways to express such semantics in BPM and their possible role in designing and operating internal control systems, which ensure and document the execution of compliance-related activities. The analysis shows that there are informal, semi-formal and formal approaches to represent security semantics in BPM. We consider the informal approaches as best suited to express security objectives and their formal counterparts as best to specify security mechanisms to enforce the objectives. All three groups of approaches have the potential to enhance the expressiveness and informative value of an internal control system.

Keywords

Compliance, IT-Security, BPM, Conceptual Modeling, Internal Control

INTRODUCTION

Business Process Modeling (BPM) has reached key importance in modern enterprises: Process models are used to plan, communicate, analyze and improve value-creating task flows within and between departments and even across multiple organizations. For a long time, BPM has reached business areas that are critical for the company's success and even survival, for example financial transactions, thus calling for the incorporation of security requirements and features. A major driver to consider security semantics in BPM is the rising need for compliant enterprise IT: Companies are facing an increasing number of legislative and contractual regulations that pose implicit and partially explicit requirements on the operation and security of the company's IT systems. A well-known example is the Sarbanes-Oxley Act, tightening the requirements for correct and reliable financial reporting. Commonly used to comply to such legislations or even explicitly required are internal control systems (ICS), composed of processes which enforce and monitor correct behavior and produce documentation of relevant actions. As of now, most of these tasks involved in planning and operating an ICS are carried out manually, resulting in a high cost of achieving compliance.

Currently, most common BPM techniques do not address security in a sufficient manner. The resulting lack of incorporation of security considerations into the software design process leads to late and incomplete embedding of security features into the application design and thus to possible vulnerabilities. A number of academic approaches tackle this issue and aim at expressing security semantics in business process models. This is considered as one of the first steps in developing a better understanding of the security requirements of the application and thus fundamental for documentation of evidence of conformity with corresponding laws and regulations. Unfortunately, the most approaches published so far do not have their major focus on the support of compliance or supporting the incorporation of the security demands of applications into the design of an ICS. In this paper, we evaluate these approaches regarding their potential contribution towards achieving compliance by incorporating security considerations into BPM and subsequently into design and operation of an ICS. This will result in a clearer definition of control objectives and automation of both compliance-related activities and their documentation.

The rest of the paper is organized as follows: In the following section, we review related work on BPM, compliance and security semantics. In the subsequent section, we derive security semantics whose incorporation into BPM would benefit the achievement of compliance followed by an analysis of how to integrate each aspect. This is followed by a section in which we compare existing approaches for modeling security in BPM using the defined semantics, followed by a discussion of open challenges and a conclusion in the last section.

RELATED WORK

A plethora of work has been published on BPM techniques and their application in research and practice. Even while academics and practitioners see partly differing benefits of it, the overall perception of BPM as a highly relevant and useful approach is well-documented (Indulska et al. 2009; Ho et al. 2008). Besides common advantages such as communication, understanding and process improvement, governance aspects gain importance due to increasing regulatory requirements.

Compliance requirements originate from legal frameworks, actual legislation, contractual agreements, standards and best practices with a range of different goals, scopes and applicability depending on industry sector, company size and region (Tarantino 2008). Legal frameworks, such as Basel II[1] or the European Data Protection Directive[2] set requirements that have to be implemented into national legislation. Laws may only be relevant for a certain industry sector such as health care, as with the Health Insurance Portability and Accountability Act (HIPAA)[3], or only in certain jurisdictions. Adherence to frameworks, standards and best practices such as COSO[4], a framework for internal control, or ITIL[5] is often implicitly or explicitly required to comply with laws, contractual agreements and market needs.

There are only few works bridging the three disciplines compliance, BPM and IT-Security. For example, Karagiannis (2008) describes a method to extend BPM in order to achieve regulatory compliance using IT, which does however not focus on IT security issues. Neubauer et al. (2009) give a brief overview of existing approaches for security in business process management and sketch a roadmap for future research emphasizing the importance of considering the strategic business value of any measures undertaken. Kharbili et al. (2008) review current work in the context of BPM from the perspective of compliance checking in a short position paper. Siponen and Heikka (2008) analyze design methods for secure information systems. However, the BPM perspective only plays a minor role in their work. In contrast to the selected work mentioned above, we focus on modeling concrete security semantics in BPM with the goal of supporting compliance.

SECURITY CRITERIA FOR ACHIEVING COMPLIANCE

In this section, we define security objectives and functions that would be useful for achieving compliance if expressed in the context of BPM and integrated into ICS. It would be ideal to be able to express any possible security requirement resulting from legislations, contracts and best-practice standards. However, the multitude of such compliance texts with differing purposes, often vague specifications and various levels of abstraction make it a complicated task to compile such a complete list of requirements. Also, some security requirements are not fully applicable to BPM. Instead, our approach is to derive only those requirements resulting from legislative texts, associated standards and frameworks that are most common and useful towards achieving compliance. In this work, we focus on the Sarbanes-Oxley Act (SOX) of 2002[6] and the European Data Protection Directive, two well-known legislations that have been a driver for compliance activities both in practice and scientific research.

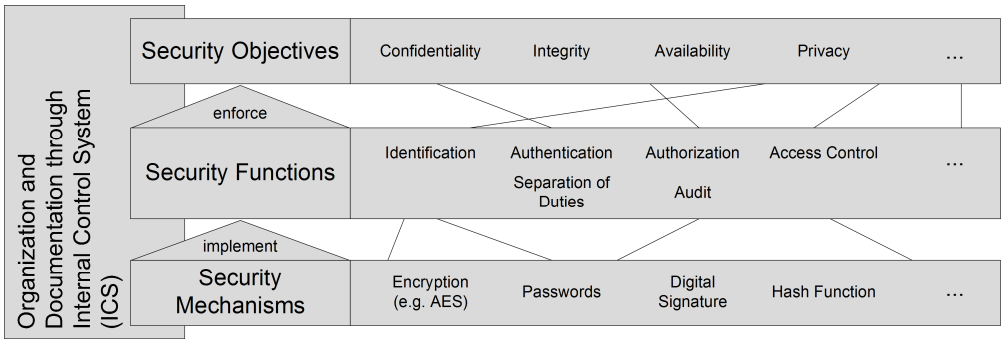

Figure 1: Security Semantics to be modeled in BPM

In order to arrive at a set of requirements with impact for compliance considerations, we propose to view security in different layers, each representing a different level of abstraction. As depicted in Figure 1, on a top layer, we see **security objectives**. A **security function** enforces a particular security objective and implements particu-

[1] http://www.bis.org/publ/bcbsca.htm
[2] http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
[3] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
[4] http://www.coso.org/
[5] http://www.itil-officialsite.com/
[6] http://www.sec.gov/about/laws/soa2002.pdf

lar **security mechanisms**, for example password use or a certain encryption algorithm. Security mechanisms are out of scope here, as conceptual modeling should focus on security objectives and functions. However, they are necessary for understanding the other two security layers with security functions as an enforcement layer between security objectives, which pose requirements and security mechanisms that are eventually implemented to enforce them. In the context of compliance, we see the **ICS** as a means for organizing and documenting corresponding activities and measures across security layers.

Security Objectives

Legislative texts rarely contain specific instructions on the operation of IT. However, one can derive security objectives from the intentions of the law. Likewise, SOX with the goal of ensuring correct and reliable financial reporting and preventing fraud through mandatory ICS and increased manager liability, does not contain any direct IT-related requirements. Yet, it is clear that correct financial reporting requires integrity of the underlying data, meaning that modification of data by unauthorized users or false modification by fault or as a deliberate action is prevented. Also, relevant records must be available, meaning that they are not withheld from the system in the sense of a denial of service.Other notable legislations, such as the European Data Protection Directive, aim at preserving consumer privacy, which is closely related to confidentiality, the prevention of unauthorized or improper disclosure of data. Privacy is defined as the right to control collection, storage and dissemination of one's information (Herrmann and Herrmann 2006). It can be enhanced through more specific security aspects, such as anonymity and unlinkability. Although related to confidentiality, the enforcement mechanisms are different for privacy.

The three security objectives confidentiality, integrity and availability are commonly referred to as *CIA* requirements. Other examples of security objectives which are not considered here due to less relevance for the ICS are orginality (i.e. a digital coin must be original and not an identical copy), proof of communication (i.e. sender cannot deny having sent a message or recipient can proof that message was sent) or enforcement of copyright.

Security Functions

Another layer of describing IT security are security functions, used to organize enforcement of the security objectives mentioned above. While the legislation in focus is vague regarding IT security requirements, further statements and frameworks get more specific, in the case of SOX the Public Company Accounting Oversight Board's[7] (PCAOB) Auditing Standard Nr. 5, the control framework CobiT and related standards such as ISO 27001. In these documents, references to particular security functions can be found.

User *identification* and authentication, as well as authorization and access control are seen as the most important security functions to achieve compliance with SOX (Haworth and Pietron 2006). *Authentication* means ensuring that an entity has the identity it claims to have, while *authorization* means specifying access rights to resources. *Access control* is important for fulfilling the security objectives, as they distinguish between authorized and non-authorized use. *Auditing*, recording security events such as access decisions for later analysis is another related security function. Being system-related, it should be distinguished from internal and external audits performed to document compliance to laws and standards that usually have a broader scope. While access control is concerned with single entities accessing resources, *Separation of Duties* (SoD) is a further security function to prevent fraud by single users. Based on access control, yet especially important when it comes to performing tasks, as with business processes, it requires that certain actions have to be performed by different actors. Another related security function is the *Four-Eye Principle*, requiring that one particular action can only be performed by two actors together.

Internal Control and Documentation

Besides fulfilling the original security objectives and functions posed by relevant legislation and frameworks, it is necessary to coordinate and document the compliant behavior to prove compliance. As illustrated in Figure 1, ICS are commonly used to organize and monitor activities to achieve compliance, including IT security measures. Internal control can be described as a process itself, providing assurance about achieving company objectives. As in SOX, which explicitly demands the use of an adequate ICS, the term typically refers to controls over financial reporting, but may have a broader scope. Each control is designed to achieve a certain control objective and it has to be tested if the design is suitable to reach the objective and if it is carried out correctly (Karagiannis 2008).

[7] http://pcaobus.org/

Table 1. Security semantics to be expressed in BPM for compliance

Security semantics	Rationale
integrity	reliable and correct financial reporting (SOX), integrity of personal data required by EU Data Protection Directive (Steinke 2002)
availability	critical financial data needed for reporting (SOX), data retention requirements (Fox and Zonneveld 2006)
privacy	EU Data Protection Directive (Fischer-Hübner 2001; Steinke 2002), HIPAA
confidentiality	support privacy, protect sensitive information (SOX) (Fox and Zonneveld 2006)
authorization, access control	enforce CIA requirements, most important for SOX (Haworth and Pietron 2006)
authentication	prerequisite for authentication and access control
separation of duties (SoD)	required by SOX-related statements (Haworth and Pietron 2006)
ICS	internal controls explicity required by SOX
documentation	prove compliant behaviour in external audits
adherence to business process control flow	ensure correct execution of critical processes, existence of required processes

Most IT-related controls fall into the categories IT General Controls (ITGC) and IT Application Controls (ITAC): ITGC cover security requirements that are process-independent such as physical access or change management and support proper functioning of ITAC, which are application-based and each related to a certain business process (Fox and Zonneveld 2006). The design of an ICS follows its purpose. To become compliant to SOX for example, processes influencing financial statements with related risks are identified. Then ITAC to cover these risks are designed, which subsequently rely on ITGC.

It would be beneficial to design controls addressing the security objectives and functions identified as relevant for compliance. Modeling corresponding security semantics in BPM would help identifying relevant processes and related IT-systems. Also useful are semantics to model *internal controls* themselves. In addition to security requirements that may be applied to business process models or their elements, one common requirement expressed in ICS is the existence and performance of certain processes such as a change management process or a user management process, as recommended by the COSO-Framework. Therefore it is necessary to ensure the existence of such processes and enforce *adherence to their control flow*. Those processes commonly include multiple actors with different privileges, thus illustrating the aforementioned need for access control. Adherence to a designed work flow is also important for critical business processes that are vital to the legislation that is considered (Haworth and Pietron 2006).

To be able to prove compliant behavior and security measures in audits, sufficient *documentation* is needed. Process models themselves may serve as a documentation of the design of security measures and controls. However, the model itself does not cover information about the actual process execution, therefore retaining of system event data for critical operations is advisable. Approaches to incorporate security semantics in business processes can contribute towards proper documentation by allowing the identification of critical activities and security measures whose execution and parameters must be recorded.

Table **1** summarizes the security semantics that we consider as useful to be integrated into BPM in order to achieve compliance.

ANALYZING CONCEPTUAL BUSINESS PROCESS SECURITY MODELING

In this section, first we examine different proposals to model **security objectives** and **security functions** in business process models in order to support achieving compliance. Then we discuss which semantics can benefit the design and implementation of an **ICS**. The analysis will be illustrated using representative examples of existing techniques.

Conceptual Modeling at the Security Objective Level

Modeling the CIA (confidentiality, integrity, availability) security objectives in the context of business processes brings about two challenges: Firstly, conceptual business process models are mostly composed of activities, which differ from data, to which the security objectives are applied originally and by definition. If a security objective, for example integrity, were to be applied to a business process activity, the question, what should be protected from unauthorized modification, occurs. One could assume that implicitly the data involved in performing the activity is meant. This would require a definition of the data related to each activity, as included in some BPM techniques. Also, according to their definitions, confidentiality, integrity and availability distinguish between authorized and non-authorized entities, thus requiring a declaration about who is authorized.

Röhrig and Knorr (2004) present a method to define security requirements concerning artifacts, activities and actors in business processes and to derive security measures. Similarly to conceptual modeling of Mandatory Access Control (Pernul et al. 1998), activities and artifacts are assigned security levels in each of the categories confidentiality, integrity, availability and accountability while actors are assigned clearance levels in those categories. Thus, the question of authorized entities is answered implicitly. Yet, there is little explanation on the semantics when the security goals are applied to activities. Consistency checks ensure that there are no conflicts between the modeled security levels and that actor's clearances are high enough to perform the tasks they were assigned to. The next step is to automatically derive appropriate security measures from a predefined matrix using a special language introduced by the authors. This step however depends on the quality of the predefined security measures. In the context of an ICS, this approach has two benefits: Firstly, the assignment of security levels and clearances serves as a documentation on which authorization decisions are based on. Furthermore, chosen security measures can be justified with the matrix resulting from the security assignments.

Röhm et al. (1999) and Herrman and Herrman (2006) distinguish between different business process elements in their approach to analyze security requirements in business process models expressed through UML activity diagrams. Among 14 distinct security requirements, confidentiality, integrity and availability may be modeled on the conceptual level using security requirement objects that are represented through icons mapped to business process elements. Being consistent with their definition, confidentiality, integrity and availability may be linked to the entities of the process element class information which is in turn linked to activities. Also, confidentiality may be linked to process activities, however the exact semantics of how an activity can become confidential are not included. Security requirements are assigned levels of importance on a scale of one to seven. In later stages of the methodology, software and hardware building blocks are selected based on these ratings. The definition of authorized entities for confidentiality, integrity and availability is not further addressed, but can possibly be performed in later refinement stages.

Rodriguez et al. (2007a; 2007b) introduce extensions for the metamodels of both UML activity diagrams and the Business Process Modeling Notation (BPMN), which allow the specification of security requirements in business process models. The extension is performed through a predefined set of stereotypes representing a broad range of security requirements which can be linked to business process elements. The security objective integrity is modeled through a stereotype that can be annotated to process elements representing stored data and messages. The stereotype allows the specification of a protection degree, a connection to authorized entities is however not made.

These three approaches show that the application of CIA requirements to business process models is best performed by addressing elements representing data or flow objects while the application of these objectives on activities leaves open questions about their actual meaning. Still, these techniques allow expressing requirements which may serve as control objectives and thus as a basis for the design of security controls in an ICS. The distinction between authorized and other entities from the security objectives' point of view has been omitted, performed implicitly or postponed so far. This issue is addressed by approaches applying notions of access control to BPM, which are discussed in the following subsection. While the CIA requirements discussed so far are mostly relevant for SOX, other legislation, for example the EU Data Protection Directive focus on privacy. To model this security objective, Herrmann and Herrmann (2006) allow placing a corresponding requirement tag on elements representing information in UML activity diagrams. They distinguish privacy, here representing control over one's information, from anonymity, which they see as hiding the true identity of an actor. Consistently, anonymity tags may be annotated to agents. This is illustrated in Figure 2 (left), in which the anonymity tag is attached to the role *Patient*. Rodríguez et al. (2007b) apply privacy stereotypes to activities or groups of activities, posing the requirement, that the identity of the actor carrying out these activities is not disclosed. In Figure 2 (right), the privacy stereotype is applied to the swim lane *Patient*, thus applying to all activities that are performed by actors of that role. Once again, such techniques allow assessment of potential control objectives and are a starting point for the design of ICS that address privacy legislation. One has to ensure that modeled semantics are clearly defined, for example also by defining against which actors the privacy needs to be protected.

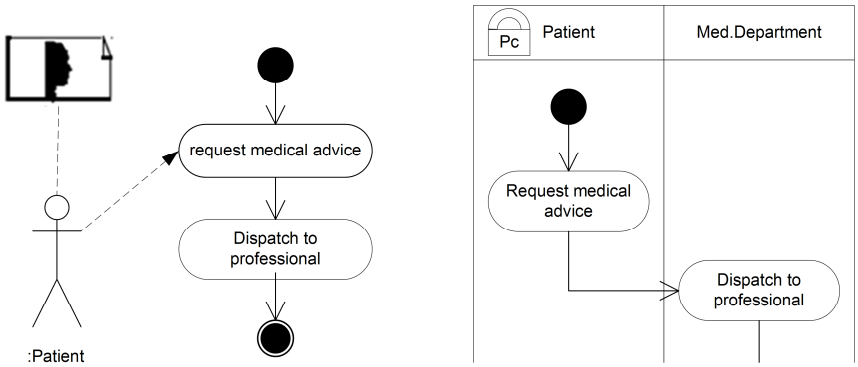

Figure 2: Anonymity requirement in the notation of Herrmann and Herrmann (2006) (left) and privacy requirement in the notation of Rodríguez et al. (2007a) (right)

Conceptual Modeling at the Security Function Level

As highlighted earlier, the notion of access control is of major importance to achieve compliance. A plethora of work has been published with the aim of applying access control to business processes. Atluri and Huang (1996) first presented a model for synchronizing data access rights to work flow activities, thus ensuring that actors currently executing a task have proper rights for documents involved in that task. The approach was later extended to applying role-based access control (RBAC) directly to business process tasks, meaning that only actors belonging to a certain role could execute specific tasks (Ahn et al. 2000). This marks the shift of focus from data objects to business process activities as a protected resource. At this point, it is important to distinguish between access rights on data, which could range from read and write to append access, while an activity can merely be executed or not. All of these approaches are presented in a formal and abstract fashion, however, a visual presentation in a process model is feasible as long as the amount of modeled semantics does not become confusingly large.

Access control semantics can be found in other approaches that are not solely devoted to it as well. Extensions for UML and BPMN introducing security semantics include access control stereotypes. In the extension presented by Rodríguez et al. (2007b), the stereotype representing the access control requirement may be linked to activities or groups of activities and has to be connected to a role, thus employing RBAC. In UMLSec, introduced by Jürjens (2005), a stereotype representing an access control requirement is applied to a whole activity diagram, specifying roles, rights and protected activities using tags. Lodderstedt et al. (2002) describe a UML meta model containing permissions that link actions, roles and model elements. Here, action types such as read may be specified for any element type, thus allowing any UML model element to become a protected resource. Due to the graphic nature of the underlying models, the annotated security semantics are displayed visually as well. Yet, some information, such as tag values of the stereotypes may not be shown in this kind of view. Swim lanes, rows or columns, in which a group of activities is placed, are a common way to denote that certain departments or actors are assigned to carry out those activities, thus complementing access control semantics.

In the context of ICS with the purpose of accomplishing compliance, these approaches are highly relevant for several reasons: They allow restricting execution rights of activities to owners of certain roles, thus decreasing the possibility to compromise integrity and confidentiality of related data and privacy. Secondly, many processes that are part of an ICS apply the concept of roles, defining for example a control owner responsible for carrying out control actions or actors that are allowed to approve software change requests (Fox 2006). Lastly, applying access control to BPM allows for further security functions, such as SoD.

These access control semantics cover authorization implicitly, basing access decisions on the fact that a user has a certain role. Also, it is assumed and required that the user has been identified and authenticated before, as the way this has been accomplished is not considered. To ensure accountability in highly critical scenarios it could become important, how reliable and trustworthy the user authentication is implemented. One could model the method of authentication, for example by knowledge or by possession, as done by Wolter et al. (2009). However, this may move the focus away from the semantic view with security objectives and functions to a more implementation centric view that names particular security mechanisms. Still, modeling the required trust in the authentication process through abstract values instead of the particular authentication method would be a feasible way.

The notion of SoD has also been identified as highly important for achieving compliance as it is a measure to avoid abuse of privileges and is also mentioned in control frameworks (Fox 2006). The application of SoD to BPM can be performed through constraints extending access control semantics. Bertino et al. (1997) introduced formal constraints on the assignment of either roles or users to tasks both at process design time and at execution

time. Another formal model that allows expressing not only SoD but also delegation semantics has been published by Wainer et al. (2007). SoD rules are mostly presented using formal statements, thus possibly unintuitive to casual users. A visual presentation of such rules has been demonstrated (Knorr and Stormer 2001), however, as with access control semantics, displaying a large amount of constraints graphically may become too confusing. Another way to hide the complexity of formal statements regarding SoD are predefined patterns as presented by Kumar and Liu (2008). However, they reduce the range of possible statements that can be defined.

Internal Control and Documentation

As stated in the previous sections, the existence and operation of an ICS is essential to organize compliance actions and even mandatory under some legislations such as SOX. Modeling business process security semantics can benefit designing and implementing the ICS: Firstly, modeled security objectives that highlight critical activities and help identify related IT-systems can be used to identify control objectives and construct corresponding control activities. Secondly, controls can utilize security functions, for example by proving their reliability through correctly implemented as access control and SoD. Furthermore, controls themselves can be modeled using BPM and incorporating security functions, such as access control for defining a control owner role.

Beyond the security semantics in a narrow sense, one needs to keep in mind that internal controls cover a very broad range and that only a small subset address IT-related issues. Thus, even in non-IT related areas, compliance can be achieved by modeling controls in business processes. Sadiq et al. (2007) model control objectives using Formal Contract Language (FCL), thus making normative assertions such as obligations and permissions and specifying consequences in case of violations. The business process model is then annotated with visual control tags that can be derived automatically from the FCL-statements. On process execution, obligations occur from the modeled control objectives. Failure to fulfill them results in violations and corresponding recovery actions have to be performed. Thus, the previously defined security aspect *adherence to control flow* is benefited as well. The modeled requirements contain predicates that use parameters such as subjects, roles, time or artifacts thus enabling assertions about access control and SoD. For such compliance requirements, a range of control patterns is proposed by the authors. The process model is not changed, but only annotated and may be viewed without any annotations. Figure 3 illustrates some possible annotations generated from FCL statements: The first tag, *GoodShipmentNotices* represents a control defining that shipments are made timely or a penalty is charged, the second tag adds a time constraint for sending goods and invoice and the rightmost tag requires that the purchase order must be included in the invoice. While the resulting annotated process models are presented in a visual fashion, the FCL statements are of a very formal nature and thus possibly unintuitive. Also, as one can see in Figure 3, the annotated model is not self-contained as the predicates and variables used in the tags are defined elsewhere.

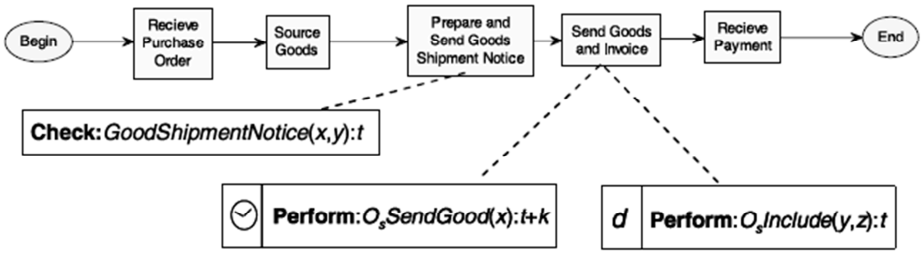

Figure 3: Process Model with annotated control tags (Sadiq et al. 2007)

As compliant structures and behavior need to be proven in audits, sufficient documentation is necessary for becoming compliant. In the context of BPM, we distinguish between documenting process models, which is independent of how, when and by whom they where performed, and documenting the actual execution of a process. Trivially, process models are documentation themselves, but they carry no meaning on whether they are compliant or not. Goedertier and Vanthienen (2007) propose expressing compliance requirements regarding obligations and permissions for executing activities and their control flow and sequence through “temporal deontic assignments”. Using these declarative statements, one can automatically generate a business process model that may be used for validation. With rules regarding the sequence of activities, time-based permissions and obligations, the range of possible security semantics is limited. Yet, for supporting compliance, the main benefit of the approach is to document that a business process design complies to a certain set of rules.

Documentation of the process execution may become quite extensive if every secure action that was carried out is included. A solution for this problem is to label those activities that are relevant for documentation, so that corresponding data is stored on execution (Rodríguez 2007a).

Table 2. Evaluation of the approaches

Authors	Security Criteria									
	C	I	A	P	Auth	A/AC	SoD	ICS	Doc	BP-CF
Informal approaches										
Herrmann and Herrmann (2006)	●	●	●	●	○	○	○	○	○	○
Jensen and Feja (2009)	●	●	○	○	○	●	○	○	○	○
Semi-formal approaches										
Röhrig and Knorr (2004)	●	●	●	○	○	●	○	○	○	○
Rodríguez et al. (2007a; 2007b)	◐	●	◐	●	○	●	○	○	●	○
Jürjens (2005)	●	●	◐	○	○	●	○	○	○	●
Wolter et al. (2009)	●	●	○	○	●	●	◐	○	○	○
Formal approaches										
Kumar and Liu (2008)	○	○	○	○	○	●	●	◐	○	○
Goedertier and Vanthienen (2007)	○	○	○	○	○	◐	○	○	●	●
Sadiq et al. (2007)	○	○	○	○	○	●	●	●	○	●
Formal approaches solely devoted to authorization, access control and SoD										
Ahn et al. (2000)	○	○	○	○	○	●	○	○	○	○
Lodderstedt et al. (2002)	○	○	○	○	○	●	○	○	○	○
Bertino et al. (1997)	○	○	○	○	○	●	●	○	○	○
Wainer et al. (2007)	○	○	○	○	○	●	●	○	○	○

C: Confidentiality, I: Integrity, A: Availability, P: Privacy, Auth: Authentication, A/AC: Authorization and Access Control, SoD: Separation of Duties, ICS: Internal Control System, Doc: Documentation, BP-CF: BP control flow,
●: Fully implemented or supported, ◐: not explicitly addressed, yet possible to express, ○: not supported

COMPARISON AND DISCUSSION

Table 2 shows the most representative approaches to incorporate security into BPM we have analyzed and indicates which of the semantics relevant for compliance we have derived are supported. We structure them into *informal*, *semi-formal* and *formal* approaches. We consider approaches that express semantics mostly using graphical notations with little or no further parameter specifications as informal. As shown in Table 2, such approaches mostly address *security objectives*, of which we selected the CIA requirements and privacy as most relevant. We define the next group, semi-formal approaches, as using security semantics that require clearly defined attributes in given data types, accompanied by a graphical notation. Their range of possible security semantics is wide, still including mostly security objectives, but also supporting some security functions. Formal approaches employ mathematically exact statements. One can see that such approaches do not consider security objectives, but security functions and support for ICS, selective documentation and adherence to the control flow. Lastly, a subset of the formal approaches only addresses authorization, access control and related SoD issues. Almost all approaches contain support for expressing authorization and access control semantics, while authentication is almost always not addressed.

This evaluation leads to implications regarding the approaches' applicability in ICS. As the identification of security objectives in BPM can aid the design of an ICS by deducting possible control objectives, this could be performed using informal approaches. Besides the support of security objectives, due to their informal nature they would carry the benefit of being accessible to most stakeholders. The formal approaches on the other hand, are suitable for the actual control design, as they support security functions that enforce security objectives and are the link to implementation through security mechanisms. Their formal nature allows for a verifiable control design. Also, surrounding organizational issues, namely documentation and adherence to control flow, are supported. Lastly, besides explicit support for supporting ICS, the semi-formal approaches address all of the selected security semantics. The challenge in applying them to ICS and achieving compliance lies in combining the advantages of both other groups, being understandable for most stakeholders while allowing concise and verifiable statements.

CONCLUSION AND OPEN CHALLENGES

Based on legislation and further related statements and standards, we identified security semantics relevant to achieving compliance by modeling them in BPM and subsequently integrating them into the design and operation of ICS. We grouped those semantics into security objectives, security functions and defined the ICS itself as a third category for organization and documentation. A wide area of security semantics may be modeled using existing conceptual modeling extensions, with authorization and access control being most important and most commonly applied. Modeling security semantics in BPM can benefit design and operation of ICS by deriving control objectives from security objectives, by making correct implementation security functions a target of control activities and by modeling the control itself. Distinguishing between informal, semi-formal and formal approaches leads to the observation that security objectives are mostly adopted by the informal and semi-formal approaches, while the formal approaches mostly address security functions and ICS-related semantics. While the various examined approaches provide ways to express security semantics in BPM in a meaningful way, an integrated model covering all identified semantics is still missing. Also, presenting the semantics in an expressive yet intuitive manner remains a challenge.

REFERENCES

Ahn, G.J., Sandhu, R.S., Kang, M.H., Park, J.S. 2000. "Injecting RBAC to Secure a Web-Based Workflow System," *Proc. of the 5th ACM Workshop on Role-Based Access Control (RBAC '00),* pp 1-10.

Atluri, V., Huang, W. 1996. "An Authorization Model for Workflows," *Proc. of the 4th European Symposium on Research in Computer Security (ESORICS '96)*, pp 44-64.

Bertino, E., Ferrari, E., Atluri, V. 1997. "A Flexible Model Supporting the Specification and Enforcement of Role-Based Authorization in Workflow-Management Systems," *Proc. of the 2nd ACM Workshop on role-Based Access Control*, pp 1-12.

Fischer-Hübner, S. 2001. *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms.* New York, Springer.

Fox, C., Zonneveld, P. 2006. "IT Control Objectives for Sarbanes-Oxley," IT Governance Institute.

Goedertier, S., Mues, C., Vanthienen, J. 2007. "Specifying process-aware access control rules in SBVR," *Proc. of the International Symposium on Rule Interchange and Applications (RuleML '07,* LCNS 4824, Springer, pp 39-52.

Haworth, D.A., Pietron, L.R. 2006. "Sarbanes-Oxley: Achieving Compliance by Starting with ISO 17799," *Information Systems Management* (23:1), December, pp 73-87.

Herrmann, P., Herrmann, G. 2006. "Security Requirement Analysis of Business Processes," *Electronic Commerce Research* (6:3-4), October, pp 305-335.

Ho, Danny Ting-Yi., Jin, Yulong. 2009. "Business Process Management: A Research Overview and Analysis," *Proc. of AMCIS '09,* Paper 785.

Indulska, M., Green, P., Recker, J., Rosemann, M. 2009. "Business Process Modeling: Perceived Benefits," *Proc. of the 28th International Conference on Conceptual Modeling (ER '09)*, LCNS 5829, Springer, pp 458-471.

Jensen, M., Feja, S. 2009. "A Security Modelling Approach for Web-Service-Based Business Processes," *Proc. of the 16th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS '09)*, pp 340-347.

Jürjens, J. 2005. *Secure Systems Development with UML.* Berlin, Germany: Springer.

Karagiannis, D. 2008. "A Business Process-based Modelling Extension for Regulatory Compliance," *Multikonferenz Wirtschaftsinformatik (MKWI '08),* pp 1159-1173.

Kharbili, M.E., Stein, S., Markovic, I. Pulvermüller, E. 2008, "Towards a Framework for Semantic Business Process Compliance Management," *Proc. of the First International Workshop on Governance, Risk and Compliance (GRCIS '08)*, pp 1-15.

Knorr, K., Stormer, H. 2001. "Modeling and Analyzing Separation of Duties in Workflow Environments," *Proc. of the 16th Annual Working Conference on Information Security (IFIP/Sec '01)*, pp 199-212.

Kumar, A., Liu, R. 2008. "A Rule-Based Framework Using Role Patterns for Business Process Compliance," *Proc. of the International Symposium on Rule Representation, Interchange and Reasoning on the Web (RuleML '08),* LCNS 2460, Springer, pp 426-441.

Lodderstedt, T., Basin, D.A., Doser, J. 2002. "SecureUML: A UML-Based Modeling Language for Model-Driven Security," *Proc. of the 5th International Conference of the Unified Modeling Language, (UML'02),* LCNS 2460, Springer, pp 426-441.

Neubauer, T., Klemen, M.D., Biffl, S. 2006. "Secure Business Process Management: A Roadmap", *Proc. of the First International Conference on Availability, Reliability and Security (ARES '06),* pp 457-464.

Pernul, G., Tjoa, A.M., Winiwarter, W. 1998. "Modelling Data Secrecy and Integrity," *Data & Knowledge Enineering* (26:3), July, pp 291-308.

Rodríguez, A., Fernández-Medina, E., Piattini, M. 2007a. "A BPMN Extension for the Modeling of Security Requirements in Business Processes," *IEICE Transactions* (90-D:4), March, pp 745-752.

Rodríguez, A., Fernández-Medina, E., Piattini, M. 2007b. "An MDA Approach to Develop Secure Business Processes through a UML 2.0 Extension," *Computer Systems Science & Engineering* (22:5), September, pp 308-320.

Röhm, A.W., Herrmann, G., Pernul, G. 1999. "A Language for Modeling Secure Business Transactions," *Proc. of the 15th Annual Computer Security Applications Conference (ACSAC'99)*, pp 22-32.

Röhrig, S., Knorr, K. 2004. "Security Analysis of Electronic Business Processes," *Electronic Commerce Research* (4:1-2), January – April, pp 59-81.

Sadiq, S.W., Governatori, G., Namiri, K. 2007. "Modeling Control Objectives for Business Process Compliance*," Proc. of the 5th International Conference on Business Process Management (BPM '07)*, LCNS 4714, Springer, pp 149-164.

Siponen, M.T., Heikkar, J. 2008. "Do secure Information System Design Methods Provide Adequate Modeling Support?, " *Information & Software Technology* (50:9-10), August, pp 1034-1053.

Steinke, G. 2002. "Data pricacy approaches from US and EU perspectives," *Telematics and Informatics* (19:2), May, pp 193-200.

Tarantino, A. 2008. *Governance, Risk and Compliance Handbook: Technology, finance, Environmental, and International Guidance and Best Practices*, Wiley, Hoboken, New Jersey.

Wainer, J., Kumar, A., Barthelmess, P. 2007. "DW-RBAC: A Formal Security Model of Delegation and Revocation in Workflow Systems," *Information Systems* (32:3), May, pp 365-384.

Wolter, C., Menzel, M., Schaad, A., Miseldine, P., Meinel, C. 2009. "Model-Driven Business Process Security Requirement Specification," *Journal of Systems Architecture – Embedded Systems* Design (55:4), April, pp 211-223.

ACKNOWLEDGEMENTS

This work was partly funded by the European Regional Development Fund (ERDF).

COPYRIGHT