7-1-2013

Control Patterns - Bridging The Gap Between Is Controls And BPM

Thomas Schaefer
Institute for Information Systems (IWi) at the DFKI, Saarbruecken, Saarland, Germany, thomas.schaefer@iwi.dfki.de

Peter Fettke
Institute for Information Systems (IWi) at the DFKI, Saarbruecken, Saarland, Germany, peter.fettke@iwi.dfki.de

Peter Loos
Institute for Information Systems (IWi) at the DFKI, Saarbruecken, Saarland, Germany, loos@iwi.uni-sb.de

CONTROL PATTERNS – BRIDGING THE GAP BETWEEN IS CONTROLS AND BPM

Schäfer, Thomas, Institute for Information Systems (IWi) at the German Research Center for Artificial Intelligence (DFKI) and Saarland University, Campus, Building D32, 66123 Saarbrücken, Germany, thomas.schaefer @iwi.dfki.de

Fettke, Peter, Institute for Information Systems (IWi) at the German Research Center for Artificial Intelligence (DFKI) and Saarland University, Campus, Building D32, 66123 Saarbrücken, Germany, peter.fettke@iwi.dfki.de

Loos, Peter, Institute for Information Systems (IWi) at the German Research Center for Artificial Intelligence (DFKI) and Saarland University, Campus, Building D32, 66123 Saarbrücken, Germany, peter.loos@iwi.dfki.de

Abstract:

While playing an increasingly important role across various industries, the efficient management of legal and regulatory compliance requirements remains a challenge in modern organizations. Commonly, compliance is handled by separate organizational units and not well integrated with core business processes. Based on the area of information systems (IS) controls as mechanism to fulfil given requirements, this paper proposes a concept to bridge this gap between regulatory compliance and business process management. The presented concept enables linking process models with internal control systems and provides a common language for all parties involved. An approach is developed to identify and extract reusable control elements for regulatory compliance from real-world process specifications. These artefacts are formalized as "Control Patterns" (CPs). Inductive analysis methods are employed to identify reusable patterns. As a proof of concept, based on a sample of proven implementations of the software change management process, the paper analyses possibilities to extract, generalize and explicitly model IS controls.

Keywords: Business Process Management, Process Modelling, Internal Controls, Compliance, Control Patterns, IS Audit and Control

1 Introduction

Process complexity is continuously increasing in modern organizations. At the same time organizations must adhere to a rapidly growing plethora of internal as well as external laws, policies, directives and regulations (Caldwell, 2012). Professional media identify this as a top driver for additional information security spendings in 2012 (Schwartz, 2011). A common way to tackle compliance requirements is the setup of an internal control system (ICS, see 2.2). For this, the requirements – which are usually presented in unstructured text format – are first transposed and grouped into "control objectives" (COs). For each objective, sets of measures are established, which support the achievement of the CO – these measures are denoted "controls". Organizations nowadays face the problem, that the link between their ICS and business processes is not well established. This starts already with a gap at the design stage. On one hand business processes are graphically modelled by BPM (business process management) experts in cooperation with business responsibles using dedicated methods and tools like EPC (Event-driven Process Chain) or BPMN (Business Process Model and Notation). On the other hand compliance and control aspects, which form the ICS, are managed by organizationally separated compliance and risk teams. The ICS is formalized separately in the shape of textual representations, often based on common frameworks like COSO (COSO, 1992), COBIT (ISACA, 1993) and ISO27001 (ISO, 2005) or control programs (e.g. SAS 70, ISAE 3402, SOx 404). An integrated perspective is not available in this case.

Business process compliance (BPC, see 2.3) as research domain aims at providing such integration mechanisms (Elgammal et al., 2011). In addition to traditional process models, compliance requirements are expressed in the shape of rules and formalized in declarative languages like LTL, FCL or CTL (Muehlen et al., 2007). Depending on the chosen method, these rules have then to be followed during process modelling stage (design-time BPC) or process execution stage (runtime BPC) (Governatori et al., 2008, Lu et al., 2008). Though research has been performed in this area for several years (Pesic, 2007) and promising approaches are available, such declarative formalization is still rarely used for managing regulatory compliance in practice. A limitation of current BPC techniques is the significant complexity and effort needed to formalize rules and maintain the rule base (El Kharbili et al., 2008). The transfer of compliance requirements, e.g. law texts, into suitable formal rules is not trivial and in practice, organizations often lack resources to accomplish this. Legal and compliance departments feature the skills to interpret law texts, but lack knowledge about process and rule modelling, vice versa accounts for BPM departments. This indicates that it is necessary to develop further concepts, which incorporate compliance and control requirements directly into process management in an efficient and accessible way.

The Control Patterns (CPs) presented here can be seen as a complementary approach to existing BPC research. Traditional BPC approaches often declare automated compliance validation of business processes as their primary objective and thus first of all build upon strict formal models, which aim at facilitating later IS implementation. This comes along with the price of usability and maintenance issues as mentioned above, especially for complex business processes and compliance topologies. CPs intend to bridge the gap between BPM and compliance from another angle: As a starting point, the CP-idea uses the currently most common business practices for process modelling (graphical activity sequences) as well as for compliance management (internal controls approach). By combining those two worlds, CPs provide a common ground for all stakeholders involved in BPM and compliance topics. As such, the CP approach clearly provides benefit on its own, but it might as well serve as an intermediary step to put organizations into a position, where they are better able leverage the potential of existing BPC approaches, ultimately heading towards extended compliance automation.

The intention of this paper is two-fold: First of all, the idea of Control Patterns shall be introduced and discussed. Second, to prove the practicability of the CP idea, an approach shall be presented, how a CP can be derived from a set of process models in a proof-of-concept exercise. Hence, the following two questions define the research goal:

a) Is it possible to transfer the "design pattern" idea to the cross-section of BPM and compliance in order to achieve better integration between current practices in both domains?

b) If Control Patterns could contribute here, how can those be created based on existing process implementations?

Subsequent to this introduction, in chapter 2 relevant terminology and related research is recapitulated. Chapter 3 describes the chosen research approach based on inductive analysis. Building upon this, the paper examines in chapter 4 possibilities to extract and generalize internal controls based on real-life process specifications. The control aspects will be formalized in the shape of reusable, modular process elements for compliance-aware process design and improvement. As a proof of concept, with the Software Change Management process a palpable example out of the IS controls domain is investigated. Three entities of this process, which are implemented and proven in practice at three different organizations, are examined, and based on this a generalized Control Pattern "Production Deployment" is derived in chapter 5. The results are summed up in chapter 6 and an outlook is given.

2 Terminology and related research

2.1 Business Process Management

Houy et al. (2010) performed a literature review on business process management. According to this, a business process can be understood as a chronological sequence of activities to fulfil a business task during which a value is delivered by transformation of materials or information. Business process management denotes a set of methods, techniques and software tools to support the design, implementation, monitoring and analysis of operational business processes in order to facilitate an optimized value creation (van der Aalst, 2013). Current research activities support an evolutionary view, where BPM itself is conducted as an iterative process following a lifecycle model to facilitate continuous improvement of business processes (Scheer and Brabänder, 2010).

2.2 Compliance and Internal Control Systems

Compliance is defined as "ensuring that business processes, operations and practice are in accordance with a prescribed and/or agreed set of norms" (Sadiq and Governatori, 2010). This is to be clearly distinguished from another understanding of the term "compliance" common in BPM research, where it denotes as "process compliance" the alignment of process instances to their respective model or model to meta-model (Chesani et al., 2008). In the given sense of regulatory compliance, it encompasses an iterative compliance and risk management process including the implementation of detective, preventative and compensating measures to fulfil compliance requirements – so called "controls". The totality of such controls constitutes an organizations internal control system (ICS). The Committee of Sponsoring Organizations of the Treadway Commission established in 1992 the de-facto ICS standard with their COSO framework (COSO, 1992). An ICS according to COSO strives to establish a process, which allows a valid assessment of the effectiveness and efficiency of business operations, the reliability of financial statements and compliance with given regulation.

2.3 Business Process Compliance

Business process compliance constitutes an important element at the junction of BPM and compliance. Conceptually, BPC denotes the execution of business processes in adherence to applicable internal and external regulations and as such represents an integrated view on business processes and compliance. El Kharbili et al. (2008) performed a review on the state-of-the-art of business process compliance checking. They distinguish between three general validation mechanisms for BPC: While the "design-time" approach uses validation of process models during the modelling phase to identify compliance conflicts, the "runtime" approach inspects via process monitoring individual process instances during

execution in order to highlight potential discrepancies towards a predefined set of rules. "Backward" validation as the third concept follows a retrospective approach and uses data and process analysis methods to extract potential compliance violations ex post. Compliance requirements are often expressed in the shape of rules and formalized in declarative languages like Event Calculus, LTL, FCL or CTL (Governatori et al., 2008, Lu et al., 2008, Sadiq and Governatori, 2010, Muehlen et al., 2007, F.M. Maggi, 2011, Pesic, 2007). Although they acknowledge the relevance of formal modelling, El Kharbili et al. (2008) view the complexity of current solutions and prior knowledge necessary for users as a significant adoption barrier.

2.4 Patterns

Patterns in the sense of observable regularities in a certain environment are discussed in various research disciplines. A specific class of patterns are "design patterns", which, after their definition, are intended to serve as modular templates for future real-world applications in a "good practice" style. The current understanding of design patterns originated from the field of architecture and construction (Alexander et al., 1978). The concept gained increased attention in computer science and IS research through the well-known Software Engineering Design Patterns (Gamma et al., 1995). With "Workflow Patterns" (van der Aalst et al., 2003) the concept was transferred to the BPM domain. As stated before, the given paper transfers the basic design pattern idea in the shape of "Control Patterns" to the domain of internal controls and regulatory compliance of business processes. The term "Control Pattern" is used in a similar context by Namiri and Stojanovic (2007), yet they follow a different approach as they primarily focus on so called "application controls", which can be implemented hard-coded into application systems to automatically support selected compliance requirements. Similarities exist as well between CPs and the concept of Compliance Fragments (Schumm et al., 2010), although the approach for the generation of patterns and the area of application differ with the latter one aiming at dynamically hiding process parts, e.g. in an outsourcing scenario.

3 Research approach

As stated before, the given paper aims at the creation of generic, reusable process snippets denoted Control Patterns, which afterwards may be drawn upon to support regulatory compliance in business processes. To achieve this, a technique from the domain of pattern research is applied, building upon the "three-occurrences-rule" (Winter, 2009) (a solution that has been deployed in three different situations can be considered a pattern). Following an inductive research approach, CPs are extracted through analysis of a set of real-world process implementations. Figure 1 provides an overview of the approach including a reference where the respective steps are discussed for the given case study:

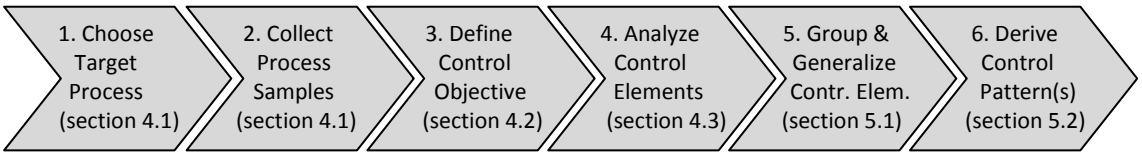

Figure 1: Research Approach

As a first step, the target process to be examined has to be chosen. Then (at least) three exemplary real-world implementations of this process have to be acquired. The sample implementations have critical influence on the quality of patterns potentially derived from them. Hence characteristics of sample organizations (e.g. industry, size, culture) are to be taken into account and mature, proven implementations should be preferred. As a sub-step, the representation of the sample processes has to be unified. They are (re-)modelled by a process expert in a common modelling notation like EPC or BPMN and reviewed by a second person for consistency. As a third step, from an internal controls perspective a control objective, where the process implementations are evaluated against, needs to be formulated. This is done based on analysis of law texts or compliance requirements for the domain of

the sample process. If standards or generalized control frameworks (e.g. Cobit, COSO) are available for the sample process domain, the control objectives defined within can be drawn upon. As it is shown in chapter 4.2, most of the time such a control objective will be multi-faceted, i.e. it will state more than one elementary requirement to be fulfilled.
In a fourth step, all sample process implementations are reviewed by a skilled person for elements supporting the defined control objective, the so called "control elements". These are highlighted in the processes, referenced and collected in a tabular overview including information, which aspects of the given, typically multi-faceted control objective are supported. This step is in large parts similar to what auditors usually do in practice during process assessments. The outcome of this step can be improved by a second independent sample process review and subsequent result matching.
When all sample processes have been reviewed, in step five a summarized set of all identified control elements (indicating the control objective aspects they support) is created. In the case that similar control elements exist, which originate from different sample processes, but represent the same subject (e.g. "user acceptance test" vs. "perform end user test"), these are merged into a single generalized control element and it is documented, in which sample processes they occur (cp. section 5.1).
In the final step six, generalized Control Patterns are derived from the prepared data. A threshold t is defined with t being the minimum number of sample processes, in which a control element must occur in order to qualify for inclusion in a Control Pattern. The reasoning behind this is, that a control element, which has been found in many of the sample processes, is likely to be relevant for other similar process implementations in the future. When the relevant control elements are identified, a process expert again reviews those areas of the sample processes, where the relevant control elements occur. Control elements, which are closely related in the process model (from a graph perspective) are grouped together. Model areas with a high density of relevant control elements are primary candidates for the deduction of Control Patterns. For such cases, the process expert attempts to derive a generalized process part from the given sample implementations, which still reflects the respective group of control elements – a Control Pattern. This pattern is then validated again by a second skilled person against the source process implementations as well as for its support of the defined control objective. With this model, there is an n:m-relationship between identified control elements and potentially derived Control Patterns.
Bearing the aim of practical applicability of the Control Patterns in mind, the following rules have been set up:

1. Don't create trivial patterns, which represent only one control element. This may lead to an abundance of patterns, which are difficult to manage and to use (trivial patterns might be interesting though from a academic perspective though, e.g. as "base" patterns).

2. Don't create overly complex patterns, which e.g. represent a whole process (even if many control elements are sequentially linked, split models in such cases). Such patterns are not easy to understand, to reuse and to integrate as fragments into existing processes. In addition, generalization from sample processes will be more complex.

From the rules above follows as a suggested rule of thumb, that a Control Pattern should contain 3-5 process steps with 4-10 model elements.

4 Software Change Management – control elements

4.1 Process Selection and Sample Aquisition

In order to discuss common IS control elements inside processes, which can be generalized into CPs later on, an exemplary evaluation is performed based on the Software Change Management (SWCM) process (also referred to as Release Management or Software Deployment process). As a first step according to our research method, this process was chosen, because it can be found in many organizations and it features several control elements. In short, it describes how requested software/program changes to application systems are migrated to production. Note, that from an IS

control perspective, this is to be distinguished from the general software development process – it's closely linked, but not the same. As defined by the research method step 2 (section 3), three real world SWCM process implementations were collected (two IT service providers, one financial institution; two organizations with 100-500 employees, one with >1000 employees). At all companies the reviewed SWCM process was in operation for at least three years at the time of the review. Given this, together with the size of the source organizations and level of regulation in their domains, the maturity of the sample processes is considered sufficient for the chosen research approach. The sample processes were initially represented as textual descriptions or (semi-formal) process models. In a first step, these representations were transposed by experienced modellers into EPCs to create a common basis for the subsequent analysis. In the EPCs, trivial events are omitted as it is common to avoid model pollution.

4.2 SWCM Control Objective

Subsequently, step 3 of the research method (section 3) requires identifying a relevant control objective. From a controls perspective, the SWCM process belongs to the domain of information security management. Thus it is reasonable to identify those elements in the sample processes, which support goals of information security[1], e.g. the well-known "C-I-A" triad of confidentiality, integrity and availability (Solomon and Chapple, 2004). "Confidentiality" means that only authorized people or systems have access to information. "Integrity" stands for the correctness of information and processing, including that information cannot be altered undetected. "Availability" describes the aim of having information available when and where it is needed. Internal control systems generally define a set of subsidiary control objectives to achieve such overall goals. As one such example, the SWCM control objective used here is derived from a common framework in the domain, COBIT (ISACA, 1993). It shall be as follows:

Controls provide reasonable assurance that changes to the production environment are approved, prioritized, tested and documented.

In practice, this would be the starting point for an auditor who is reviewing an organizations SWCM process. According to step 4 of the research method (section 3), the SWCM control objective is used as a reference for the analysis of the three sample processes. In the following chapter, the evaluation procedure is described in detail based on one of the sample process implementations. Corresponding evaluations for the two other samples can be provided on request. The process description is accompanied by a figure showing a process overview. In this overview, the control elements discussed subsequent to each description are marked with circles containing counters as identifiers for reference in the format [Process Number].C[Control Number], e.g. "I.C4".

4.3 SWCM Process Analysis

4.3.1 SWCM I. – Process Description

In the presented sample SWCM process (Figure 2), a business department starts the process by requesting a software change. This leads to the initiation of a linked sub-process for software development with a new or changed component developed as its result. Now the Business Analyst (BA) as responsible for the change triggers the deployment. He fills in a dedicated change management paper form. Based on this, the IT Operations department installs the changed software in a test environment. When done the BA performs a unit test. If the test fails this is documented, the current change is closed and a new change is requested. Otherwise if the unit test is successful a User

[1] It is not feasible to discuss the topic of information security, related control objectives and the C-I-A triad on a technical level in detail within the given scope. Please refer e.g. to Solomon et al. (2004) for further insights. For the purpose of this paper, information security shall serve as one example control domain, having confidentiality, integrity and availability of information systems as its major goals.

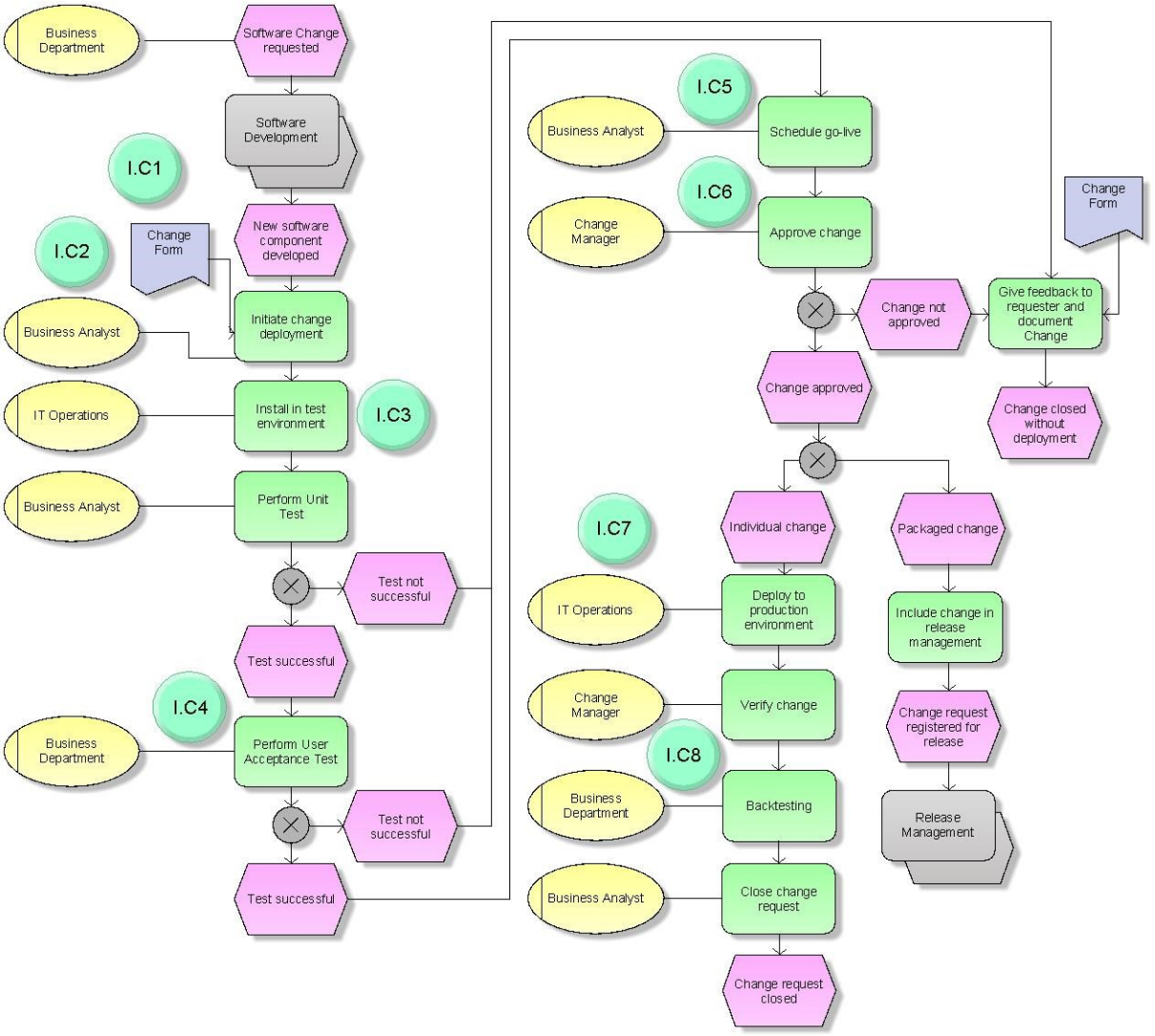

Figure 2: Software Change Management Process I.

Acceptance Test is to be performed by the affected business users and a sign-off is requested. If the test was successful the process proceeds to the next phase. In coordination with the involved entities the BA schedules the go-live of the given change. Here it is distinguished between changes that are put into production individually (high urgency) and changes that are accumulated and bundled into periodic software releases for go-live. After all relevant information has been collected the change form is given to the supervising Change Manager for final approval of the change. Now the current process either links to the release management process or IT Operations carries out the actual implementation. Subsequently the Change Manager verifies the change and depending on the change impact business departments perform backtesting (validation) activities. Finally the BA closes the change instance.

4.3.2 SWCM I. – Control Elements

Based on the previous process description, a selection of control elements can be identified, which support the control objective (CO) defined in section 4.2. As a reminder, it stated that changes shall be appropriately approved, prioritized, tested and documented. The control denoted I.C1 in Figure 2 refers to the fact, that the process model explicitly includes a paper form to document software changes. This supports a structured, repeatable process and helps to collect all relevant information.

Obviously this supports the documentation requirement of the CO. Furthermore this document constitutes the reference point for all approvals during the process. The next control I.C2 highlights the fact, that with the BA a defined individual takes responsibility for a change. This ensures follow up and timely processing of the change as goals within the given CO. Usage of a test system constitutes control I.C3. The next control I.C4 relates to the user acceptance test required during the given sample process. This again supports the CO requirement to test changes, but even more important this is a crucial step for appropriate change approval before go-live, another core aspect of the CO. The relevant business departments perform tests here. The following control I.C5 is concerned with scheduling of changes and as such is coherent with the change prioritization required by the SWCM CO. It could be argued that this is late for prioritization as a lot of resources have already been invested in a change here; still there might have already been earlier prioritization in the hidden sub-process for Software Development. Regardless of this, prioritization of change implementation is an important element at the current process stage as it decides whether changes are supposed to go live directly or as part of a future release, potentially several months later. After all preparation steps have been performed the Change Manager as a supervising entity for all changes is asked for final approval before go-live in I.C6. This clearly supports the CO objective of proper change approval and the completeness of documentation is checked. The next control in Figure 2, I.C7, points out that the actual implementation of a change is performed by dedicated IT Operations personnel. Though not very obvious at first glance, this is a very valuable control. The capabilities to implement changes in a production system can be limited to a small group of people this way. This limits the risk of transport of unauthorized software changes or even malware to production systems which could severely impact system confidentiality, integrity and availability. Without such proper segregation of duties, e.g. developers might unintentionally move unapproved test software to production. The last control aspect highlighted in the process, I.C8, covers ex-post controls for changes. The change verification by the Change Manager as well as a backtesting procedure from business side support the integrity of the system.

5 Control Patterns

5.1 Control Elements Consolidation

After all sample processes have been analysed, the identified control elements are collected in a common table as described in step 5 of the research method (section 3). As a reminder, elements appearing in multiple processes are combined into a generalized control element. Table 1 presents an overview of the identified control elements and the process samples where they occurred. It lists both the link to high level “C-I-A” information security goals and the specific SWCM control objective aspects as they were identified during the assessment (see chapter 4.3.2).

The overview visualizes common ground between the three process representations. It also shows where the position and order of certain control elements in relation to the process sequence varies between our sample processes. The reviewed sample SWCM processes differ in perspective: While SWCM I., which was presented in detail in section 4.3, puts an emphasis on the testing and rollout of a change after development, the second implementation SWCM II. rather takes a developers perspective and aims at ensuring that all relevant approvals have been given and proper prioritization has been performed before a change is developed. SWCM III. features as a specific, that it is the only process with an explicitly modelled backout procedure. Furthermore it goes beyond the perspective of a single change and indicates surrounding support processes. None of the sample processes explicitly covers all of the extracted control elements. Some of these differences might indicate potential areas for improvement in the individual processes. The previously extracted control elements can be used as a foundation to develop generalized process fragments as will be shown in the subsequent chapter.

Control Element[1)]	IS goal[2)]	SWCM CO[3)]	SWCM I.[4)]	SWCM II.[5)]	SWCM III.[6)]
a) Standardized, structured case documentation	I, A	d	I.C1	II.C3	III.C1
b) Timely case processing through establishment of case ownership	A	p	I.C2	II.C1	III.C2, III.C6
c) Business prioritization for change	I, A	p	-	II.C4	-
d) Business approval for change before development	I	a	-	II.C2, II.C4	III.C3, III.C4
e) Staging concept – usage of dedicated test infrastructure	C, I, A	t	I.C3	-	-
f) Testing (general)	I, A	t	I.C3	II.C9	III.C5
g) User acceptance testing and business sign-off	I	t, a	I.C4	-	-
h) Technical scheduling of implementation in production	I, A	p	I.C5	II.C6, II.C8	III.C4
i) Final go-live approval by supervison entity	I, A	a	I.C6	II.C7	-
j) Communication of change schedule to relevant entities	I, A	a, p	-	II.C8	-
k) Change migration to production system performed by designated personnel (distinct from development)	C, I, A	t, d, a	I.C7	-	-
l) Ex-post change verification	C,I	a, d	I.C8	II.C10	III.C6
m) Defined Recovery Procedures for unsuccessful changes	I, A	d	-	-	III.C7
n) Validation of documentation completeness	I, A	d	I.C8	II.C5	III.C6

Table 1: Overview of control elements

[1)] short text description of the control; [2)] overall Information Security goals supported by the control, values (C)onfidentiality, (I)ntegrity, (A)vailability; [3)] supported aspects of Software Change Management control objective, changes shall be (a)pproved, (p)rioritized, (t)ested and (d)ocumented; 4),5),6) reference to the matching control in each sample process if existent, e.g. I.C1, III.C6

5.2 Control Patterns – Generalization

As already stated, it is the intention of this work to leverage design patterns – in sense of "formalized best practices" (Winter, 2009) for given problems – to better integrate BPM and compliance requirements. Following this, a Control Pattern is an abstract process building block introducing an "internal control system"-perspective into process modelling. CPs are supposed to be used as a partial template at the process design stage or as a guideline during process review and improvement exercises. A pattern may contain various process elements as defined in the used modelling language, e.g. functions, events, systems, organizational units and flow control elements. Beyond this, it is always extended with information relevant from an ICS perspective. This includes the supported overall domain goals (here the Information Security "C-I-A" triad) as well as the support aspects for the concrete control objective (here the CO Software Change Management with its "approved, prioritized, tested and documented" aspects). This makes it possible to create reference catalogues of such control patterns structured by domain, control objectives and support aspects. Based on given compliance requirements, appropriate patterns can be identified and thereupon be employed for process design and improvement. A CP is designed to be reusable and thus remains abstract to a certain degree. This shall be illustrated with an example CP "Production Deployment", which is derived according to step 6 of the research method (section 3): From the consolidated list of control elements (Table 1) those elements are considered for CP generalization, which occur in at least two of three sample processes (threshold t=2). When locating those "relevant" control elements in the sample processes, a grouping can be identified towards the end of the process models representing control elements i), l) and n) – while j), k) and m) are not considered due to threshold (see Table 1). As described by the method, a generalized process part is derived from the given samples, which still reflects the respective group of control elements. The resulting CP is shown in Figure 3.

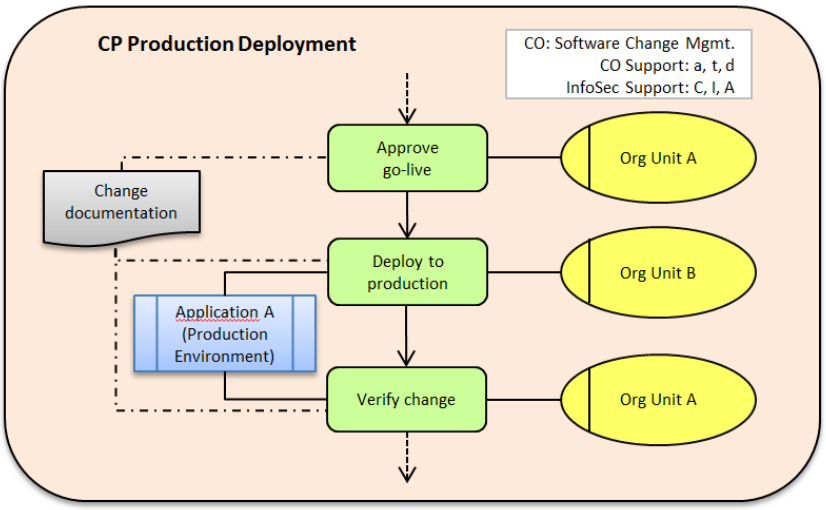

Figure 3: Control Pattern "Production Deployment"

The CP expresses "distilled" requirements i), l) and n), which shall be fulfilled in this context:

- before a change is moved to production, the go-live has to be approved to avoid conflicts
- structured case documentation is required for all steps in the pattern, e.g. the approval should be given based on a sound change documentation
- an entity independent of the change implementer should verify ex post, that the change has been deployed correctly in the production system as defined in the change documentation

The visualization of internal control requirements as a process building block makes it easier to understand the requirements and facilitates consideration of control requirements during process design. Depending on an organizations individual need, various CPs might be chosen from available reference catalogues and combined as required. As the patterns serve as generic templates, they may be adapted according to individual demand. In case of significant changes to a pattern, a reflection would be advised on whether the pattern still fulfils its designated control objective as expected. Conceptually, CPs offer high flexibility concerning the abstraction level. It may vary depending on the intended purpose, i.e. be (information security) domain specific as in the example above or more general like the following one: A generic Control Pattern "Testing" for example could be defined in a way that it could be used in control objectives for software development, hardware change management, project management, product design and so on. An even more abstract CP could define a pattern like "Authorization for subsequent process step" based on completeness and correctness of input information and the appropriate role for authorization. More general patterns require higher expertise when they are integrated into a process. In return they allow more flexibility regarding application and can be transferred to new domains or control objectives, where specific patterns may not be available.

6 Conclusion and Outlook

The given paper proposes an approach to extract/generalize internal controls based on real-life process specifications, make them explicit and harness the results in the shape of reusable patterns for process improvement. It is shown, how the idea of "design patterns" can be transferred to the domain of BPC with Compliance Patterns. A method for pattern creation is developed and applied in a case proof of concept. Though the conducted case study extracted a broad set of control elements from the sample processes, which could be used for generalization, it showed at the same time, that from a controls perspective all three real-world processes had deficiencies and were lacking some controls modelled in the other cases. This makes clear, that concepts to consider control aspects during process design offer

potential for process improvement. Explicit modelling of control elements in process representations can help to support transparency between business processes and compliance requirements.

Research in this area is still evolving. BPC offers well-grounded concepts with the formalization of compliance rules and linking these to processes. However, the formalization of requirements as formal rules involves a significant initial evaluation and modelling effort combined with on-going maintenance. In addition, it relies on intensive cooperation of organizational units with special skill sets. Thus, many companies are reluctant to invest into such an integrated approach and continue to manage business processes and their internal control system separately from one another.

CPs may contribute to mend this issue by taking real-world control elements and making them reusable as structures defined with well-proven BPM modelling techniques. As a result, the usage of CPs facilitates the design of compliance-aware processes. As for all pattern approaches, CPs are not finished designs, which can be implemented 1:1 in processes. They are to be considered blue-prints for how to solve a certain problem, i.e. support a given control objective. This allows for a high degree of freedom concerning their implementation. CPs may be used one at a time for a "soft", less intrusive step by step improvement of existing processes or in combination at the design stage for new processes. Reuse of CPs helps to avoid common control design mistakes, due to CPs being "formalized best practices", derived from proven real-world processes. They provide a common language for parties involved with transfer of control requirements to operational business processes. However, CPs are to be distinguished from prevalent best practice process templates as they are e.g. provided by ITIL. Instead of only giving hints "how" a certain task should be performed, CPs are always closely linked to control objectives and thus offer reasoning "why" a certain control element is established. Building on this, they may significantly increase efficiency of audits, because by providing an explicit control perspective on processes, auditors may be able to understand these processes faster and thus may easier assess audit relevant aspects.

The given paper serves as proof of concept for the deduction of CPs from real processes. Current limitations include the extent of the case study, which is linked to availability and quality of suitable sample processes, as well as dependency on the expertise of the process reviewers for steps like the identification of control elements and generalization. Additional research will be required regarding the formalization and application of CPs. Among other things, this includes the visualization and maintenance of a (customized) CP, once it has been integrated in an organizations process, considering the aim of making control elements explicit for audits. Furthermore it will be necessary to extend the available set of CPs beyond the presented examples before a real benefit e.g. for process design can be expected. It is self-evident, that (as for all pattern-based approaches) the added value of the concept increases with the number of supported domains, control objectives and patterns. Therefore, if the current work and feedback from the research community indicates further potential, it is planned to set up an open web platform, structured by adequate characteristics (e.g. by business domains and common ICS control objectives), where through collaborative process review and modelling efforts a library of reusable Control Patterns will be created, thus supporting enhanced compliance in business processes.

References

Alexander, C., Ishikawa, S. and Silverstein, M. (1978). A Pattern Language: Towns, Buildings, Construction. Oxford University Press, New York

Caldwell, F. (2012). Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms [Online]. Gartner Inc. Available: http://www.gartner.com/id=2186915 [Accessed 28/03/2013].

Chesani, F., Mello, P., Montali, M., and Riguzzi, F. (2008). Checking Compliance of Execution Traces to Business Rules. *In:* BPM Workshops 2008 (Ardagna, D., Mecella, M. and Yang, J., eds.), 134-145. Springer, Berlin.

Coso (1992). COSO Framework [Online]. Committee of Sponsoring Organizations of the Treadway Commission. Available: http://www.coso.org [Accessed 28/03/2013].

El Kharbili, M., Medeiros, A., Stein, S. and van der Aalst, W. M. P. (2008). Business Process Compliance Checking: Current State and Future Challenges. *In: MobIS* (Loos, P., Nüttgens, M., Turowski, K. & Werth, D. (eds.). GI, Saarbrücken.

Elgammal, A., Turetken, O., van den Heuvel, W.-J. and Papazoglou, M. (2011). On the Formal Specification of Regulatory Compliance: A Comparative Analysis. *In:* Service-Oriented Computing (Maximilien, E., Rossi, G. eds.). Springer, Berlin.

Maggi, F., Westergaard, M. and van der Aalst, W. M. P. (2011). Monitoring Business Constraints with Linear Temporal Logic: An Approach Based on Colored Automata. Springer, Berlin.

Gamma, E., Helm, R., Johnson, R. and Vlissides, J. (1995). Design Patterns. Elements of reusable object-oriented software. Addison-Wesley Longman, Amsterdam.

Governatori, G., Hoffmann, J., Sadiq, S. and Weber, I. (2008). Detecting Regulatory Compliance for Business Process Models through Semantic Annotations. *In:* BPM Workshops 2008 (Ardagna, D., Mecella, M. and Yang, J. eds.), 5-17, Springer, Berlin.

Houy, C., Fettke, P. & Loos, P. (2010). Empirical research in business process management – analysis of an emerging field of research. BPM Journal. Emerald Group Publishing Ltd., Bingley.

ISACA (1993). Control Objectives for Information and Related Technology [Online]. ISACA. Available: http://www.isaca.org/COBIT/Pages/default.aspx [Accessed 28/03/2013].

ISO (2005). ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements [Online]. International Standards Organization. Available: http://www.iso.org/iso/catalogue_detail?csnumber=42103 [Accessed 28/03/2013].

Lu, R., Sadiq, S. and Governatori, G. (2008). Measurement of Compliance Distance in Business Processes. Information Systems Management, 25**,** 344-355.

Muehlen, M. z., Indulska, M.and Kamp, G. (2007). Business Process and Business Rule Modeling Languages for Compliance Management: A Representational Analysis. *In:* ER Tutorials, Posters, Panels and Industrial Contributions 2007 (Grundy, J. C., Hartmann, S., Laender, A. H. F., Maciaszek, L. A. and Roddick, J. F. eds.), 127-132, Australian Computer Society.

Namiri, K. and Stojanovic, N. (2007). Pattern-Based Design and Validation of Business Process Compliance. *In:* CoopIS, DOA, ODBASE, GADA, and IS 2007 (Meersman, R. and Tari, Z. eds.), 59-76, Springer, Berlin.

Pesic, M. and van der Aalst, W. M. P. (2007). DECLARE: Full Support for Loosely Structured Processes. IEEE Computer Society.

Sadiq, S. and Governatori, G. (2010). A Methodical Framework for Aligning Business Processes and Regulatory Compliance. *In:* Handbook of Business Process Management (Brocke, J. and Rosemann, M. eds.), Springer, Berlin.

Scheer, A.-W. and Brabänder, E. (2010). The Process of Business Process Management. *In:* Handbook on Business Process Management 2 - Strategic Alignment, Governance, People and Culture (Brocke, J. and Rosemann, M. eds.). Springer, Berlin.

Schumm, D., Turetken, O., Kokash, N., Elgammal, A., Leymann, F. and Heuvel, W.-J. v. d. (2010). Business Process Compliance through Reusable Units of Compliant Processes. ICWE'10, 10th international conference on current trends in web engineering. Springer, Vienna.

Schwartz, M. (2011). 2012 Security Spending To Hold Strong [Online]. Information Week USA. Available: http://www.informationweek.com/news/security/management/231903274. [Accessed 28/03/2013]

Solomon, M. and Chapple, M. (2004). Information Security Illuminated, Jones and Bartlett, Burlington.

van der Aalst, W. M. P. (2013). Business Process Management: A Comprehensive Survey. ISRN Software Engineering 2013**,** 37.

van der Aalst, W. M. P., ter Hofstede, A. H. M., Kiepuszewski, B. and Barros, A. P. (2003). Workflow Patterns. Distributed and Parallel Databases, 14**,** 5-51.

Winter, R., Fettke, P., Loos, P., Junginger, S., Moser, C., Keller, W., Matthes, F. and Ernst, A. (2009). Patterns in Business and Information Systems Engineering. Business & Information Systems Engineering, 06/2009**,** 468-474.