

# Towards A Formal Framework for Business Process Compliance

Kioumars Namiri<sup>1</sup>, Nenad Stojanovic<sup>2</sup>

<sup>1</sup>SAP Research Center CEC Karlsruhe, SAP AG, Vincenz-Prießnitz-Str.1, 76131  
Karlsruhe, Germany  
Kioumars.Namiri@sap.com

<sup>2</sup>FZI Karlsruhe, Haid-und-Neu-Str. 10-14, 76131 Karlsruhe, Germany  
Nenad.Stojanovic@fzi.de

**Abstract:** The advent of regulatory compliance requirements such as Sarbanes Oxley Act has forced enterprises to set up a process for managing an effective internal controls system on business processes. In this paper a formal framework consisting of a formal definition of business process compliance and a set of properties is proposed. A system implementing the formalization must satisfy the given properties. The advantage is that enterprises can verify whether their system responsible for achieving business process compliance itself is compliant in terms of checking whether its current state fulfills the given properties. The proposed model and its properties are motivated and exemplified using a scenario, showing the current challenges in achieving business process compliance at a use case company.

## 1 Introduction

Effective and efficient compliance management has become a very important issue for successful businesses. Regulation such as the Sarbanes Oxley Act 2002 (SOX) [Sox02] requires the documentation and implementation of an effective Internal Controls system in enterprises. COSO (Committee of Sponsoring Organizations of the Treadway Commission) defines in [Cos92] the internal controls as a “process” designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Following is a summary of the internal controls process:

Identify all the **Significant Accounts** in the company. Identify all **relevant Business Processes** that affect those accounts. Define one set of **Control Objectives** for each relevant business process. These control objectives are specific to the enterprise and must hold for that particular process. Continuously assess the **Risks** for the enterprise by identifying their identification for each control objective. Based on the risk assessment, design and implement a set of effective **Controls** in order to prevent or detect the occurrence of the identified risks. The controls must be tested and used in daily operations.

The realization and testing of the internal controls process effectiveness as described above is considered to be expensive and time consuming [HFL05]. A part of the problem is the ad-hoc implementation of the process above, i.e. there is no clear separation of the business and control objectives in business processes (BPs). The source of the problem is that in most cases the regulations do not give any specific recommendation on how a company has to achieve the compliance, thus the compliance teams in companies mostly select an ad-hoc and not enterprise-wide integrated approach to achieve the internal controls compliance on business processes.

In this paper we introduce a formalization of the internal controls process for operative business processes, which we call *business process compliance*. Further we give a set of properties based on the sets and relations between them given in the specification. The properties should assure the consistency of the system developed for achieving business process compliance. The advantage of having a precise formal specification of business process compliance is the following: It gives a team consisting of technical engineers and compliance experts in a company who are responsible for implementing the compliance, the possibility to check whether the system developed for achieving business process compliance satisfies the formal specification given. Satisfying the formal specification means that the system responsible for achieving the business process compliance must i) contain the sets and implement the relations given in the formal definition of business process compliance and ii) behave consistent to the sets of properties given. The added value is that it can serve as i) the basis for the verification of the business process compliance at a company – i.e. assure that the system is built as specified in the formal definition, ii) the basis for high level validation of the system responsible for business process compliance -i.e. assure that the system works as originally intended.

This paper is structured as follows: section 2 starts with a scenario that shows how the internal controls process is achieved at a use case company. In section 3, the formal definition of business process compliance as an interconnection of business process management and internal controls management is introduced. This is further exemplified by revisiting the scenario. Section 4 introduces and discusses the properties responsible for the consistency of business process compliance, whereas sections 5 and 6 describe the related work and concludes the paper stating some future research directions

## **2 Motivating Scenario**

The scenario presents how business process compliance is achieved at a use case company by highlighting the first class entities involved. It exposes the reasons along which the formal model proposed in this work is established, i.e. presents the scenario-driven methodology used to derive the sets and relationships between them, which are used to formally define business process compliance.

The business of the use case company looks as follows: For serving its customers orders, the company depends on material types supplied by external vendors in the market. The market for those material types – lets say material types 4 and 5, required for the production - is highly dominated by big market players. The company has decided to keep a certain amount of material types in stock in order to eliminate potential production delays caused by delayed suppliers' delivery.

In following the way the controls are derived and assured on *purchasing process* of the use-case company is shown. The concentration is on the *purchase-request* sub process, which deals with creating and approving internal requests for purchasing goods before they are submitted to an external supplier. The purchase request sub-process of the company looks as follows: It begins when an *Operational Department (OD)*, which releases a *Demand* for materials and submits it to the *Purchasing Department (PD)*. The PD selects a possible *Supplier* and forwards the *quotation* of the selected supplier (*SupplierQuote*) to the OD. The OD can either accept or reject the quotation. Acceptance is signaled to the PD by creating a *Purchase Request (PR)* based on the originally created Demand and submitting it to the PD. The PR then has to be approved by the PD before it is sent to the selected supplier.

## **2.1 Identification of significant accounts, relevant business processes and risks**

Compliance experts together with accounting experts identify *Inventory* as one of the most important (significant) account items in the balance sheet of the company. The reason is that this account has several influences on the liquidity situation and the profitability of the company. Hence, the company faces the permanent **risk**, that it is forced to *reject additional customer orders due to a lack of credit limit*. Compliance experts together with management reach a conclusion that the *purchasing process* together with the *warehousing process* is a *relevant business process* for the inventory account.

## **2.2 Control Identification**

The purchasing manager meets with the compliance experts and they identify the following list of *controls* on purchase request sub-process to *mitigate* the identified risk:

### **2.2.1 Control CA1: Purchase Release Strategy**

Each involved employee in the OD has to create the necessary PRs for material types 4 and 5 at least two months before they arrive in the warehouse.

### **2.2.2 Control CA2: Check requests for materials in stock**

A PR containing materials of type 4 or 5 and a total volume amount greater than 10000 \$ will not be approved if the available material type in stock is two times higher than the total volume of the PR.

### **2.2.3 Control CA3: Minimum Number of Suppliers**

For PRs which contain materials of type 4 or 5 and a total amount greater than 10000 \$, there must exist valid contracts with at least two different possible suppliers and the according supplier quotes (*SupplierQuotes*) are not allowed to be older than six months.

## 2.3 Control Implementation

In following describes how each control is implemented:

### 2.3.1 Implementation of control CA1 (Purchase Release Strategy)

The control will be implemented by analyzing the monthly generated reports of type *A1Report*. This report contains the necessary information about the date of the PR creations. A new role called *Control Tester* is conscribed by the management team to test the effectiveness of the control implementation.

### 2.3.2 Implementation of control CA2 (Check availability of materials in warehouse)

Similarly a report type (*A2Report*) exists, which contains the necessary information about all materials in the warehouse and their availability. The output of the monthly manually generated *A2Reports* and *A1Reports* are analyzed to determine possible violations of the conditions in the control. As well, the control tester has to verify the effectiveness of this control implementation.

### 2.3.3 Implementation of control CA3 (Minimum Number of Suppliers)

The control tester waits until the valid *SupplierQuotes* become older than six months, hence the minimum number of suppliers of at least *two* would be violated. The tester then creates a PR for material types 4 and 5 to test whether it gets approved or not.

## 2.4 Results of Control Effectiveness Tests and Corrections

**Test of CA1:** ReportA1 was not generated at all for several months. Thus assessing the effectiveness of this control for these months is not possible.

**Test of CA2:** The control tester reports for the months the *A1Report* was generated that the effectiveness for CA2 can be verified, but no statements regarding the effectiveness of CA2 for the months the *A1Report* was not generated can be made.

**Test of CA3:** The control tester reports that he generated three purchase requests for one of them the minimum number of suppliers was 1 and for the other two requests the *SupplierQuotes* were older than six months. The latter two purchase requests were passed and became approved, thus he considers the control as not effective. There were interviews conducted with the employee responsible for maintaining the *SupplierQuotes*. He explains that one month before the ending of the supplier quote's validity he triggers a process called *RfQ-Processing*, which generates a *request for quotation* for certain material types for some selected suppliers. Since he is not aware of the *PRs*, in particular the total amount of them, he does not know when to trigger the *RfQ-Processing*. This is due to the fact that a valid supplier quote can be taken for a *PR* with a total amount lower than 10000 \$ and the same supplier quote can not be taken for another *PR*, which has a total amount higher than 10000 \$.

Based on the problems detected above the management of the company together with compliance experts decide to define the following additional control:

**Control CA11: Report Execution Control** The *controlling department* has to generate the A1Report and A2Report on a monthly basis.

Further the *RfQ-Processing* will be integrated into the purchase request sub-process.

### 2.5 Analysis: First class entities and relations in a business process compliance

The first obvious result through the observation of the internal controls process described in the introduction and its instantiation at the use case company is the following: The first class entities in a model for business process compliance in a company are the *accounts*, *risks*, *business processes*, and the *controls* on them.

In addition, the control tests at the company resulted that the existence of the newly added control CA11 was required for the effectiveness of some other controls (CA1 and CA2). Thus, an *interdependency* relationship between some controls in a business process exists. On the same note, the existence of some controls on a business process in parallel could block the execution of the business process. In this case the controls would *contradict* each other. Moreover, the effectiveness of the “Minimum-Number of Suppliers”-control on purchase request sub-process requires the integration of another process, namely the *RfQ* sub-process into the purchase request sub-process.

## 3 A Formalization for the Definition of business process compliance

In the following, the logical relationships between the first class entities identified and introduced by the scenario are captured. The core elements of the formal definition following are a set of accounts (*ACCOUNTS*), the risks (*RISKS*), the business processes (*BPS*) in a company and a set of controls (*CONTROLS*) on the business processes (See figure 1). A system responsible for business process compliance must contain the given sets and implement the relationships between them.

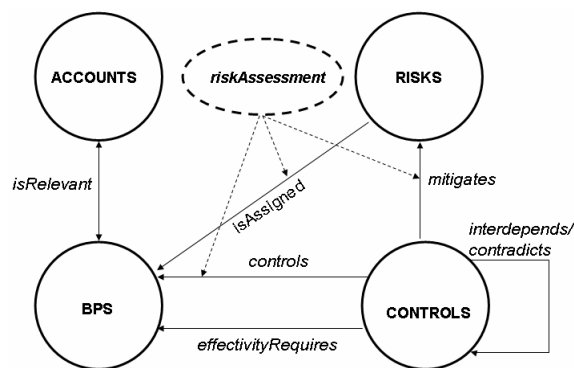


Figure 1: The involved entities and their relationships in business process compliance

### 3.1 Business Process Compliance Definition

**Definition:** A tuple  $BPCD = (ACCOUNTS, BPS, RISKS, CONTROLS, isRelevant, controls, effectivityRequires, mitigates, isAssigned, riskAssessment, interdepends, contradicts)$  is called the *Business Process Compliance Definition*, with:

- $ACCOUNTS$  is a set of significant accounts
- $BPS$  is set of business processes
- $RISKS$  is a set of risks
- $CONTROLS$  is a set of controls
- Relation  $isRelevant \subseteq BPS \times ACCOUNTS$  is a many-to-many mapping of BP-Account assignments.
- $Controls$  is a total function  $CONTROLS \rightarrow BPS$ . Further:  
 $control\_assigned\_bps : (ctl:CONTROLS) \rightarrow 2^{BPS}$  (with  $2^{BPS}$  denoting the power set of BPS) is defined as:

$$control\_assigned\_bps = \{bps \in BPS \mid controls(ctl, bps) == TRUE \}$$

- Relation  $effectivityRequires \subseteq CONTROLS \times BPS$  is a partial mapping of Control-BP-assignments.
- Relation  $mitigates \subseteq CONTROLS \times RISKS$  is a total mapping
- Relation  $isAssigned \subseteq RISKS \times BPS$  is a partial mapping of risk-BP-assignments.

Further:  $risk\_assigned\_bps: (rsk:RISKS) \rightarrow 2^{BPS}$  is defined as:

$$risk\_assigned\_bps = \{bp \in BPS \mid isAssigned(rsk, bp) == TRUE\}$$

- Relation  $riskAssessment \subseteq (2^{RISKS}, BPS, CONTROLS)$  is a set of tuples of type  $(rks, bps, ctl)$ , where  $rks \in 2^{RISKS}$ ,  $bps \in BPS$  and  $ctl \in CONTROLS$ .
- Relation  $interdepends \subseteq CONTROLS \times CONTROLS$  is a partial mapping, which identifies those controls depending on each other.
- Relation  $contradicts \subseteq CONTROLS \times CONTROLS$  is a partial mapping, which identifies those controls contradicting each other.

### 3.2 Scenario revisited

Figure 2 illustrates the occurred relations in BPCD  $effectivityRequires$ ,  $controls$  and  $interdepends$  using the scenario discussed in section 2.

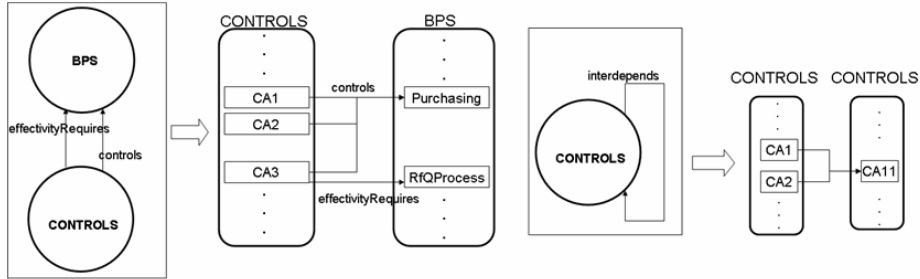


Figure 2: The relations *controls*, *effectivityRequires* and *interdepends* in the scenario

## 4 Semantics of Business Process Compliance Definition (BPCD)

Based on the formal definition of business process compliance, a set of properties that must hold on a system responsible for business process compliance is introduced, i.e. a system implementing the formal definition BPCD. The following set of properties should support the verification of that system in such a way that during its definition and evolution these properties must be satisfied. The evolution of business process compliance in an enterprise is forced by the continuous change in the business environment and the risk landscape of an enterprise. This change forces the enterprises to continuously adjust their business process compliance. In this context COSO directly calls to “manage the change” in the enterprise, which implicates the evolution of a system for business process compliance.

### 4.1 The Properties of Business Process Compliance

The existence of pair wise disjoint countable infinite set of elements in *ACCOUNTS*, *BPS*, *CONTROLS*, and *RISKS* is assumed. The description of each property and its formalization is as follows:

**P1.** The accounts are subjects to transactions caused by business processes. Thus a significant account has always a relevant business process. Formally:

$$\forall acc: ACCOUNTS \mid \exists bps: BPS \wedge isRelevant(bp, acc) == TRUE$$

**P2.** A relevant business process (respectively its control objectives) may contain several risks. The controls on business processes only exist in order to prevent or detect risks. If no risk is assigned to a relevant business process, then there is no control assigned to it and thus for that business process no risk assessment exists. Formally:

$\forall bps: BPS; ctl: CONTROLS \mid bp \notin \text{ran}(isAssigned) \Rightarrow \text{controls}(ctl, bp) == FALSE \wedge (isAssigned \circ \text{controls}^{-1} = \emptyset)$ , where  $R \circ V$  represents the relation composition between two relations  $R$  and  $V$ ,  $R^{-1}$  is the inverse relation of  $R$  and  $\text{ran}(R)$  is the range of a relation  $R$ .

**P3.** A control in some constellations requires other sub- respectively side business processes related to the relevant business process to be effective. In order to assure the effectiveness of the compliance of such related business processes, they have to be treated as relevant business processes, thus a business process which is required for a control to effectively control a relevant business process is also a relevant business process itself. Formally:

$\forall ctl: CONTROLS; bps, bps': BPS; acc: ACCOUNTS \mid$

$isRelevant(bps, acc) == TRUE \wedge \text{controls}(ctl, bps) == TRUE \wedge \text{effectivityRequires}(ctl, bps') == TRUE \Rightarrow$

$isRelevant(bps', acc) == TRUE$

**P4.** Closely related to the above property is the fact that a control is not allowed to be assigned to a relevant business process and at the same time require that business process for its own effectiveness. Formally:

$\forall bps, bps': BPS \mid$

$bps \in \text{ran}(\text{effectivityRequires}) \wedge bps' \in \text{ran}(\text{controls}) \Rightarrow bps \neq bps'.$

**P5.** For each business process, which is considered to be risk relevant, there must exist at least one control assignment. Formally:

$\forall bps: BPS; rsk: RISKS; \exists ctl: CONTRLOLS \mid$

$isAssigned(rsk, bps) == TRUE \Rightarrow \text{controls}(ctl, bps) == TRUE$

**P6.** A risk assessment must be consistent. Consistency in this context is defined as follows: if a business process is subject to risk assessment (i.e. is risk relevant), at least one control must be assigned to that business process. The risk assessment is only consistent, if the assigned control in fact mitigates the risk that was assigned to that business process. Formally:

$\forall (bps, rks, ctl) \in \text{riskAssesment}; rsk : RISKS \mid$

$\text{control\_assigned\_bps}(ctl) = \text{risk\_assigned\_bps}(rsk) \wedge rsk \in rks \wedge$

$\text{mitigates}(ctl, rsk) == TRUE$

**P7.** If a risk is assigned to a relevant business process, then there is at least one control assigned to that business process and a risk assessment for that business process exists. Formally:

$$\begin{aligned} & \forall bps: BPS; \exists ctl: CONTROLS / \\ & bp \in ran(isAssigned) \Rightarrow isAssigned(ctl, bps) == TRUE \wedge (isAssigned \circ \\ & controls^{-1} \neq \emptyset). \end{aligned}$$

**P8.** Two controls that block each other are not allowed to be assigned to the same business process. Formally:

$$\begin{aligned} & \forall ctl, ctl': CONTROLS; bps: BPS / \\ & controls(ctl, bps) == TRUE \wedge contradicts(ctl, ctl') == TRUE \Rightarrow \\ & controls(ctl', bps) == FALSE \end{aligned}$$

**P9.** A control must always have a purpose, which means it must always control a business process; otherwise its existence is not necessary in the system. This property is guaranteed through the design of the *controls* relation as a total function. Formally:

$$\begin{aligned} & CONTROLS \rightarrow BPS == \\ & \{controls: CONTROLS \rightarrow BPS \mid dom(controls) = CONTROLS\}, \text{ where} \end{aligned}$$

$dom(R)$  is the domain of the relation  $R$  and  $X \rightarrow Y$  is a partial function from set  $X$  to set  $Y$ .

**P10.** A control always interdepends on itself i.e. the relation *interdepends* is reflexive. Formally:

$$\forall ctl: CONTROLS \mid interdepends(ctl, ctl) == TRUE$$

**P12.** A control is not allowed to be designed in such a way that it blocks the business process i.e. the relation *contradicts* is not transitive. Formally:

$$\forall ctl: CONTROLS \mid contradicts(ctl, ctl) == FALSE$$

**P13.** The relation *interdepends* is transitive. Formally:

$$\begin{aligned} & \forall ctl, ctl', ctl'': CONTROLS / \\ & interdepends(ctl, ctl') == TRUE \wedge interdepends(ctl', ctl'') == TRUE \Rightarrow \\ & interdepends(ctl, ctl'') == TRUE \end{aligned}$$

**P14.** The relation *contradicts* is symmetric. Formally:

$$\forall ctl,ctl':CONTROLS /$$
$$contradicts(ctl,ctl') == TRUE \Rightarrow contradicts(ctl',ctl) == TRUE$$

**P15.** All controls that are in an interdependency relationship are assigned to the business process. Formally:

$$\forall ctl,ctl': CONTROLS; bps :BPS /$$
$$interdepends(ctl,ctl') == TRUE \wedge controls(ctl,bps) == true \Rightarrow$$
$$controls(ctl',bps) == TRUE$$

A system for business process compliance according to the formal specification given in section 3.1 and its evolution is considered to be consistent, if the properties P1-P15 are permanently satisfied by the system.

#### 4.2 The Determination and Validation of the Properties

The domain-specific-knowledge about the internal controls compliance for business process reflected in the properties above is determined by following sources:

- Analysis of non IT-related COSO framework as a de facto-standard for realizing the internal controls compliance recognized by regulation bodies and compliance/auditing experts
- Analysis of Accounting Standards of the Public Company Accounting Oversight Board (PCAOB) [Pca2], which has also ratified COSO.
- Participation in internal controls compliance projects

The resulted constructed formal framework including the properties has been introduced and discussed with compliance experts in order to verify its business level correctness. Based on the taken approach described above, the completeness of our proposed model has been assured as much as possible.

### 5 Related Work

[SGN07] shows how business processes can be annotated with the controls modeled through a specialized modal logic based on a normative system theory. In [NS07], the *controls* relationship given in BPCD has been detailed by showing the semantic relationships between a control and different dimensions of a business process. A concrete approach for assuring the effectiveness of controls on business process executions equipped with a flexible reaction strategy in case of control violations was shown there.

The works concerned with formalization of risks, business processes and the relationships between them have been considered as related. [BA02] proposed a conceptual model of risk and defines it as a probable *event* and its impact on an *entity*. Putting our formal model in the context of that work, the entities in the conceptual model of risks are operative business processes affecting a significant account. A risk on such a business process is any probable event which can cause some deviations on expected outcomes, namely in our case financial misstatements asserted by an enterprise or some unexpected operative results of that business process.

The work of [MR05] provides an appealing method for integrating risks in business processes. The proposed technique for “risk-aware” business process models is developed for EPCs (Event-driven Process Chains) using an extended notation. Their notation however is not able to capture *all* types of process-related risks as introduced in that work. In particular, it is not possible to capture risks related to process elements other than functions.

Similarly [GV06] present a logical language PENELOPE that provides the ability to verify temporal constraints arising from compliance requirements on effected business processes. Distinct from that work, the contribution of our work provides a precise model for business process compliance that can be used in a model driven approach to develop a system for managing the business process compliance.

[SKLP06] proposes a vertical and horizontal integration of risk management into process management: Horizontal integration is concerned with applying the risk management in a given process management phase in order to manage uncertainties or opportunities specific to the current context. Vertical integration is about managing the information about risk management while moving down in the process management lifecycle. We consider their approach as orthogonal to our model of business process compliance. We are concerned to formally capture the model of business process compliance in order to provide a formal specification of a system for business process compliance. While we see the four elements (account, business process, risk and control) as the essential first class entities in such a model, the above introduced works capture the interrelationship between risks and business processes including their management life cycles.

## 6 Future Research and Conclusion

In this paper a formal specification of business process compliance and a set of properties that must hold for a system that implements the formal definition given have been provided. The occurred sets and relations in the model were motivated by showing how the internal controls compliance on business processes is defined and achieved at a use case company. The usage of the formal model and the properties given can serve as a basis for verification of a system for business process compliance, i.e. to check whether the system implements the required sets and relations between them. Furthermore, validating whether the system remains consistent during its evolution can be performed with the help of properties.

Currently our model captures the entities involved and not the internal syntax and semantic of each entity. For instance the model does not make any statement about the composition of a business process or a risk, respectively its formalization. In addition, capturing the semantics of the relations *interdepends* and *contradicts* is currently not performed, i.e. it is not possible to detect any contradicting respectively interdependent controls automatically. The same applies for the adjectives *significant*, *relevant* etc, - i.e. it is not possible to determine what is a significant account or a relevant business process in a company. The advantage of having a precise formal model of the relations mentioned above and the risks in relation to formalized business processes would be the following: As seen in the scenario (see section 2), the starting point of each business process compliance project is the risk assessment for the enterprise. Having a well formalized representation of those risks and their semantic relationship to business processes and controls, a cooperative system landscape, which can propose a set of required controls on the business process according to the enterprise specific risk assessment can be provided.

## References

- [BA02] Bernard, J.-G., A. B. Aubert, et al. (2002). Le risque: un model conceptuel d'integration. Montréal, CIRANO: Centre interuniversitaire de recherche en analyse des organisations.
- [Cos92] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control – Integrated Framework, 1992.
- [GV06] Goedertier, S., Vanthienen, J. (2006): Designing Compliant Business Processes with Obligations and Permissions. International Conference on Business Process Management (BPM06) Workshops, LNCS 4103, S. 5-14
- [HFL05] Hartman, T.; Foley & Lardner LLP, “The Cost of Being Public in the Era of Sarbanes-Oxley,” June 2005
- [Pca2] Public Company Accounting Oversight Board (PCAOB), PCAOB Accounting Standard No. 2
- [NS07] Namiri, K., Stojanovic, N. (2007): Pattern-Based Design and Validation of Business Process Compliance. In: Proceedings of OTM Federated Conferences, Cooperated Information Systems (CoopIS), S. 59-76
- [SGN07] Sadiq, S. Governatori, G., Namiri, K. (2007): Modeling Control Objectives for Business Process Compliance. In: 5. International Conference on Business Process Management (BPM07), S. 149 – 164
- [SKLP06] Sienou A.; Karduck, A; Lamine E.;Pingaud H: Management of Business Processes: The contribution of Risk Management, Proceedings of COLLECTeR Europe 2006, 2006
- [Sox02] Pub. L. 107-204. 116 Stat. 754, Sarbanes Oxley Act (2002)
- [MR05] zur Muehlen, M.; Rosemann, M.: Integrating Risks in Business Process Models, Australasian Conference on Information Systems , ACIS05.