Achieving Flexible and Compliant Processes in Disaster Management

Kai Kittel  Stefan Sackmann  Hans Betke  Marlen Hofmann
Martin-Luther-University Halle-Wittenberg
Faculty of Law and Economics
Chair of Information Management
kai.kittel@wiwi.uni-halle.de  stefan.sackmann@wiwi.uni-halle.de  hans.betke@wiwi.uni-halle.de  marlen.hofmann@wiwi.uni-halle.de

Abstract

Workflow management systems are becoming increasingly flexible and thus open up new areas of application, such as the coordination of activities in disaster response management. However, for managing disaster events effectively, flexibility is seen as a necessary but not sufficient condition. Moreover, effective disaster management processes require comprehensive access to and the processing of public as well as private information. Since extensive data usage without adequate controls will not be accepted in any open and free society, validating compliance for flexible disaster management processes is becoming crucial for realizing the enormous options of new information and communication technologies.

In this contribution, we present a novel approach for realizing adaptive controls in flexible disaster management processes.

1. Flexibility and Compliance for Effective Disaster Management Processes

Flexibility is an obvious topic in managing disaster events where many unforeseeable situations can arise [1]. Flexible adaptation of ongoing disaster management processes (DMP) to new situations and demands, such as maintaining basic services or organizing rescue missions, is necessary and challenging [2, 3]. For supporting similar DMP and processing associated data, e.g. when coordinating drug allocation in the event of an international epidemic, adaptive Workflow Management Systems (WFMS) provide a promising technical basis [4, 5].

Apart from flexibility, validation of compliance is a second important characteristic of any DMP [6]: At first glance, compliance might not be recognized as a necessary precondition for effective DMP, since staying compliant with given rules and laws becomes less relevant when lives are at stake. However, institutions for disaster management provided with comprehensive access to (sensitive) public and private data as well as services and infrastructures might be a threat to security and privacy in non-disaster situations: the power given for managing disaster situations effectively opens up enormous opportunities for misuse, e.g., surveillance, espionage, or intrusion into privacy. Such a potential of misuse could be expected to trigger a lot of social resistance as happened with current approaches in automating data collection, integration, and analysis (e.g., SWIFT, e-Identity, RFID, or Google Street View [7-9]). Thus, as long as threats might outweigh social benefits, powerful institutions for disaster management will not gain acceptance in any open and free society without effective controls. Furthermore, companies or private persons will only cooperate on a voluntary basis and provide access to their data with adequate “guarantees” and effective controls for compliance. This leads to an apparent trade-off, since restrictive and comprehensive controls confine the required flexibility of DMP.

To solve this trade-off between flexibility and compliance, we propose a novel approach for flexible integration of controls into workflows during process execution. With respect to modeling IS for disaster management, the conceptual separation of controls and processes is discussed as a precondition. Subsequently, a novel model-based method for integrating controls flexibly and instance-specific into DMP is presented. The contribution is completed by a short conclusion and an outline of a future research agenda.
2. Varieties of Workflow Flexibility

Research results show that process flexibility has to be tackled at least on two levels [10, 11]: firstly, on the conceptual level of the process and, secondly, on the operational level performing activities.

Flexibility on the conceptual level mainly addresses the capability to alter or extend the sequence of activities as well as the allocation of resources according to changed terms and conditions [12]. Managing DMP requires the integration of (real-time) information (e.g., about an increasing number of infections in the case of an international epidemic) and of additional activities into instances of processes already started (e.g., new drug information and therefore new immunization activities) [13]. Innovative methods and tools for providing such flexibility at this conceptual level have already been developed and tested, e.g., by [4, 14].

On the operational level, flexibility mainly addresses the execution and support of activities with required and available IT infrastructure, e.g., the coordination and execution of IT services. To do so, the connection to different available databases should be easily changeable or the interface for information input should be adaptable to other services or data sources.

One of the most promising approaches to gain flexibility on both levels is that of service-oriented architectures (SOA). SOA provide a dynamic coupling of process activities with their underlying IT services (e.g., [15]) and thus allow (business) processes to be decoupled from their actual execution (e.g., [16]). The standardization of web service interfaces (e.g., [17]) allows IT services to be quickly changed on the technical level as well as web services provided by third parties or the organization itself to be integrated [18]. Thus, every instance of a workflow can be executed by different web services according to the actual execution environment without any changes on the conceptual level (e.g., [19]).

Transferring the principles, methods and tools of business process management (BPM) and SOA with their increasing support of data and flexibility to DMP is very promising (e.g., [6, 20]): firstly, web services mean a sound technical basis for integrating any kind of information and service into DMP without rolling out a new infrastructure. Secondly, further diffusion of web services can be expected, since many companies follow extensive integration strategies, e.g., IBM with its vision of a “smart planet” [21]. By advancing representation of real objects (with their characteristics and status) as services, they could be flexibly integrated into DMP even “on the fly” [22]. For instance, if water supply via a communal pipeline network is contaminated through bacteria, it can be sustained, e.g., with tank trucks or by distributing bottled water. To integrate such alternative actions into an ongoing DMP effectively, additional real-time information about current storage capacities or transportation facilities would be required, e.g., from (stand by) services of companies that run tank trucks or beverage manufacturers. Relying on such interlinked and distributed data sources can undoubtedly improve DMP.

3. Compliance for Disaster Management through Flexible Controls

Flexible adaptation of DMP is not a sufficient condition for realizing effective management of disaster events. A further crucial, but usually neglected aspect is the ability to check and validate compliance of DMP. At first glance, any disaster event where human lives are in danger seems to excuse non-fulfillment of compliance requirements. However, any free and open society will only provide private or company data on a voluntary basis if the institutions for disaster management can also show their compliance to rules and regulations in non-disaster situations (see discussion in [6]).

Achieving transparency and validating compliance is a current, well-known challenge for many companies and their IT governance (e.g., [23, 24]). In BPM validating the adherence to and the fulfillment of various regulations (e.g., Sarbanes Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), or German Freedom of Information Act) when executing business processes has been an issue for several years (e.g., [25, 26]). Disaster management could benefit from this discussion and further progress of methods and tools in the business domain.

From the view of compliance the situation of disaster management institutions in non-disaster situations is more or less equal to the one of companies, so in principle, the same approaches and mechanisms for compliance achievement can be used. However, the situation differs drastically in the case of a disaster event: rigid control mechanisms result in lacking flexibility, which is a significant disadvantage for disaster management [27] as well as for flexible business processes. Since the conflict between compliance and “ad hoc” flexibility is not yet solved in current BPM approaches, possible
contributions of both a classical IT security view and a BPM view are discussed in short.

An important foundation for validating compliant use of data and services is provided by “classical” IT security mechanisms. Following an IT security approach for internet-based IT infrastructures means the adherence to protection goals (e.g., [28, 29]) that can result from laws, contracts, service usage conditions, etc. Available security mechanisms usually assume that a (data) object has to be protected from unauthorized access. Furthermore, providing compliance requires usage control complementing the conditions for data access with so-called obligations [30]. For expressing compliance conditions and obligations in a formal manner, policy languages (e.g., [31, 32]) can also be used in the context of BPM (e.g., [33]). However, many obligations cannot be enforced by IT security mechanisms [30]: while compliance to formal specified access rules can be enforced by security monitors during runtime (e.g., [34]), compliance to formal specified usage rules (obligations) can only be observed [35]. At least the following compliance issues still remain unsolved:

Firstly, for controlling obligations no mechanisms capable of preventing any misuse exist. Current mechanisms (e.g., secure logging [36] or forensics [37]) merely allow non-compliance with policy rules to be subsequently detected. In the event of detected misuse, WFMS can, at best, start additional processes for palliating or trigger non-technical sanctions [38].

Secondly, enforcement or negotiation of different compliance/policy specifications provided by various services cannot be realized yet. Although, advanced policy languages allow the comparison of different rules and the detection of contradictions [39], a practical implementation of such policy approaches still lacks standardization. Furthermore, protocols for finding and communicating relevant policies are in an early stage [40, 41].

Since compliance and especially usage control cannot be enforced by technical solutions, institutions for DMP and their use of data/services are not yet controllable to an adequate level. To address this gap, non-technical so-called risk aware business processes were developed, e.g., [42, 43]. The proposed annotation of risks in process models on a conceptual level can give at least indications of possible misuse scenarios. While this might work for well-defined and company-intern business processes, it is not sufficient for controlling cross-institutional DMP or for preventing any misuse. Although the usage of external data is necessary in DMP, addressing risk in an external domain is not achievable by annotation approaches.

More promising is the integration of control activities into workflows [29]. Controls for business process compliance can be summarized and clustered into two categories differing in their restrictiveness and probability (and risk) of non-compliance (e.g., [29, 44, 45]): Compliance can be achieved “by design”, for example by redesigning a business process itself according to the laws. Alternatively, the originally intended business process can be extended with additional control activities preventing (or reducing the probability of) non-compliant execution. Then, an enforcement of compliance can be achieved by automated WFMS guaranteeing the execution of a process instance as intended.

A second category of controls follows a “by detection” approach. In this case compliance of processes is supported through analysis of process execution according to its coherence with policy or business rules (e.g., [46]). Then, secure monitors can be used for validating the actual data usage with formal specified usage rules.

In summary, companies are forced to transparency and to validate compliance with regulations, therefore changing their processes (by design), or at least protocling whether breaches of regulations have happened (by detection) is necessary [47, 48]. While this might work well for business processes the situation in DMP differs and has the following problems:

Firstly, an unexpected and unintended halt of any DMP due to a control activity might interfere or disturb the originally intended DMP. This means, at best, only a conflict with the aims of effectiveness; at worst, it could directly or indirectly endanger human lives.

Secondly, since DMP are usually difficult to plan and to predict, approaches preventing misuse “by design” are very limited in their applicability to DMP. On the other hand, control approaches that are capable of subsequently detecting misuse “by detection” keep DMP very flexible. However, their capability to prevent non-compliance and to reduce the risk of misuse is very limited.

The conflict between enforcing compliant execution of DMP and the flexible adaptation to new and unforeseeable situations is obvious: while a rigid compliance enforcement provided “by design” is wanted and helpful from the policy side, it is not applicable in the management of disaster events. Solving this dilemma on a general level seems impossible and requires a more detailed analysis. Therefore, our approach aims at a methodical separation of control and process models on different levels and a model-based adaptation of control
activities in workflows supporting both flexibility and compliance.

4. A Model-based Approach Supporting Flexibility and Compliance

To achieve both flexibility of DMP and compliance to policy rules, we aspire to an automated integration of control activities into disaster management processes “on the fly”. The presented approach is model-based, relies on the conceptual level, and works with the flexibility of SOA on the technical level.

The approach aims at shortening the gap between design and execution level and is based on an integration of controls into workflow instance rather than into the general workflow schema as usually done in BPM (see figure 1).

To realize an automated integration of controls into workflows “on the fly”, three main research areas have been identified [6, 49]: Firstly, a method for modeling and identifying suitable controls that fulfill the compliance requirements. Secondly, provision of a separated view on processes and controls. Thirdly, a method for integrating control activities “on the fly” into DMP on the level of single DMP instances. These three topics are discussed in the following in more detail.

4.1 Control Cascades – Flexible Selection of Controls for DMP Integration

Usually each compliance requirement can be addressed by different control activities at different points in time. For example, controlling the number of bacteria in drinking water can be controlled by the water supplier at different points of the supply process, e.g., by analyzing the water sources, the water depots, the hand-over to the consumer or by the consumer him/herself. Each of these controls can be of different types again (e.g. through an automatic water quality metering device or through a laboratory-confirmed test), differing in efficiency and cost involved. Furthermore, control activities can also be combined to increase effectiveness and to achieve a more satisfying control situation. Thus, a decision about which concrete control activities (and at which point of a process) shall actually be integrated requires a description of available alternatives. The control model proposed in this contribution is one of so-called control cascades.

The basic idea of control cascades is not to focus on one single control activity that could be integrated into a DMP, but also on (all) alternative control possibilities that support the achievement of one and the same compliance requirement. This means, in a first step, that different control possibilities (addressing a specific compliance requirement) are to be identified/defined. These control possibilities are modeled as so-called reference controls. In a second step, integration points within the underlying DMP have to be identified and modeled for each activity of a reference control. Identifying and describing alternative controls with their possible integration points in a formal way provides a systematic basis for the aim of flexible integration (e.g. earlier in the process) or for replacement (e.g. by an alternative reference control). Thus, control cascades build a model-based overview and selection of known and available controls that could be flexibly implemented and combined to achieve a compliance requirement (see figure 2).

(a) Intended DM process (with all possible controls)

(b) Instance of DM process – example with C1 executed

(c) Instance of DM process – example with C1 skipped and alternative C2 integrated

Figure 2. Example of Control Cascades

Thus, control cascades provide a methodical basis for flexibility: whenever a DMP is endangered by a control activity, it could be skipped by the process owner with the consequence that an alternative
control can be integrated automatically in the following process “on the fly” (see figure 2, example c).

If there is no such further control activity available then the resultant compliance breach could at least be logged and evaluated/sanctioned later on.

While the decision where to integrate control activities into a process has to be taken only once in the case of static processes, it becomes complex and challenging when the dynamic of the process increases. In DMP, process activities as well as the executing entities are usually subject to unforeseen changes requiring the adaptation of the ongoing workflow. Adapting a workflow over and over to new occurring situations, e.g. by skipping single (control) activities as well as by changing services and/or resources in use, can lead to (unintentional) ineffective controls and thus negatively affecting compliance achievements. For managing such dynamic adaptations systematically, control cascades serve for integrating/replacing necessary controls when changing the original process by (1) skipping activities or outsourcing a part of the process to external services, by (2) identifying controls that are no longer active, by (3) providing alternative controls and points for their integration into a changed process, and by (4) finding controls in a process which are still possible if an intended control activity is skipped. For realizing such a control cascade, however, the fundamental concept has to be substantiated with the help of so-called reference controls.

4.2 Modeling Reference Controls

For each compliance requirement at least one or a set of general reference controls (control patterns) has to be defined. Reference controls can be seen as a template where activities and involved objects as well as the general structure of the control are already designed. For instance, the “second set of eyes” principle (compliance requirement) can be performed in several ways: it can be realized as a sequential execution of control activities or with two control activities in parallel. Furthermore, it can be performed executing two control activities straight consecutively or with other business process activities in between. This template then has to be instantiated at the moment when the reference control is instantiated. Thus, reference controls are similar to the schema of a workflow which can produce several instances if executed [22].

Modeling of controls is not discussed exclusively in BPM literature and thus the identification and definition of reference controls is still an open research question. In principle, two types of control processes are known [50]. The first type of controls are so-called stand-alone controls that can be executed without any information of the underlying process. These controls can be executed like usual workflows and can thus be automated by WFMS like every other process. The second type of controls cannot be executed without integration into the underlying process. For an automated execution, both types of controls need to be formalized. The formal specification means a critical success factor for an automated compliance management: like a business process designer, a compliance officer has to consider cornerstones prior to his modeling when specifying controls. While in BPM a lot of solutions have been developed and discussed manifold [51, 52], solutions exclusively for compliance are missing. Therefore, for modeling reference controls, we discuss similarities of controls and processes in the following.

Known approaches with a more specialized focus on business process compliance provide several criteria for modeling controls: Goedertier and Vanthienen [53] mention control-flow (sequence and timing of activities), data (data validation and requirements) and resource perspectives (task allocation and data access rights). On the basis of a comprehensive compliance legislation review, the COMPAS project [54] identifies similar generic criteria for business process compliance, namely control flow concerns, information used and produced, locative concerns (where business process activities are carried out), resource used, and temporal concerns. Last but not least, Sadiq, et al. [29] identified flows, data, resources, and time in form of tags as relevant criteria for specifying controls. Summarizing the mentioned literature and extending the discussion of [55], we derive the following set of ten criteria for modeling reference controls:

- **Sequence of activities:** the first criterion is derived from the basic structure of controls. In their simplest form, they are an amount of activities to be executed in a designated order. Sequences of activities and sub-processes are well known in business processes as well and are a fundamental element of all business process models [56]. Therefore, this criterion can be addressed by usually all modeling languages for business processes.
- **Various organizational units and roles involved:** roles as well as organizational units are an important part of many compliance requirements and internal controls, e.g. addressing...
a separation of duty for protecting from fraud and errors. Representing organizational structures and associated roles are also known in many business processes, e.g., Architecture of Integrated Information Systems (ARIS) with its organizational view [57]. In principle, this criterion can also be fulfilled since the most well-known modeling languages have an organizational view.

- **Different views and abstraction levels:** different persons involved in a process do not always have the same interests in control details. While an employee managing the WFMS is interested in technical details, a purchasing agent is more interested in the functional aspects of compliance. Without an ability to generate different views and the possibility to create different abstraction levels, even simple processes can become very complex and “polluted” by controls [58]. In business process management, the problem of different interested parties is the same, e.g., the great complexity of a model for the whole company must be divided for different departments with their specific view [59]. Different views and abstraction levels are common concepts and part of nearly all modeling languages for business processes.

- **Temporal features and conditions:** Temporal features are important for functional controls. There are a lot of compliance requirements that rely on temporal conditions, e.g. wait activities, obligations, or processes have to be cancelled after a specified time of no (re)action. Modeling temporal conditions is also well known in modeling languages for business processes. However, there are differences in the concrete notation: while extended event-driven process chains (eEPC) have no dedicated elements for temporal conditions they are known and part of the business process modeling and notation (BPMN) [60].

- **Concurrency (parallel, sequential):** Concurrency is an important concept in realizing controls. Control patterns like the four-eye-principle can be realized by a parallel or a sequential process flow depending on whether, e.g., processing time, control effectiveness, or rescuer workload is to be taken into consideration. Effectiveness is an important aim in every business process therefore parallelization of activities is used to save time and costs and is also already well known in business processes [61] and can thus be expressed by nearly all modeling languages.

- **Message and data types:** Most of the controls refer to dedicated documents. For compliance requirements, a way to distinguish between different types of document, e.g. in what form (paper, electronic) it is actually mentioned, is very important. Processing business activities needs documents, too. Reading and generating documents is a core feature of all modeling languages and every workflow management system [22].

- **Information and data flow:** For satisfying some compliance requirements addressing the avoidance of mistakes and misuse of data, it is important to specify which document is used, on what channel it is posted and at what point of a process it is used. Logging information flow should be an integrated feature of every workflow management system, to do this safely is an aim of secure logging [36]. Thus, information and data flow is in principle, also known in business process management and the used modeling languages.

- **IT systems and interfaces:** For many compliance requirements, e.g. to avoid mistakes due to incorrect file formats or addressing security aspects, a more technical view on IT systems, applications and interfaces is necessary. Such a view is especially helpful in institutions for disaster management with a lot of departments executing their processes through different IT systems. The problem of the consideration of different IT systems and associated interfaces is not new to huge companies with several departments, suppliers and customers. For this reason business process modeling languages, e.g. eEPC, provide special modeling elements to take these requirements into account [62].

- **Formulation of control conditions:** Control conditions often refer to the states of objects of the process, e.g. when the number of bacteria exceeds 100,000, then a separate check has to be done. Such conditions are also well known in the business context, and the existing field of modeling and expressing business rules discusses this extensively [63].

- **Global conditions and exceptions:** Compliance requirements often have control conditions that can be triggered at different points in a process, e.g. the abortion of a fire rescue process after identifying an unknown hazardous material. Global conditions have even to be fulfilled in the business context, e.g., when a customer cancels an order. Although global exceptions are not part of all modeling languages for business processes.
(e.g., eEPC), the concept is not unknown. For example, the exception and event handler in business process execution language (BPEL) provide such a feature [64].

Comparing these ten criteria with the requirements known from business processes the similarity is obvious. Therefore, in principle, the same languages that are used for modeling business/disaster management processes can also be used for modeling reference controls.

4.3 Integrating Controls into DMP “on the fly”

The flexible integration of controls into DMP can be realized with a separated model of controls at the design-time, whereas an automated integration of DMP model and control model assures the flexibility. Therefore, an integration of reference controls in the form of concrete control activities into DMP at the moment of the instantiation or during execution has a significant advantage: there are more pieces of information available than at design time. For instance, in the already mentioned water supply scenario the number of people waiting for water or the road condition for truck delivery. Such information is extremely relevant for adapting instances of DMP and for integrating control activities corresponding to the actual environmental context.

Therefore, integration means adherence of control integration parameters from the DMP like inputs, outputs, or the timeframe defining the setting for the control activities to the reference controls. This information means pre- or post-condition for a control activity and thus defines integration points within the DMP where an integration of controls is possible. Following the control cascade approach, this information also defines which alternative controls are actually relevant for achieving compliance of the DMP addressed.

Since there might be many points for integration possible, a selection is inevitable. In the long run, domain-specific selection methods would be part of a research agenda; however, established and well-known methods from BPM could serve as promising starting point, e.g., path analytics calculating the so-called critical path [47]. Since time matters in DMP particularly, further methods, e.g., for cycle times, error ratios, or process costs could also be used in addition. By simulating the execution of the relevant process and by calculating different workflow scenarios, activity paths can be optimized and control activities can thus be transferred into uncritical areas [14].

For an automated integration of control activities by a WFMS, all relevant control integration parameters of a reference control have to be specified in a formal manner. The proposed separated definition of reference controls and DMP in combination with control cascades allows more than one set of control integration parameters to exist. Therefore, developing an algorithm which handles the integration of control activities into workflow instance will be a next promising step for automating compliance in DMP.

5. Conclusion and Open Research Issues

Disaster management processes (DMP) are mainly challenged by achieving both flexibility and compliance. This contribution focuses on achieving compliance in highly dynamic and flexible DMP that is neither taken into consideration adequately nor solved in current BPM approaches. The deployment of control cascades as methodical basis for modeling a control view, the definition of reference controls and their transformation into control activities, and the integration of control activities into DMP “on the fly” are presented as a novel approach. Bringing these three concepts together provides a methodical basis for reacting flexibly in disaster event situations, e.g., by skipping control activities, without losing control over achieving compliance requirements: a possible loss of control is counterbalanced by automatically searching and integrating alternative control activities into the DMP.

However, the approach is not providing “pure” technical or provable correct solutions for achieving compliance in the sense of classical IT security. In fact, it is focusing at a reduction of the probability of misuse and, thus, providing a way for managing the risks involved with the potentials for misuse. Reducing the required trust in disaster management institutions with a comprehensive and powerful access to data, processes, and services in the case of a disaster event might provide a new basis for a social discussion on realizing the potential of IT in disaster management.

There is no doubt that several hurdles need to be overcome before disaster management institutions can realize all options of modern IT. As part of a future research agenda for solving the apparent trade-off between achieving flexibility in process execution and compliance, the following topics are seen as crucial:
• searching for modeling languages which support control and process modeling on all abstraction levels and with different modeling teams,
• developing domain-specific methods for control selection,
• detecting available services in an automatic manner in order to execute a DMP through those services and within those infrastructures that are still available in the event of a disaster,
• standardization of policy transmission to specify and protocol the finding and communication of relevant policies.

Following the design-science paradigm [65], a first prototype integrated into the flexible BPM-software Aristaflow [66] is already in development, laying the necessary foundation for future research and sketching a promising outline not only for improving disaster management but also for companies. Integrating controls “on the fly” is also a promising way to automate compliance in the business context.

6. References


