



A comprehensive framework for the application of process mining in risk management and compliance checking

Filip Caron, Jan Vanthienen and Bart Baesens

DEPARTMENT OF DECISION SCIENCES AND INFORMATION MANAGEMENT (KBI)

A Comprehensive Framework for the Application of Process Mining in Risk Management and Compliance Checking

Filip Caron^{a,*}, Jan Vanthienen^a, Bart Baesens^{a,b,c}

^a*Department of Decision Sciences and Information Management, KU Leuven, Naamsestraat 69, B-3000 Leuven, Belgium*

^b*Vlerick Leuven Gent Management School, Vlamingenstraat 38, B-3000 Leuven, Belgium*

^c*School of Management, University of Southampton, Highfield Southampton, SO17 1BJ, United Kingdom*

Abstract

As process-aware information systems are becoming omnipresent in contemporary organizations, the requirements for risk management and compliance checking have evolved and demand a more process-centered approach. The business events recorded by these information systems are systematically and securely logged, which results in a wide variety of opportunities to evaluate dynamic or multi-state process properties. Process mining research has proposed a spectrum of techniques for analyzing the functional, control-flow, organizational and data perspective of the business processes.

The framework presented in this paper structures the relationship between the process mining techniques, the organization's stakeholders with a control function and their activities. Focus will be placed on proposing a process-oriented approach that enables a timely analysis of large amount of event data and provides a high process deviation detection effectiveness. Additionally, in this contribution we analyze the optimal settings for the process mining techniques and provide suggestions for further adapting the techniques to the specific needs of risk management and compliance checking. The applicability of the framework is tested and evaluated.

Keywords: Process Mining, Process-Aware Information Systems, Risk Management, Auditing, Compliance Checking

1. Introduction

The value creation abilities of an organization are increasingly determined by the flexibility of their information systems [89] and business processes [57]. This flexibility represents the organization's ability to timely adapt its operations in order to accommodate crucial changes in its operating environment and thereby safeguarding its economic performance [90]. Information systems research, as a consequence, has focused on improving the flexibility of process-aware information systems that support and manage the

*Corresponding author, Telephone: +32 16 32 65 58, Fax: +32 16 32 66 24

Email addresses: `filip.caron@kuleuven.be` (Filip Caron), `jan.vanthienen@kuleuven.be` (Jan Vanthienen), `bart.baesens@kuleuven.be` (Bart Baesens)

business operations [103]. While improving the flexibility of process-aware information systems helps in maintaining a fit with the organization’s environment [10], it may also pose significant risks that could have an enormous impact on achieving the corporate objectives [87].

Process-aware information systems typically record detailed and structured information on the business events in a process instance’s audit-trail [113]. These business events represent relevant occurrences that happen at a certain point in time for a specific process instance, e.g. the completion of an activity. Event information, such as the timestamp, the process instance identifier, the activity identifier and the originator, is systematically and securely stored in the event log [110]. Consequently, the resulting event logs conceal an untapped reservoir of knowledge about the business operations. Process mining refers to the set of techniques that analyzes these event logs to acquire insights into the real business processes [115].

This contribution aims at proposing a process mining applicability framework for shareholders with a control function. Throughout the paper a basic insurance claim handling process will be used as an example of a process configuration in an information system. The basic process model can be found in figure 1.

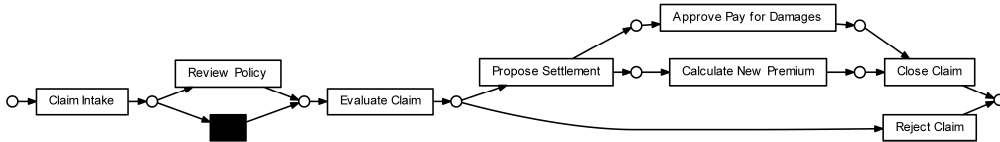


Figure 1: Basic insurance claim handling process model

The outline of the paper is as follows: section 2 provides an overview of the related research, while section 3 provides the problem statement, the research objectives and the research design. Section 4 introduces the process mining applicability framework for a risk management and compliance checking environment. In the body of the paper we discuss the different dimensions of this applicability framework in detail. Section 9 and 10 respectively provide an example and a comprehensive evaluation of process mining support in this setting. The final section concludes the paper.

2. Related Literature

The business process risk management and compliance analysis research developed and presented in this paper, is related to the information systems’ governance, risk and compliance research (GRC). In particular, the research focuses on the intersection between process mining and compliance analysis in process-aware information systems. Note that compliance checking can be a strong risk identification and assessment tool.

Process mining research, also known as workflow mining, aims at inferring process and business knowledge from event logs, as well as providing process diagnosis tools [107]. While process mining research has been around for more than a decade (e.g. [1, 18]), the field has recently seen a substantial increase in research output. As a result a plethora of process mining techniques has been presented. Contributions focusing on the *analysis of activity sequences* in the event log with process discovery as the most important sub-domain [99], represent the lion’s share of the contributions. Process discovery techniques

aim at reconstructing business process models from event logs. Heuristic process discovery techniques use a three step algorithm: the construction of an activity dependency graph, the mining of splits/joins and the mining of long-distance dependencies [122, 120]. The evolutionary approaches use adaptive search algorithms to generate successive process patterns that are evaluated through specific fitness measures (i.e. measure for the ability to reproduce the behavior in an event log), e.g. the genetic miner [3]. Goedertier et al. describe how negative events can be used to represent business process discovery as a multi-relational classification problem [35] and inductive programming for workflow discovery [30]. Metrics for evaluating process mining based models have been developed, e.g. the performance event log replay-based conformance checking metrics presented in [84] or the process model similarity metrics of Dijkman et al. [29]. Finally, specific activity sequence statements can be tested against the event log [23, 105, 68].

In addition process mining research has focused on analyzing other aspects of business processes. The originator-by-task matrix [112] and the social network miner [108] provide respectively an overview of the task allocations and different types of collaboration between employees. The performance aspect and in particular bottleneck analysis are discussed in e.g. [85]. Process variant analysis based on specific case data has been performed in e.g. [107]. Finally, the process mining literature body covers multiple case studies, e.g. in the telecom industry [34], in the healthcare industry [14, 64] or in the banking industry [53] (internal fraud).

Whereas research towards **compliance in process-aware information systems** has embraced the use of business rules as the most suitable approach for modeling internal controls [86], there does not yet exist a consensus on the optimal approach nor on the ideal (formal) specification language [40]. A multitude of process model annotation approaches, both on process and on task level, has been presented. Ghose and Koliadis developed an approach for annotating the tasks in a business process modeling notation (BPMN) model with their effects and enable to propagate and cumulate the effects from a task to the successive task [32]. Sadiq et al. propose a business process annotation technique that visualizes internal controls on process models by means of different types of tags based on deontic logic [86]. Liu et al. propose a visual rule language for annotating business processes with general purpose compliance requirements [62]. In [60], Kuster et al. present a method for comparing object life-cycles that provide reference models for data artifacts. In [124], zur Muehlen and Rossman propose an extended event-drive process chains (EPC) notation in order to integrate risks in business processes. Goedertier and Vanthienen propose PENELOPE, a logical language that is used for verifying temporal constraints derived from internal and external directives.

Other approaches focus on run-time business process compliance. Mandatory constraints in declarative process models that can be directly mapped on imposed directives, can be used to ensure compliant process executions. With Declare [73] as the most notable declarative process enactment approach. Giblin et al. propose a set temporal rule patterns for event monitoring [33]. As flexibility has become an important issue, approaches for ensuring compliance during process adaption were presented. For example, AdeptFlex provides extensive support to prevent non-permissible structural changes [79], while the constraint specification framework enables the creation of a compliant on-the-fly composition in the underspecified process parts (i.e. the pockets of flexibility) [87]. Several comparable after-execution rule-based process analysis methods have been proposed, e.g. LTL-Checker [23] and SCIFF-Checker [68]. Process mining proposes

techniques that can be used for after-the-facts compliance evaluation in process-aware information systems.

3. Problem Statement, Research Contributions and Design

3.1. Problem Statement: Lack of Adequate Process-Oriented Audit-Trail Analysis

Recent studies have uncovered the high financial and legal risks of non-compliant behavior, e.g. [70, 45, 63]. Additionally, new regulations have raised a new set of compliance challenges for businesses information systems and processes [59]. For example, the Sarbanes-Oxley act and the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5 place an important responsibility for internal control assessment on respectively the management and the external auditors. In combination with the evolution towards process-aware information system we identified two significant problems for business process mining and analytics: the **absence of a process mining applicability framework** for risk management and compliance, and the **lack of adaption of existing techniques** to this setting.

Firstly, while most of the process mining research contributions vaguely refer to auditing as a potential application (e.g. [84, 107]), they do not tend to specify which *specific (auditing) activities* can be supported by process mining. Additionally, no distinction has been made between internal and external auditors. While we do agree that auditors of both types have a common core set of activities, their objectives and consequently the required activities and the used techniques can strongly differ [75]. Moreover, none of these contributions broadens the target audience beyond auditors. A much *broader set of stakeholders* commonly takes part in corporate governance, risk management and compliance checking activities [22]. These stakeholders (with a control function) could potentially benefit from process mining techniques as well.

Secondly, the existing process mining techniques are often not fully adapted to the *contemporary requirements* of risk management and compliance checking. Problems might arise from the selection of a log comparison base (including the process overspecification), from the tendency to generalize discovered models or from the interpretation of coarse metrics. Furthermore, the process mining researchers have primarily focused on improving techniques for control-flow and (to a lesser extent) for social/organizational analysis. Stakeholders with a control function, however, would benefit from the ability to perform controls on the additional data in the event logs (e.g. amounts) [61, 95].

3.2. Research Objectives and Contributions

In this paper we present a framework for risk management and compliance checking with process mining, which can be considered as a management information systems artifact. Management information systems artifacts can be defined as “innovations that define the ideas, practices, technical capabilities and products through which the analysis, design, implementation, and use of information systems can be effectively and efficiently accomplished” [47, 27, 98].

The process mining framework for risk management and compliance checking structures and models the relationship between the GRC stakeholders, the GRC activities and the process mining techniques. During the construction of the process mining framework we concentrate on:

- identifying and describing support options for *specific GRC activities*.
- *extending the scope* of the process mining applicability in the governance, risk and compliance checking setting
- an improved *efficiency and effectiveness* of process-oriented risk management and compliance checking. In the process-oriented risk management and compliance setting we define efficiency as the ability to provide a timely analysis of a large volume of process data (preferably the complete event log). Effectiveness can be defined as the ability to precisely detect all deviating process behavior.
- providing *insight on fundamental misfits*, proposing *optimal settings* and on suggesting *ideas for further adapting process mining techniques*.

In addition this paper will demonstrate the principle feasibility of our process mining framework and will provide an evaluation of process mining as a technique for risk management and compliance checking.

3.3. Design Science Research Process

The design science research paradigm has been used to conduct the research preceding the results presented in this paper. Hevner et al. describe design science in information systems as “a paradigm that seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts” [47]. We adhered to the design science research methodology presented in [71]. Figure 2 provides an overview of the design process and summarizes the highlights of each phase.

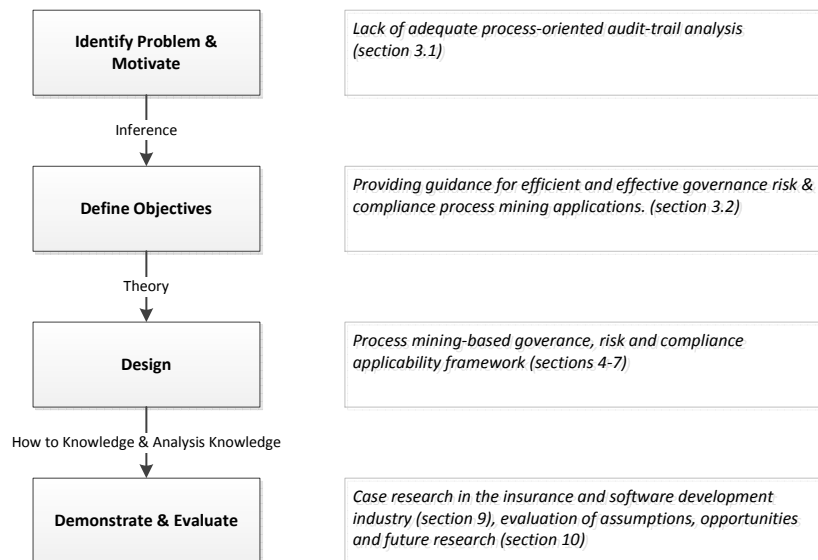


Figure 2: Overview of the applied design science research process applied in this paper

Firstly, the **problem** needs to be precisely *identified* and its *relevance* needs to be motivated motivated. Our previous research towards business process compliance elicited

the lack of adequate process-oriented audit-trail analysis for risk management and compliance checking [37, 38, 36]. While process-aware information systems are heavily adopted across industries and used to enforce certain types of internal controls [51], no formal framework has been presented to apply the theoretical process analysis techniques in this context. In section 3.1, we provided a full description of the problem (conform [81]) and motivated its relevance, which is in accordance with the problem relevance guideline in [47].

Secondly, the research **objectives** for the solution, i.e. the design artifact, need to be specified. In section 3.2, we presented the research objectives that were inferred from the problem statement. These objectives focus on the creation of an artifact that represents both a model and a method. According to [92] a model represents a real-world situation, in this case the solution space. Methods, on the other hand, provide guidance on how problems should be solved [47], in this contribution we focus on creating guidelines for process mining support.

Thirdly, the **design and development** stage deals with creating the innovative artifact itself. This stage has been twofold: the construction of the dimensions (i.e. GRC stakeholders, GRC activities and process mining techniques) and the identification of the specific applications at the intersections of these dimensions. The dimension construction sub-stage is mainly based on an extensive review of the different bodies of literature, which resulted in the different classifications for each dimension. These dimensions will be discussed in sections 4 - 7. In order to link the different dimensions (i.e. sub-stage 2) at the different category combinations, we first performed a requirements analysis (based on document analysis and a review of the domain knowledge) for each GRC activity. Afterwards, we matched the requirements of the different activities to the known strengths and weaknesses of each set of process mining techniques. The results are presented in section 8. As encouraged in [47], research rigor is in both sub-stages derived from an effective use of the exiting knowledge base. The references to these research contributions are included in the respective sections.

Finally, section 9 provides a **demonstration** to prove that the idea behind the artifact works, followed by an **evaluation** of the challenges and opportunities of process mining applications in the risk management and compliance checking context in section 10. The demonstration section provides the results of both a controlled experiment, based on an artificial insurance claim handling process, and an observational case study, based on a software development process.

4. Process Mining Applicability Framework

The literature review in section 2 indicated that there exists an abundance of process mining techniques, which results in a need for *clear guidance* on the process mining applicability in the governance, risk and compliance setting. In this section we introduce a comprehensive process mining applicability framework that will fill this need, see figure 3.

The applicability framework consists of **three interrelated dimensions**:

- ***Process Mining Techniques Dimension***: The first dimension encompasses the process mining techniques that are suitable for risk management and compliance checking: *Process Discovery & Visualization, Conformance Checking & Delta*

Analysis and Rule-Based Property Verification. In section 5 we discuss the different techniques, their abilities and their optimal settings. Furthermore, we propose a universally applicable rule-based approach.

- **Control Functions Dimension:** An organization may have different sets of governance, risk & compliance stakeholders that each perform a specific control function: the *Management*, the *Internal Auditor(s)*, the *External Auditor(s)* and the *Audit & Risk Committee*. The roles and responsibilities of each of these controller types are further elaborated in section 6.
- **Control Function Activities Dimension:** The third dimension groups the common activities for these control functions into three categories: *Risk Identification & Assessment*, *Control Activities* and *Generation & Communication of Information*. The different activities are described in section 7 and linked to the other dimensions in section 8.

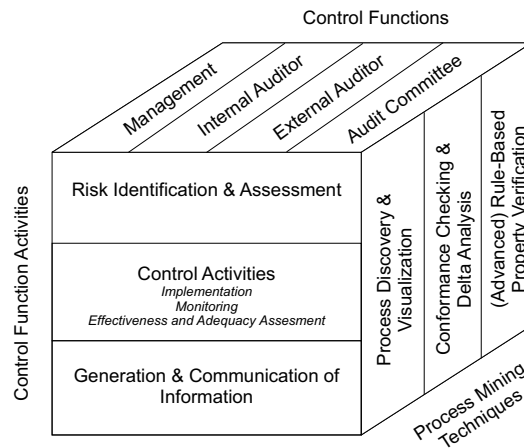


Figure 3: Process mining applicability framework for risk management and compliance checking

Two **important remarks** must be made about this application framework. Firstly, while the main dimensions of this applicability framework will remain fixed, the set of *elements for each dimensions may evolve* together with new research and other events. For example, new process mining techniques that create value for GRC-processes may become available. Secondly, inherent *limitations* exist as the framework partially relies on human judgement, e.g. in identifying exact risks or establishing the correct monitoring capabilities, and on process mining techniques, e.g. one can only analyze the events that are actually logged.

5. First Dimension: Process Mining Techniques

Recent research contributions in process mining have developed an extensive set of tools and techniques, e.g. [110, 108, 101, 18, 46, 123, 121, 35]. This section explores the

process mining techniques that could effectively support the organization’s controllers in their governance, risk & compliance activities. Additionally, we discuss their general applications, their points of interest and their optimal settings.

Figure 4 provides an overview of the process mining architecture. The actual business process will be directly influenced by the existing legislation, business policies and external directives, which pose restrictions on the process model designed by the business analysts. Afterwards, the process model is used to configure the process-aware information systems. At run-time detailed descriptions of the process support are recorded in the information systems’ event logs. Finally, these event logs can be analyzed with process mining techniques. The inputs of each type of process mining technique have been visualized as well.

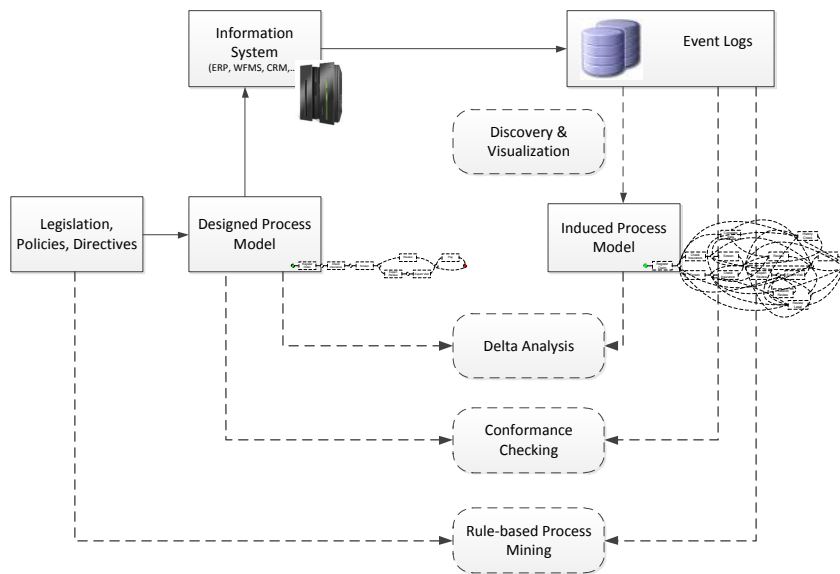


Figure 4: Process mining architecture

The process mining approaches can be roughly categorized into three classes:

- techniques for process discovery & visualization
- techniques for conformance checking & delta analysis
- techniques for rule-based property verification.

While the first two approaches promote the analysis of the process as a whole, the last one can be used to analyze specific process characteristics. All the individual techniques discussed in this section are implemented in the academic open-source tool for process mining, ProM [111, 112].

5.1. Process Discovery & Visualization

Business process models describe the process as it should be or as it is perceived by the business. In reality, however, it appears that the business processes executed in a

process-aware information system significantly deviate from their model, as people often create workarounds for special situations [102].

General technique applications of process discovery & visualization. The set of process discovery and visualization techniques enables the acquisition of a *full and precise insight in the real business process, summarized in one visual*. Therefore process visualization can be considered as the ideal technique for process exploration and thus a first step in a risk or compliance analysis [100]. In a risk management and compliance checking setting techniques such as the α [101], the $\alpha + +$ [25] and the heuristics miner [122] are suitable to *obtain a process model* from the event log of an information system.

Whereas process visualization traditionally focused on the overall control-flow, the *visualization of other business process aspects* can be of benefit for someone in a control function. The performance sequence diagram analysis plug-in [111], for example, allows for the inspection of rare control-flow patterns, which might suggest non-compliant behavior. Moreover, this tool enables you to focus on specific process related data in an event log. A third interesting additional aspect of a process is the set of employees involved. The originator-by-task matrix [112] gives an overview of the employees involved per activity, which can be used for analyzing specific authorizations or segregation of duties constraints. Additionally, the controller could use the social network miner/analyzer tool [108] to uncover possible collusion issues (based on both the handover and subcontracting metric). Finally, a broader resource-based bottleneck analysis can help uncover efficiency and effectiveness issues [85]. Process visualization as an auditing tool is advocated, for example, in [53, 100, 2].

Points of interest of and optimal setting for process discovery & visualization. Desirable characteristics for process discovery and visualization techniques in risk management and compliance checking tend to be atypical compared to other applications, unless the controller aims at understanding the general flow. As harmful process deviations tend to be rather exceptional, the discovery and visualization techniques are not required to be able to deal with noise. Controllers do not demand any abstracting from exceptional or infrequent behavior and might even *desire overfitting*. By focusing on precision and not taking into account the models general applicability, there will be no cover up of harmful process deviations that might lead to material weaknesses. Additionally, a very *strong event log completeness assumption* will be required: i.e. if one activity is directly succeeded by another activity in the induced process model, this sequence should occur at least once in the event log. This requires optimal configurations from the process discovery techniques, e.g. for the (flexible) heuristics miner [120] we prefer a low dependency threshold, a low positive observations threshold and a low relative to best threshold.

Contemporary organizations tend to require high levels of process flexibility in order to deal with the variations in interaction with clients, suppliers, etc. [106]. This rather dynamic and non-deterministic context affects the ability of conveniently organizing the models of a business process. Messy, spaghetti-like models are hard to understand and thereby limit the possibilities for an open-minded analysis and for an effective communication on the business operations. These findings on the process model understandability are related to the number of elements guideline (G1), the minimize the arcs guideline (G2) and the process decomposition guideline (G7) in [65].

The visualization challenge should be partially tackled by the introduction of a technique that combines the *effective filtering of infrequent patterns* combined with process visualization of the non-compliant executions. This filtering could be done with a rule-based process model (i.e. declarative model) or with a trace clustering technique (e.g. the technique presented in [52]). As a result we should be able to unlock the full potential of visualization techniques in the context of advanced (fraud) investigations and communication.

5.2. Conformance Checking & Delta Analysis

Conformance checking or delta analysis aims at detecting *inconsistencies between a prescriptive process model and its corresponding real-life process*. The difference between both lies in the comparison base for the real-life process, conformance checking uses the event log while delta analysis uses a derived process model [83, 84]. A multitude of business drivers, such as the need for unequivocal communication [21] or ISO9000 certification, have resulted in an omnipresence of prescriptive process models in contemporary organizations.

While the conformance checking in process mining is mostly based on the contribution of Rozinat [82], other fitness based techniques might be relevant for the controller (e.g. the comparison of digraphs [6] and the concept of process validation [19]). The latter has as main advantage its ability to differentiate the relative importance of specific types of events.

General technique applications of conformance checking & delta analysis. The execution paths specified in a process model contain multiple *implicit internal controls*, e.g. a segregation of duties internal control can be implemented by decomposing an activity in a sequence of activities with different authorizations. Quantifying the inconsistency with the prescriptive process model allows the controller to get a first impression of the overall risk involved in this specific process. In the governance, risk and compliance setting this quantification solely relies on the *recall or fitness* dimension, which describes the extent to which the behavior in the event log can be associated with valid execution paths in the prescriptive process model. Some conformance checking tools allow the controller to *locate the problematic areas*, e.g. the event log replay-based conformance checker [84] helps identifying the problematic areas based on missing tokens (corresponds to the execution of transition that was not enabled) or remaining tokens (corresponds to mandatory transitions that were not executed) in the petri-net [84]. Retrieving the specific problem instances will be less straightforward.

Points of interest of and optimal setting for conformance checking & delta analysis. The most important factor to consider when deploying conformance checking and delta analysis techniques for governance, risk and compliance purposes is the process model that will be used for log comparison. In addition to the interpretation of legislation, policies and directives there are a lot of possible distortions, which affect the business process model design and consequently the results of a compliance analysis. Generally, these distortions can be classified in three groups: interpretation & design distortions, implementation distortions and process execution & mining distortions. Figure 5 presents a detailed overview of the possible distortion sources.

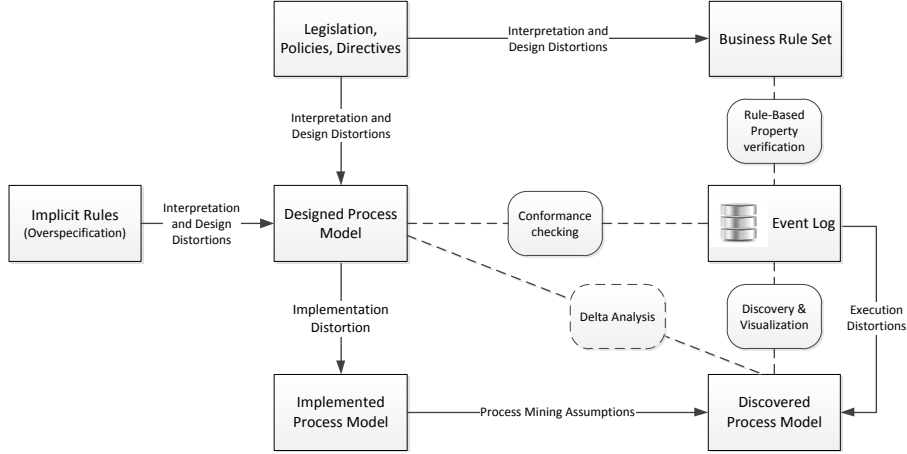


Figure 5: Basis for log comparison and sources of distortion

Firstly, both in designing an explicit business process model and in specifying a business rule set there can occur *interpretation & design distortions*. Legislation, policies and directives can remain vague and ambiguous [117], therefore assumptions are often made in the interpretation phase. During the actual design of the information systems, including business process modeling and business rule specification, the analysts are often confronted with expressibility limitations of the chosen design languages (e.g. the lack of support for interleaved parallel routing in BPMN [109]). Moreover, common procedural process modeling approaches require a full specification of all possible execution paths. Control-flow dependencies that are not dictated by internal or external directives may need to be modeled, i.e. implicit rules that result in an overspecification of the process model [74, 10]. Obtaining conformance with this possibly overly strict designed process model, can be adverse to the organization’s operations and business success.

The second set of possible sources of distortion focuses on the information systems *implementation* phase. Firstly, comparable to the design phase, technical analysts make assumptions on ambiguous specifications in design-time process models. Moreover, there may be a conceptual mismatch between the design-time process modeling language and the process execution language (e.g. business process execution language BPEL can only be used for a core set of BPMN constructs) and related expressibility restrictions [78]. Additional restrictions may stem from the limitations in construct support of the chosen business process enactment engine. Examples can be found in [109].

Thirdly, distortions may occur during the *actual process execution* and due to *process mining assumptions*. Case study research in process mining has indicated that the actual process can significantly deviate from the designed process, e.g. [107]. Consequently, event logs may only represent a distorted version of the designed process. Moreover, process discovery and visualization techniques tend to make important assumptions. For example a trade-off is made between specificity and generalization of the behavior [83], which may result in discarding ‘insignificant’ execution paths. Additionally, the completeness assumption, as specified in [104], for an event log can often be challenged.

Due to important distortions (such as interpretations, overspecification, etc.), differ-

ent approaches may result in different results. Figure 6 provides the different models for the evaluate claim subprocess. The following audit-trail: expert review \rightarrow legal consult \rightarrow formulate opinion \rightarrow increase provision, would be supported by the designed model but not by the implemented nor by the discovered process model. Moreover, audit-trails of process instances that do not conform with the process model, may fully comply with all relevant legislation, policies and regulation. For example, the subprocess in figure 6 is restricted by the following directives: ‘second review must be preceded by expert review’, ‘formulate opinion must be preceded by expert review’, ‘reduce provision must be preceded by formulate opinion’, ‘expert review must be followed by formulate opinion’ and ‘formulate opinion must be followed by reduce provision *or* by increase provision’. Increasing the provision right after the execution of an expert review and based on new precise information will not be allowed in any model.

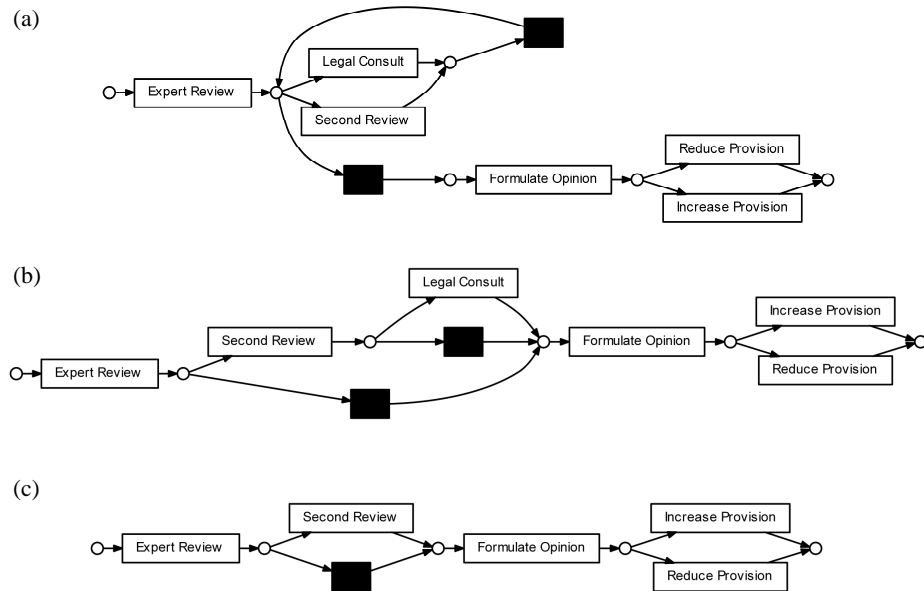


Figure 6: Differences in models at different phases (a) design-time model, (b) implemented model and (c) discovered model

Furthermore, the correctness of the designed process models can often be questioned. In addition to process overspecification, defining all possible execution paths to deal with natural variations in a business environment can be challenging [72]. Recent research contributions even indicated that at least 5.6% of the process models in a major enterprise risk management (ERP) package contain modeling errors [66]. Therefore an event log that is fully equivalent to the designed business process might not always be desirable from a business/operational viewpoint. Additionally, this full equivalence might not be required by regulations and business policies.

5.3. Rule-Based Property Verification

5.3.1. Description of Rule-Based Property Verification

Rule-based property verification techniques represent a process mining approach that can be used to assess and evaluate *specific process properties*, e.g. segregation of duties or activity ordering. This is in sharp contrast with the previous techniques that focus on the overall process model compliance.

A variety of rule-based property verification techniques has been proposed. The LTL-Checker provides sixty application-independent and configurable templates, based on linear temporal logic, that can be used to define the (un)desired process properties and provides the possibility to check them against the event log [23, 105]. The Semantic LTL-Checker extends the original LTL-Checker by adding the functionality that allows the user to provide concepts as input to the parameters of LTL formulae [24]. SCIFF Checker uses configurable CLIMB rule templates to verify process properties [68]. Rules specified in CLIMB strongly resemble the Event-Condition-Action rules, with the exception that they specify expectations about executions rather than actions that need to be performed [76]. The applicability of these sets of standard configurable pattern sets has been demonstrated in e.g. [53, 54, 116, 16].

General technique applications of rule-based property verification. In order to ensure compliance with the imposed legislation, directives and internal business policies, organizations implement a set of internal controls. These internal controls put restrictions on the set of possible process characteristics, e.g. authorization controls for certain tasks. Translating the internal controls to a set of business rules, where one internal control is mapped to one or more business rules, has been considered as rather straightforward [13]. Consequently, rule-based property verification techniques can be applied to evaluate whether the actual process executions do not possess undesired process characteristics. In conclusion, rule-based property verification techniques provide precise information on the process instances that do not comply with specific rules, and consequently specific internal controls and regulations.

Points of interest of and optimal setting for rule-based property verification.

While the interpretation and design distortions as discussed in the previous section and in figure 5 remain, these techniques are inherently robust against process flexibility and noise. Moreover, they do not consider any implicit rules introduced by process over-specification nor do they have to deal with the issue of generalization. Hence they have a wide-spread applicability in the governance, risk and compliance setting. These techniques are however limited by their expressibility, e.g. the standard configurable patterns in the LTL-checker lack extensive support for taking into account specific case data.

5.3.2. Proposals for an Advanced Rule-Based Process Analysis Approach

Business rule research has mostly focused on improving the business rule specification languages in terms of expressibility [44, 42], comprehensibility [119, 15] and formalisms [39, 105]. This has resulted in business rule classifications that focus on specific technical aspects (e.g. possible ways to react to an event [80]) or on a partial view (e.g. data-oriented business rules [44]). Rule-based risk management and compliance checking applications require adequate support for translating regulations, directives and other elements of the business environment in to business rules. The adequacy of the approach is mainly determined by the expressiveness, the ability to produce understandable specifications and the absence of ambiguity.

Figure 7 presents a proposal for an advanced rule-based process analysis approach. In order to analyze and ensure compliance with the legislation, business policies and other directives an internal control system is put in place. The set of internal controls that are implemented in support of a specific piece of regulation is mapped on a set of formal and structured rule-based controls, which results in a non-ambiguous specification. The controller can make use of an comprehensive set of rule patterns (expressibility), with rules specified in plain English (understandability). The structured rules can be tested against the enriched process data, i.e. the event log data that was enriched with information residing in other external data sources such as human resource management systems or customer relationship management systems.

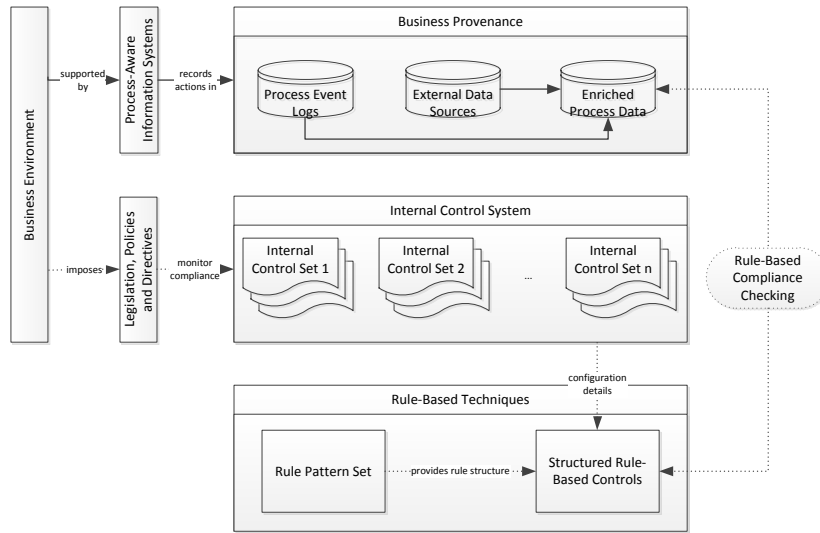


Figure 7: Advanced rule-based compliance checking architecture

In [12] we presented a two dimensional business rule classification structure covering the most common business rule types, and templates, that can be used to implement internal controls with process mining. The classification structure is based on two dimensions: the process mining perspective and the rule restriction focus.

The first dimension of the classification refers to the process mining perspective that is used in the business rule. Four different perspectives on business process modeling were introduced in [21] and can also be used to classify the business rule types in this context.

- *Functional process perspective* that deals with the process elements (e.g. activities) that are being performed/occur in a process instance, as well as the relevant process artifacts linked to these process elements (e.g. an invoice artifact for a pay activity).
- *Control-flow process perspective* that covers the process behavior in terms of when process elements can be performed/occur in a process instance.
- *Organizational process perspective* that focuses on the organization behind the business process, which agent performs the different process elements in a process in-

stance taking into account factors such as timing, environmental conditions, etc.

- *Data process perspective (also known as informational perspective)* that represents the informational elements (e.g. event data, case date, etc.) that are used, produced or manipulated during the process, as well as relationships among them.

Secondly business rules can be classified along their main rule restriction focus, which represents the type of restriction that is imposed by the business rule. Five new and distinctive business rule restriction focuses are identified:

- *Cardinality-based rules* are business rules that restrict the number of allowed instances of a specific process element (i.e. of a specific activity, a specific originator or other relevant event data element) in a specific process instance.
- *Coexistence rules* can be defined as business rules that restrict the coexistence of process elements of different types over the execution of a specific process instance.
- *Dynamic data-driven rules* specify the influence of certain data elements (i.e. case or event data) and their value on the occurrence of process elements in a specific process instance.
- *Relative time rules* focus on specifying a time restriction on process elements relative to certain points in a process execution (e.g. start of a process, completion of a specific activity, etc.).
- *Static property rules* deal with specifying a specific property for a particular type of process element at a predefined process state.

While the first four rule restriction focuses deal with dynamic properties (i.e. history-based or future constraining), the last focus deals with static properties (i.e. properties in one specific process state).

An unambiguous interpretation of the business rule patterns and consequently the specific configurations, can be obtained by formally specifying them. Since business process management systems can be considered as reactive systems, linear temporal logic (LTL) is suitable to specify them. In addition to the classical logical operators, linear temporal logic specifies both unary and binary temporal operators. The unary operators $\Box p$, $\Diamond p$ and $\bigcirc p$ respectively specify that p has to hold at every position, at least at one position and in the next position of the process execution audit trail. Amongst the main binary operators we find pUq that specifies that there is a position where q holds and p has to hold in all the preceding positions of the process execution audit trail. A weak until (i.e. pWq) for which the condition that q has to hold somewhere has been dropped, has been specified.

Table 1 presents an application of rule-based compliance analysis in the insurance claim handling process. The rule-patterns belong to the control-flow perspective and deal with a coexistence rule restriction focus.

6. Second Dimension: Control Functions

The second dimension of our framework identifies and characterizes the different types of control functions that could potentially benefit from the introduction of process mining

Table 1: Rule-based compliance process analysis applied on provisions discarding in insurance claim handling

Legislation, policies and directives	The holding of unnecessary provisions in insurance is not permitted as it reduces the taxable profit (<i>legal</i>) and not desirable as it increases the required capital (<i>business</i>)
Internal control	Introduce an explicit discard of provisions in the claim handling process
Configured rule-patterns	A <i>pay for damages</i> activity must be succeeded by a <i>discard provisions</i> activity if the damages are lower than the provisions (rule 1) A <i>send rejection letter</i> activity must be succeeded by a <i>discard provisions</i> activity (rule 2)
Structured rule-based controls	$\diamond(\text{PayForDamages} \wedge (\text{damages} < \text{provisions})) \Rightarrow \circ(\text{DiscardProvisions})$ (rule 1) $\diamond(\text{SendRejectionLetter}) \Rightarrow \circ(\text{DiscardProvisions})$ (rule 2)

as a controller’s method. A distinction is made between the organization’s management, the internal auditors, the external auditors and the audit and risk committee, which is in accordance with contributions such as [75]. The rest of the paragraph discusses their respective roles and responsibilities from a corporate governance point of view, while taking process mining applications into account.

6.1. Management

The management of an organization is put in charge of running the business with a focus on accomplishing the desired goals and objectives in an efficient and effective manner [20]. In order to achieve the targets set by the Board of Directors, the management is authorized a certain budget [88]. Resulting in a strong concept of management accountability or the acknowledgment and assumption of responsibility for actions, decisions, etc. Therefore, the organization’s management is expected to implement **risk management processes**. As a result a comprehensive **internal control system** that defines adequate responses to the identified threats, is designed, implemented and maintained by the management. Effective internal control systems are relevant for achieving the organization’s objectives and preventing criminal conduct [48].

6.2. Internal Audit

The internal audit is an independent organizational function that provides an **objective opinion** (i.e. assurance) **on the effectiveness and adequacy of the risk management and control measures** implemented by the management [4]. Therefore, the internal audit department performs *substantive testing* of the implemented internal control systems. *Reporting* on the performed activities and their results (e.g. report on significant risk exposures, control issues, fraud risks, etc.) is crucial. Moreover, *recommendations* for improvements are provided when deficiencies or opportunities have been identified [75].

While the financial dimension of the operations is an important aspect of an internal audit, other dimensions can be found in the scope of the internal audit plan (e.g. assessment of operational efficiency, consistency between results and goals, IT audit, etc.). Moreover, the internal audit department can perform **consultancy engagements** for the management or special assignments at request of the audit committee (i.e. mostly gathering information) [49].

6.3. External Audit

The main responsibility of the external auditor is to articulate, as a completely independent actor, an **opinion on the reliability of the provided financial statements** [5]. Any shortcomings in the information provided in the directors report must be expressed by the external auditor. In order to come to well-founded conclusions, the external auditor performs *extensive testing* routines [4].

Additionally, an external auditor can carry out other **(internal) audit assignments on a contract basis** as long as his/her independence is not impaired [7]. For example, the external auditor can not perform both internal auditing services (i.e. a form of outsourcing) and external assurance services for the same company.

6.4. Audit and Risk Committee

The audit and risk committee refers to the operating committee of the Board of Directors that is charged with **overlooking the other organization's control functions** [56]. The committee members ensure a comprehensive and ongoing risk management process, as well as the implementation of strong and effective risk responses, i.e. internal controls. Additionally, they review policies, oversee internal audit activities and establish a communication between the different control functions.

Since the audit committee makes heavily use of the services of the other actors in corporate governance, we can conclude that they are at most an indirect user of process mining techniques.

7. Third Dimension: Control Function Activities

The control function activities that can benefit from process mining support can be grouped into three major categories: 'risk identification & assessment activities', 'control activities' and 'activities related to the generation and communication of information'. Their existence of these categories was confirmed by the Committee of Sponsoring Organizations' (COSO) Enterprise Risk Management Integrated Framework, the Internal Institute of Auditors' (IIA) International Standards for the Professional Practise of Internal Auditing and the Public Company Accounting Oversight Board's (PCAOB) Auditing Standards. While the different stakeholders all perform comparable activities in the different categories, the objective might be different [75]. In this section we provide a general overview of the communalities. The next section will go further into detail as it combines the three dimensions.

7.1. Risk Identification & Assessment Activities

The first category of control function activities focuses on identifying and assessing the impact of events that might adversely affect the achievement of the corporate objectives, i.e. risks. Note that not all events have a negative impact on the achievement of the objectives, they might also represent opportunities. During risk identification a wide variety of risks are considered as well as the internal (e.g. resource utilization and throughput times) and external factors (e.g. price movements and increases in demand) that might influence these risks [69].

The identification of potential risks is followed by an assessment of the extent to which these risks might influence the achievement of corporate objectives [20]. Risk assessment takes both the likelihood and impact of the potential risk into account [69]. Special attention must be given to uncovering relationships between risks, correlated risks need to be assessed together.

7.2. Control Activities

Adequate risk responses (e.g. internal controls) must be implemented for the identified risks. There exists a wide-variety of risk responses, ranging from passive after-the-fact detection to preventing mechanisms [48]. Depending on the severity of the risk's potential impact, management selects a specific response to mitigate that specific risk [69]. Several types of risk responses can be implemented with process mining techniques, e.g. detective controls.

Additionally, the different stakeholders have an important role in the effectiveness assessment of the risk responses. Both managers and auditors perform a combination of separate and ongoing evaluations of the internal controls (i.e. respectively monitoring and effectiveness assessing) [49, 61]. Furthermore, auditors will investigate sets of transactions to determine whether adequate risk responses were formulated in the first place [75]. Similarly, monitoring of risks that were accepted by the management, i.e. no risk mitigation response was implemented, remains required as a changing environment might affect their potential impact [31].

In conclusion the set of control activities covers all activities related to implementing internal controls, monitoring activities and processes as well as assessing the effectiveness and adequacy of the implemented internal controls.

7.3. Activities Related to the Generation and Communication of Information

The third group of control function activities focuses on the generation and dissemination of information. Every stakeholder requires a wide range of information to identify, assess and respond to risks, as well as to run the organization [88].

Historical data, as can be found in event logs, allows for evaluating actual performance to targets, plans and expectations [20]. Moreover, by carefully partitioning the data the performance can be analyzed under different conditions, trends can be discovered, etc. Historical data can also contain symptoms of important risk events for the future. Capturing the data in actionable information that can be easily interpreted by the right stakeholder has become a major challenge. Additionally, important uncovered process deviations must be carefully documented and communicated to the relevant stakeholders [4].

8. Combining the Three Dimensions: Proposals for Effective Process Mining Support to Control Function Activities

Combining different positions on the three dimensions of the applicability framework results in proposals for an effective use of process mining in the context of risk management, compliance checking and auditing. The guidance proposals are grouped per stakeholder category, as the interpretation of the control function activities are often determined by the stakeholder type. In the next section we elaborate two sample cases.

8.1. Process Mining Applications for (Risk) Management

Contemporary organizations are confronted with a lot of uncertainties, which will partially result in **business risks** eroding the organizational value. As the management is ultimately responsible for the GRC-processes [88], they should assume ownership of them. The **Enterprise Risk Management Integrated Framework (ERM)** proposes eight interrelated components that together describe the way management typically runs an organization [20]. Table 2 presents an overview of the different types of process mining support for managers.

The first two stages that provide the basis for risk management and compliance checking, are not considered within the scope of the proposed applicability framework. However, there exist opportunities for (indirect) process mining support in these stages.

Firstly, the *internal environment* component covers a wide variety of internal factors, which provide the basis for the organization's enterprise risk management approach as well as discipline and structure. Some of the most notable include the risk appetite (i.e. amount of risk the entity is willing to accept), ethical values, organizational structure, authority and responsibility. Process mining can provide effective support in the context of *uncovering organizational structures, roles and responsibilities*. Conclusions can be drawn from the results of the organizational miner with the doing-similar-tasks metric [94] and from the originator-by-task matrix [112]. Indirectly, process mining can *improve the internal environment* by enabling the implementation of procedures to monitor the operations. The applicability of process mining for monitoring will be further illustrated in the manager's control activities section.

Secondly, the *objective setting* component deals with broadly defining what the organization aims to achieve. Objectives are defined at strategic level and form a basis for operational, reporting and compliance objectives. In this context process mining can be effectively used for constructing *an overview of high frequent process behavior and performance*, building a strong foundation for this component. The frequent process behavior could be best uncovered with the heuristics miner with standard parameterizations [120] or with the fuzzy miner [43]. Process performance could be analyzed with the performance sequence diagram plug-in and the performance analysis with petri nets plug-in for ProM [111].

The remainder of this section provides an overview of the process mining support in the different ERM-framework components that are directly linked to the proposed control function activities.

Risk identification & assessment activities performed by managers. The risk identification & assessment control activity category covers the activities performed in the context of the following ERM-framework components:

- the event identification component
- the risk assessment component
- the risk response component

Firstly, *event identification* deals with identifying internal and external business events that might (adversely) affect the achievement of the organization's objectives. In this setting process mining techniques that allow for an *open-minded analysis* (e.g. visualization techniques presented in 5.1) and that enable the identification and *classification of execution patterns* will be most suited (e.g. performance sequence diagram [111] or trace alignment and clustering [52]). Significant deviations can indicate underlying risk [9]. Focus will be placed on identifying internal business events. In addition, this component could benefit from techniques that *combine history-based findings with simulation techniques* (e.g. with ARENA) to predict the effects of events that were not previously encountered, such as the impact on a bottleneck when the organization attracts an important new contract.

Secondly, the *risk assessment* requires accurate estimations of both the business risk's probability of occurrence and the severity of its impact [69]. As specific risks can usually be formally specified in specific process patterns, rule-based property verification techniques as presented in section 5.3, can provide the necessary information for the calculation of descriptive statistics and for the *determination of the possibility of occurrence*. Additionally, when the available data spans periods with different environmental conditions process mining enables the *analysis of the relation between the event frequency and specific environmental conditions*. General data mining algorithms will typically be used to uncover these relationships. Furthermore, the event log can be used for *uncovering correlations between business events*. In-depth analyses of the additional case data in event logs can assist in *estimating the severity of the impact of a certain event*. Trace clustering based on profiles different from the activity profile can be used in this case, e.g. the technique presented in [93].

Thirdly, Process mining can not directly support the *risk response* activities. However, process mining techniques allow for creating clear visualizations, reports and statistics. These representations enable the decision makers to more precisely *position the identified risks on a risk matrix*, which projects a risk on the different bands of risk significance based on the likelihood of occurrence and the magnitude of the impact [20]. Depending on the band of risk significance, the management will opt for a specific risk response: risk acceptance, risk detection, risk avoidance or risk insurance [69].

Control activities performed by managers. The second activity category of the proposed applicability frameworks can be composed of the following ERM-framework components:

- the control activities component
- the monitoring component

The *control activities* component covers the activities related to the design of the internal controls and the control implementation. These activities focus on ensuring an

adequate execution of the risk responses. Traditional process mining techniques, especially the rule-based verification approaches presented in 5.3, are suited for *implementing retrospective detective internal controls*. These controls are usually applied in the context of a risk acceptance response, which are risk responses that do not require preventive measures. Additionally, process mining pattern recognition techniques, such as [111, 52], can be used to identify the *occurrence of specific patterns that tend to be symptomatic* for particular risk types, and thereby form a partial solution for corrective controls.

Process mining is extremely applicable for the **monitoring** component of the ERM-framework. The rule-based process mining techniques (section 5.3) can be used to evaluate the *evolution in both the risk's impact severity and possibility of occurrence*. Regular targeted process mining analyses (e.g. visualization of certain process parts, specific property testing with business rules, etc.) can therefore add to existing approaches. These observation activities are especially important for risks that are accepted previously, but that can evolve into significant threats. Moreover, these process mining techniques enable the *validation of the procedures* put in place for an effective implementation of the risk responses. Note that the assessment of the internal control effectiveness in the context of the monitoring component is primarily oriented towards the corrective and preventive controls.

Information generation and communication activities performed by managers. Indirectly process mining techniques can also improve the **information and communication** component of the ERM-framework, as these techniques allow for the construction of comprehensive and clear *reports*, graphs and other visualizations. Pattern analysis results in information that might suggest important improvements of the existing processes.

8.2. Process Mining Applications for Internal Auditing Activities

The responsibility of the internal audit consists of both providing assurance services and consulting services. Assurance services focus on providing an independent and objective opinion on an entity, an operation, an internal control or another subject matter [75]. The consultancy services are performed at the specific request of a stakeholder (e.g. the management or the audit and risk committee) and are advisory in nature [49]. However, management responsibility should never be assumed. A wide variety of applications for process mining exist in the context of internal auditing. The remainder of this section is primarily based on the responsibilities of an internal auditor as described in the *International Standards for the Professional Practice of Internal Auditing (Standards)* [97]. The codes used in this section refer to sections in this document. Table 3 presents an overview of the different types of process mining support for internal auditors.

Risk identification & assessment activities performed by internal auditors. An internal auditing activity starts with *establishing a risk-based plan of engagements* that identifies the priorities of the activity and delineates the scope of the activity (2010). These plans of engagements are based on regular documented *risk assessments* and must be consistent with the organization's goals (2010.A1). When *determining the exact engagement objectives* the internal auditor conducts a preliminary assessment of the risks related to the subject under review (2210.A1). Consulting engagements require the internal auditors to be alert to the existence of other (*correlated*) risks (2120.C1).

Table 2: Overview of the process mining support for managers (●: full support, ◐: partial support and ○: no support)

Control Function Activity	ERM-Framework Component	Specific Management Activity	PD&V	CC&DA	RBPV
Risk identification and assessment	Event identification	Perform an open-minded analysis	●	●	◐
		Classify the execution patterns	●	○	○
		Simulate	●	○	○
	Risk assessment	Estimate risk probability	◐	◐	●
		Estimate risk impact	○	○	●
		Uncover relation between event and environmental conditions	◐	◐	●
	Risk response	Position the identified risk	◐	◐	◐
Control activities	Control activities	Implement detective internal controls	◐	◐	●
	Monitoring	Recognise patterns	◐	◐	●
		Evaluate evolution in probability	◐	◐	●
		Evaluate evolution in impact	○	○	●
		Validate internal controls	◐	◐	●
Information generation and communication	Information and communication	Support reports	●	●	●
Other	Internal environment	Uncover organizational structures, roles and responsibilities	●	○	●
		Improve internal environment	◐	◐	◐
	Objective setting	Acquire an overview of high frequent behavior	●	○	○
		Evaluate process performance	●	◐	◐

Results obtained through analysis in the context of a consulting engagement must be taken into account when evaluating the organization’s processes (2120.C2).

The internal auditor can make use of the process mining techniques described in the context of risk identification and assessment activities for the management: i.e. an open minded analysis, the clustering of trace patterns, simulations, rule-based risk assessment and correlation analysis.

Control activities performed by internal auditors. The international standards for professional practice of internal auditing document stipulates two important sets of activities that are related to the control activities performed by the internal auditors: (1) the actual performance of the engagement and (2) monitoring progress. The use of technology-based audit techniques and other data analysis techniques, e.g. process mining, is advisable according to the statement on due professional care in (1220.A2).

Internal auditing activities provide support to the organizations in maintaining effective controls by providing an objective and independent opinion on the effectiveness and the efficiency of these controls (2130). Consequently the *performance of the en-*

gagement determines whether the controls are able to respond to risk related to the organization, its operation and its information systems regarding (1) the reliability of the financial and operational information, (2) the safeguarding of the assets and (3) compliance with laws, regulations, policies, procedures and contracts (2130.A1 and 2120.A1). Process mining techniques can provide the internal auditor with effective support for the identification, analysis, evaluation and documentation of sufficient information in order to achieve the objectives stipulated in the engagement plan (2003). A wide variety of techniques allow the auditor to form an opinion on the effectiveness of a specific control (ranked according to a decreasing suitability):

- Rule-based property verification: As laws, regulation, policies, procedures and contracts can be easily translated into control objectives and business rules [37], rule-based property verification approaches as presented in section 5.3 are highly suited. The rule classification framework described in section 5.3.2 is populated with a wide variety of rule-patterns covering the most common constructs in control objectives [12].
- Conformance checking: When the auditor possesses an approved and fully compliant prescriptive business process model, the auditor can apply the conformance checking approaches presented in section 5.2. However, the results tend to provide an interesting overview but often lack the required detail. Deriving which law, regulation, policy or procedure has been violated in which specific cases might be an arduous task.
- Process discovery and visualization: Certain process discovery techniques (mostly originator perspective oriented) can be used as data analysis techniques during the performance of the engagement. For example the originator-by-task matrix, as presented in [112] or the organizational miner with the hand-over metric [94], can be used to analyze task allocations including segregation of duties controls based on exclusive roles.

The conclusions presented by the internal auditors must be based on engagement results that are obtained with the appropriate analysis techniques (2320). Where necessary, *appropriate recommendations* for improving the processes must be provided (2110). If the analysis indicated that a specific variant of cases frequently results in a violation of a law, regulation, policy, procedure or contract, the recommendation can focus on this specific subset of the population.

The Internal auditing department provides a ***wide variety of consulting and assuring service types***, including IT-auditing, forensic auditing, operational auditing, regulatory compliance analysis, etc. Process mining can be used in the context of *IT-auditing* when the audit object is the information system (not an IT-strategy) and the scope is limited to evaluating both the existence and the operational effectiveness of the implemented control measures (2110.A2). The process mining techniques can also be effectively used in the context of *forensic auditing* in order to analyze specific fraud issues (2120.A2). Answers to questions such as the how, where, what, why and who can be answered. Moreover, process mining techniques combined with statistical tests allow for the identification of hidden relationships between people and events or multiple events. They are often an expedient to analyze suspicious process cases. Both IT-auditing and

forensic auditing can make use of the techniques described above. *Operational auditing* that deals with assessing the performance of an organizational object, on the other hand, can benefit from a wide variety of additional techniques. Performance has two dimensions: the effectiveness (i.e. the extent to which organizational objectives are accomplished such as reducing cycle times, attaining sales levels, etc.) and the efficiency (i.e. the amount of resources needed to attain those objectives such as limited reworks, limited external consultation, bottleneck identification, etc.). Event logs usually contain a lot of information that can be used to *quantify the most common key performance indicators* for both efficiency and effectiveness. An overview of the set of process mining tools for analyzing overall performance and in-depth analysis of certain cases can be found in [112]. This set includes the the performance sequence diagram, the (advanced) dotted charts analysis, the basic performance analysis, the performance analysis with petri nets, etc. Additionally, rule-based property verification approaches can be used, e.g. to determine the existence of reworks [105].

According to (2500.A1) the chief audit executive is responsible for establishing and maintaining a system to *monitor* and ensure that the actions implemented by the management have been effective (in case the management has not accepted the risk) and *follow-up* on the recommendations. Since the event log data collection techniques, the process mining methods and the rules are well defined at this stage, the internal audit department can reuse them to monitor and follow-up on the evolution in the effectiveness of the internal control system.

Information generation and communication activities performed by internal auditors. Sections (2330 and 2400) respectively specify that the internal auditor is obliged to *document* the relevant information supporting his opinions and *communicate* the results of the engagement. Process mining enables the internal auditor to produce and communicate accurate, objective, clear, concise and timely information, as dictated in section 2420 on the quality of the communications. When using configured rule patterns that do not suffer from interpretation distortions, rule-based analysis techniques can provide faithful and accurate information on the underlying facts. Objectiveness of the information comes from the ability to test the complete population in a fair and impartial manner. Process discovery and visualization tools can be applied to provide a clear graphical representation of the ineffectiveness of the internal controls. Rule-based testing approaches enable the auditor to individually identify all non-compliant cases. All process mining techniques can be used to provide a timely assessment of the full population, making a timely dissemination of the results possible.

8.3. Process Mining Applications for External Auditing Activities

In this section we discuss the applicability of the different process mining techniques for the individual control function activities performed by external auditors. While external auditors can provide internal auditing services, this section will focus on their independent assurance services with regard to the financial statements of an organization. Table 4 presents an overview of the different types of process mining support for external auditors. The remainder of this section provides references to the corresponding Audit Standards (AS) as they were drafted by the Public Company Accounting Oversight Board.

Table 3: Overview of the process mining support for internal auditors (●: full support, ◐: partial support and ○: no support)

Control Function Activity	International Standards for the Professional Practice of Internal Auditing	Specific Internal Audit Activity	PD&V	CC&DA	RBPV
Risk identification and assessment	2210.A1	Determining objectives	◐	◐	●
	2010.A1	Establish a risk-based plan of engagements	◐	◐	●
	2120.C1	Examine correlations between risks	○	○	●
Control activities	2130.A1 and 2120.A1	Assess and formulate an opinion on control effectiveness	◐	◐	●
	2110	Uncover variants and correlated violations for appropriate recommendations	◐	○	●
	2110.A2	IS auditing: operational effectiveness of IS implemented controls	◐	◐	●
	2110.A2	Forensic auditing	◐	◐	●
		Operational auditing: effectiveness	●	◐	●
	2500.A1	Operational auditing: efficiency	●	○	●
Monitor evolution		◐	◐	●	
Information generation and communication	2330, 2400 and 2420	Document information supporting the opinion	●	●	●
		Communicate the results from the engagement	●	●	●

Risk identification & assessment activities performed by external auditors.

External auditors are especially interested in determining the risks related to accepting and performing an engagement with a client, this type of risk is called the *engagement risk*. Rule-based property verification approaches, as described in section 5.3, can be employed to analyze some of the determining factors for engagement risk. Examples of these factors that can be distilled from the event log are: the identification of operations that are dominated by a single individual, the determination of the actual number of clients that have done business with the organization that year, or the identification and analysis of the presence of a high volume of significant year-end transactions in specific business processes [28]. Beside these quantitative factors that can be analyzed with process mining, the engagement risk also has qualitative determining factors such as a judgement on the integrity of the client’s management.

The external auditors have to find an optimal selection of controls to test and determine a right amount of testing that will be needed. In addition to relying on previous risk identification and assessment results, experience and additional process exploration, the external auditor may wish to rely on the work performed by the internal audit department (AU Section 302). Thereby, the external auditor can focus on complementary tests that increase the total test coverage [5]. Performing an *assessment of the technical capabilities of the internal audit department* is advised, and can be obtained by

performing a limited set of overlapping testing procedures. The process mining-based methodology is comparable to the one used by the internal audit department.

Control activities performed by external auditors. External auditors provide an opinion on the reliability of the provided statements. Therefore, the external auditor should analyze and assess the risk of material misstatements at two levels: the risk without the implementation of an internal control system and the risk of not preventing or detecting a misstatement after the implementation of the internal control system (AS 12). The former is the inherent risk in the business process, the latter the control risk. The fifth paragraph of AS 12 discusses six risk assessment procedures, containing two procedures that could benefit from process mining support:

- obtaining an insight in the internal control system
- the performance of analytical procedures

The first procedure, obtaining an *insight into the individual components of an internal control system*, is based on identifying and assessing the types and factors of potential misstatements which should result in the design of further audit procedures (AS 12 paragraph 18). One way to obtain a thorough understanding of the different components of the internal control system is by performing *walkthroughs*, i.e. analysis of individual transactions in the organization's operation (AS 12 paragraphs 20 and 37, as well as in [28, 5]). Process discovery algorithms, as described in section 5.1 enable the external auditor to visualize this process. This is a combination of observing the operations and inspecting the relevant documentation. A key assumption in this context is that the business operations can be completely decomposed into business processes. In more traditional auditing approaches it is common to decompose the business operations in a set of transaction cycles. In [4] the sales cycle is described, this cycle is composed of different business processes such as processing customer orders or shipping goods. For assessing the effectiveness of the individual *internal controls*, the external auditors can use the same techniques as the internal auditor (AS 13 paragraph 16-35).

Secondly, external auditors can perform *analytical procedures* with process mining techniques, and rule-based property verifications in particular. Analytical procedures enable the external auditors to obtain an understanding of the organization's operations and the related significant events (AS 12 paragraph 46 a). Additionally, these procedures should allow the external auditors to identify areas that might represent specific risks, such as the occurrence of unusual transactions or events, unexpected amounts or ratios and trends that require further investigation (AS 12 paragraph 46 b). Analytical procedures underwrite the basic premise that plausible relationships among data exist, which is found reasonable in AU section 329 paragraph .02. Variations in this relationship may indicate amongst others: specific unusual transactions or events, accounting changes, business changes, random fluctuations or misstatements. These variations can be identified with process mining techniques. While rule-based property verification techniques seem the most suitable in this context, the same technique ranking as for internal audit testing applies. Using process mining enables the auditor to inspect the real business processes of the different transactions and not just the outcomes.

Information generation and communication activities performed by external auditors. The generation and communication of information recurs in multiple paragraphs of different auditing statements, but always falls back on the concept of *audit documentation* also known as the *auditor’s working papers*. Auditing statement 3 paragraph 4, provides a description of the facts that evidence the auditor’s decision and thus need to be documented. This audit documentation is mandatory and should provide sufficient detail (AS 4 paragraph 4). In paragraph 12 of AS 3, the Public Company Accounting Oversight Board prescribes the documentation of significant findings or issues. AS 13 paragraph 18 discusses the documentation on the testing of the effectiveness of the implemented internal controls.

Process mining techniques provide clear and detailed outputs for all the analyses and is therefore suited in the context of the audit documentation as specified in the auditing standards.

Table 4: Overview of the process mining support for external auditors (●: full support, ◐: partial support and ○: no support)

Control Function Activity	Auditing standard	Specific External Audit Activity	PD&V	CC&DA	RBPV
Risk identification and assessment	AU section 302	Determine engagement risk	◐	◐	●
		Assess the technical capabilities of the internal audit department	◐	◐	●
Control activities	AS 12 §20 and 37	Obtain insight in ICS: walkthroughs	●	○	◐
	AS 13 §16-35	Assess internal controls	◐	◐	●
	AS 12 §46 a-b	Analytical procedures	◐	◐	●
Information generation and communication	AS 3 §4, AS 3 §12, AS 4 §4 and AS 13 §18	Draft audit documentation	●	●	●

9. Process Mining for Risk Management and Auditing: Case Research

This section demonstrates the applicability of the presented framework on a controlled experiment in the insurance industry and on an observational case study in software development. The former presents the analyses from an auditing perspective, while the latter focuses on the analyses traditionally performed in the context of management control.

9.1. Controlled Experiment: Auditing in the Insurance Industry

Case description. The controlled experiment in this section is based on an artificially generated event log for an insurance claim handling process, which focuses on processing insurance claims that do not include bodily injuries. The use of an artificially generated event log enables us to precisely demonstrate interesting and detailed concepts, e.g. event correlation. The generic structure of such a claim handling process can be conceptualized as a three-stage process: the claim intake stage, the claim evaluation stage and the claim settlement or rejection stage. In this experiment we focus on the last stage that groups all activities related to the settlement or rejection of a claim: sending the insured a

notification on the evaluation's outcome, proposing a settlement, approving the pay for damages and calculate the new insurance premium.

The event log contains 694 cases covering 2847 business events. Three scenarios were simulated for the handling of an admitted insurance claim and one for dealing with rejected insurance claims.

Risk identification and assessment. Figure 8 provides a visualization of the real-world third stage subprocess, which has been obtained with the heuristics miner [120]. The two main variants can be distinguished: the rejected and the admitted claims. Whereas for the rejected claims the handling process is immediately ended after the notification, the admitted claims are further processed. However, from an event identification point of view, two major issues with this process can be immediately identified. Firstly, in 38 claim handling cases the settlement proposal was not approved nor did a recalculation of the insurance premium took place. Secondly, while the approval took place in 474 claim handling cases, the insurance premium was recalculated in only 472 cases. Both deviations might have a significant impact: unapproved settlements might indicate insurance fraud and unchanged insurance premiums may result in premiums that do not reflect the real risk involved in the insurance contract.

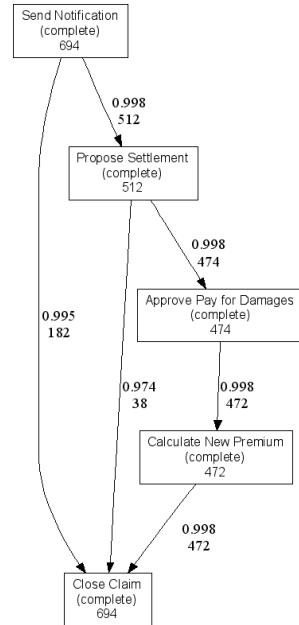


Figure 8: Event identification based on visual inspection of a heuristics net

The historic data included in the event log allows for an extensive risk assessment. Relatively straightforward is the calculation of the *relative frequency* (f) of the instances with important process deviations, i.e. the number of deviating instances (n_d) to the total amount (n_t).

$$f = \frac{n_d}{n_t} = 0.057$$

However, different types of risk related events might frequently occur together. For example, further analysis of the event log uncovers that when an approval or premium recalculation is missing, the other activity is often missing too. Quantifying the strength of association between different events can be done with a χ^2 test. In this context the H_0 can be defined as *the presence of one activity is not associated with the presence of the other activity*.

Table 5: Related events: classification of process instances

	Premium recalculated	Premium unchanged
Approval present	472 (<i>a</i>)	2 (<i>b</i>)
Approval absent	0 (<i>c</i>)	38 (<i>d</i>)

$$\chi^2 = \frac{(ad - bc)^2(a + b + c + d)}{(a + b)(c + d)(b + d)(a + c)} \Rightarrow p \ll 0.01$$

The H_0 is hereby strongly rejected. Consequently, during the risk assessment this association should be taken into account.

Control activities. After determining the scope of the audit plan based on the risk identification and assessment, the actual control effectiveness evaluations have to be performed with substantive testing. A rule-based property verification approach seems the best option in this context. Table 6 provides an overview of the rule-based substantive testing performed for this subprocess. The first two rules are activity coexistence rules that require the execution of a certain activity if an other activity has been performed. This type of rule belongs to the set of business rules that combine the functional perspective and the event coexistence rule perspective. These two rules directly map on the issues found in the previous risk identification and assessment phase. An analysis of the segregation of duties is performed with the last rule, as an issue was uncovered by reviewing the hand-over work metrics in the social network miner [108]. All the tests were performed with the LTL-checker [105].

Table 6: Configured rule patterns for testing the internal control effectiveness

Configured rule pattern	Number of violations
$Activity(ProposeSettlement) \Rightarrow \diamond Activity(ApprovePayForDamages)$	38
$Activity(ProposeSettlement) \Rightarrow \diamond Activity(CalculateNewPremium)$	40
$\forall P((Activity(ProposeSettlement) \wedge Originator(P)) \Rightarrow \neg(\diamond Activity(ApprovePayForDamages) \wedge Originator(P)))$	52

Information and communication. The results from the rule-based process mining analysis enable an exact documentation of the evidence on the lack of internal control effectiveness in this process subpart. Moreover, it enables the (internal) auditor to provide motivated recommendations to the management for improving the internal control system. As it appears that there exist correlated risks in this process, the management has several risk response options to choose from.

9.2. Observational Case Study: Management Control in the Software Development Process

Case description. The event log for the observational real-world case was retrieved from the process-oriented project tracking and management tool JIRA. This event log originates from an organization that focuses on providing human resources management services to companies that want to contract out specific business processes, such as payroll administration. In this industry a competitive advantage can be obtained by providing a superior (i.e. user-friendly, lots of functionalities, etc.) web-based platform to upload the data necessary to perform the outsourced processes. Additionally, the organization faces a highly evolving regulatory environment, requiring continuous updates and adaptations of its information systems.

The event log describes the unclassified and completed real software development activities for a month. In total the event log contains 463 events scattered over 158 cases, which either relate to an important software update or a debugging request. The activity subset $\mathcal{A} = \{\text{new feature business analysis, bug report analysis, information request, functional analysis, development, testing}\}$, the originator set \mathcal{O} encompasses 36 employees and the property set $\mathcal{P} = \{\text{case ID, timestamp, type of intervention, priority, summary}\}$.

Risk identification and assessment. Figure 9 presents the process model that was obtained with the alpha++ miner [25]. Amongst the uncommon transitions, several major issues can be immediately observed. Firstly, in some process instances no form of business analysis has been performed: the transition between start and functional analysis and the transition between start and development. Secondly, for some process instances the control-flow does not contain any actual development activity. In addition there are unusual transitions in the process model that do not appear in the data set (determined with rule-based property verification techniques) and therefore can be attributed to the need for generalization in process mining, e.g. according to the process model an instance could exist solely of testing.

Similar conclusions can be drawn from the result of the conformance checker [84], see figure 10. This model shows the designed process overlaid with information on the actual process executions. The positive numbers in the places of the petri net indicate that for a specific instance an activity was expected to occur at that point in time but did not happen, while the negative numbers indicate that the activity was performed when it should not have taken place at that point in the sequence. The amounts also give an idea of the number of issues in this process.

Control activities. Due to space considerations, we restrict the example to a subset of control objectives related to the main objective of keeping customers satisfied. As the produced software is the main product of our service provider, the control objectives ‘ensure that clients requirements are identified and communicated’ as well as ‘ensuring that these requirements are adequately addressed’ become crucial. In order to achieve these objectives a multitude of internal controls can be devised and implemented, e.g. ‘the existence of a new feature business analysis’, ‘a bug report analysis or an information request’ and ‘a separation of the development and testing responsibilities’. Table 7 presents two rules that could be used to implement detective controls in the information system or to assess the effectiveness of the implemented internal controls. Firstly, an activity inclusion rule that is related to the functional process mining perspective and

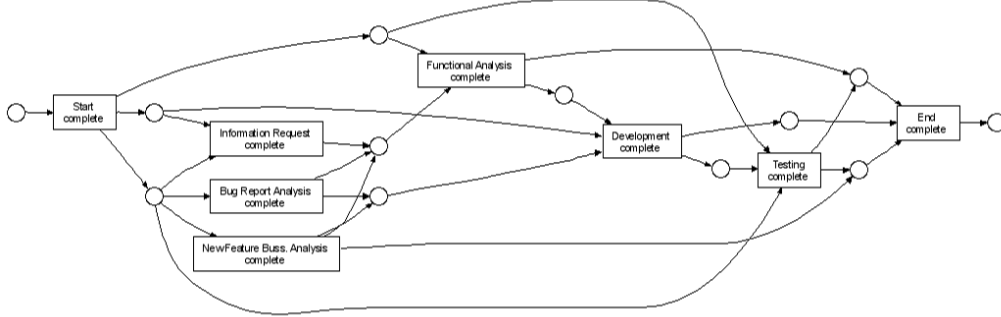


Figure 9: Event identification based on visual inspection of a discovered process model (alpha ++ miner)

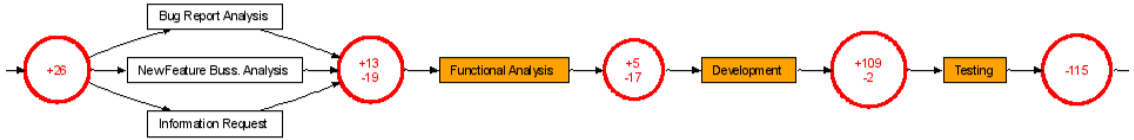


Figure 10: Event identification based on a conformance checking result

the cardinality-based rule restriction focus. The second rule, a temporal deontic rule, which belongs to the combination of the organizational process mining perspective and the coexistence rule restriction focus.

Table 7: Risk management in software development case

	Rule 1: Activity inclusion	Rule 2: Temporal deontic rule
Objective	Ensure that the clients requirements (functional, legal, contractual, etc.) are identified and communicated.	Ensure that these requirements are adequately addressed in the developed software.
Risk	Non-compliance areas not identified, outdated requirements remain in effect, etc.	Financial losses and penalties, decreased customer satisfaction, increased likelihood of disputes, etc.
Internal control	Each process instance must contain a <i>new feature business analysis</i> , <i>bug report analysis</i> or <i>information request</i> activity.	<i>Person P</i> with role <i>tester</i> must perform the <i>testing</i> activity after the <i>development</i> activity and that <i>person P</i> may not have performed the <i>development</i> activity.
Business rule	$\diamond(\text{Activity}(\text{newfeaturebusinessanalysis})) \vee \diamond(\text{Activity}(\text{bugreportanalysis})) \vee \diamond(\text{Activity}(\text{informationrequest}))$	$\forall P \in \mathcal{P} : (\text{Activity}(\text{development}) \wedge \text{originator} = P) \Rightarrow \bigcirc(\diamond(\text{Activity}(\text{testing}) \wedge \text{role} = \text{tester} \wedge \neg(\text{originator} = P)))$

Information and communication. A wide variety of information can be retrieved from the process executions. In the context of the management control activities earlier presented, the management could provide an in-depth overview of the issues based on the additional data present in the event log. The resulting information is summarized in table 8.

Table 8: Results of a rule-based business process analysis in the software development case

	Rule 1: Activity inclusion	Rule 2: Temporal deontic rule
Number of compliant instances (relative percentage)	132 (83.5%)	156 (98.7%)
Number of compliant instances = ‘Bug’ (relative percentage)	57 (87.7%)	64 (98.5%)
Number of compliant instances = ‘New Feature’ x Priority = ‘Critical’ (relative percentage)	28 (80.0%)	0 (0.0%)

10. Evaluating Process Mining Support for Control Function Activities: Assumptions, Opportunities and Future Research

The previous sections presented a comprehensive framework for the applicability of process mining in the context of risk management, compliance checking and auditing. Here we evaluate the potential process mining support for the control function activities. Two important assumptions for process mining are presented, i.e. the improvement of the data quality and the preprocessing capabilities. Furthermore, this section discusses the opportunities for strategic advantages that can be obtained with process mining over more traditional techniques. In addition to the fact that the auditors credibility is generally higher when they use new technologies [96], we distinguish four opportunities to improve the (auditing) process: (1) pursuing absolute assurance and its related effects, (2) acquiring full insight in the real business processes, (3) high independence and (4) the persuasiveness of the evidence provided with process mining techniques. The major topic for future research deals with the reduction of the time-delay between the occurrence of an event and the reporting on that event. Tackling this challenge will result in a further improved fit between process mining and the needs for control activities.

10.1. Data Quality & Preprocessing Assumptions

Control-oriented analyses require event logs that meet high quality standards in order to derive meaningful conclusions. Four main quality criteria can be distinguished: the recording of the events should be done in a **trustworthy, securely, systematic and accurate** manner. The data in an event log of an information system must be recorded in a *trustworthy* manner, e.g. ID fraud or backdating must be impossible. Additionally, these recordings must be kept *securely*, which refers to the prevention of any tampering with the data after the recording. The third quality criteria, *systematic recording*, reflects the need for a timely recording of every important business event (i.e. completeness). In addition to the start and end events for activities, the recording of denial events (resulting from trying to perform unauthorized activities) and the activity cancel events might be interesting from a control perspective as they might indicate potential fraud attempts. *Accuracy* can be regarded as a measure that reflects the correctness of the representation in the event log compared to a real-life event. This can be determined both on syntactical as semantical level. In [50], for example, it is argued that major ERP systems can contain missing and faulty data values. While trustworthy & securely recording looks at the possibilities for humans to influence the recorded data, accuracy

focuses on the ability of the provenance system to correctly record the data (i.e. noise because of technical errors). As for other computer-assisted auditing and monitoring approaches, the data quality of the event logs needs to be tested.

Traditionally, there exists a **conceptual mismatch between ERP systems and process mining**, as these information systems are conceived with a data viewpoint in mind [55, 77]. Contemporary information systems consist of thousands of tables and transaction codes [50]. While tables are linked with foreign keys, a single process identifier can often not be found. Additionally, we often observe an overlap in the functionality of these transaction codes, multiple transaction codes can be related to a single activity [50]. Therefore, (re)composing a business process can be challenging and requires the ERP systems reference models. Moreover, since timestamps are often not accurately specified the ordering of the activities in a process model can become rather arbitrarily [110].

The actual preprocessing challenges are: **the selection of a suitable instance level, dealing with convergence/divergence and attribute selection**. Instance level selection is partially determined by the scope of the control-oriented analysis, i.e. the business object under evaluation. However, the major determinant will be the granularity of the available events (e.g. availability of order related events versus order line related events). Related to the instance selection challenge are convergence and divergence issues [91]. Convergence refers to the phenomenon in which the same activity is executed on multiple process instances at once, e.g. a client pays for multiple orders at once. Divergence on the other hand refers to the business situation in which the same activity is executed multiple times for one process instance, e.g. for each order line of a single order a delivery activity is recorded. Another important preprocessing decision is the attribute selection. When too many attributes are included in the event log, the log becomes unnecessarily large, hard to handle, difficult to load in various tools, etc. On the contrary, if too few attributes are included some analyses will become impossible. The scope of the analysis should help clear this up.

10.2. Approaching Absolute Assurance & Achieving Low Detection Risk Opportunity

The major enabler for process mining as a computer-assisted auditing technique (CAAT) will be the increased level of audit assurance and its effects on the provided evidence and audit risk. Audit assurance is a measure used to indicate the level of certainty that an auditor has obtained about the statements, which are mostly related to the absence/existence of material weaknesses, made in his audit report [4]. Different levels of assurance have been identified: limited, reasonable and absolute assurance [5]. However, no strict definitions have been provided in the literature.

Process mining techniques enable the auditor to perform the tests on the full population and thereby offering (near) **absolute assurance**, with a marginally higher cost in terms of processor time compared to sample-based testing with process mining. Consequently, the risk that the evidence will fail to detect any misstatements, i.e. detection risk and an important driver for the engagement risk of an external auditor, is likely to be insignificant.

10.3. Gaining Insight in (Non-Deterministic) Processes & Achieving Effective Communication Opportunity

Flexibility in business processes and client interactions is becoming an important determinant of operational excellence in organizations [57]. In order to deal with the idiosyncracies of the real-world it is not uncommon that business processes significantly deviate from their process model [107]. Therefore process visualizations, discovered with process mining techniques, may provide the stakeholders with a much richer input compared to traditional process design models [11]. Additionally, the business processes performed by knowledge workers often tend to be rather non-deterministic [67]. Process visualizations enable **effective communication**, which may lead to a more focused, efficient and effective continuation of the control process [65].

10.4. Realizing Complete Auditor Independence Opportunity

The value of an audit (report) is largely dependent on the independence of the persons involved in the auditing process from the organization that is being audited [4]. Two major architecture types have been proposed in the context of analytic CAATs; internal (e.g. embedded auditing modules architecture [41]) and **external** (e.g. monitoring and control architecture [118] and process mining based auditing) auditing modules. In contrast to the internal auditing module architectures that directly affect the clients information systems, the external auditing module architectures only use the output of the client's software. Consequently, process mining based auditing approaches belong to the group of external monitoring architectures. The external monitoring modules provide a high auditor independence, as required in sections 1100 and 1110 of the International Standards for the Professional Practice of Internal Auditing (Standards) [97].

Firstly, the functionality of the audit modules is **designed and maintained by the auditor** (or his/her firm), without any possible interference from the client or his system administrators. Secondly, architectures based on external auditing modules can fully guarantee that the **non-existence of a-priori knowledge** of the client about the auditing approach and procedures. In contrast, the implementation of internal auditing modules would require cooperation of the client, which might result in a-priori knowledge with the client. Consequently, the client could use this information to conduct fraudulent behavior that would not trigger any alarms with the auditor. Other advantages of external over internal auditing modules include: the absence of legal liability for side-effects (e.g. decrease in performance) [58] of the modules in the client's information system and the reusability of the modules as they are not written in information system specific languages (e.g. ERP programming languages) [26]. Note that the independence is primarily focused on auditing, but not restricted to this GRC function.

10.5. Obtaining Persuasive Evidence Opportunity

The persuasiveness of the evidence obtained through process mining techniques is expected to be high, due to the competence and the sufficiency that can be attained. According to [4], the **competence of the evidence** is mainly determined by the independence of the provider, the evaluator's direct knowledge, the degree of objectivity and the timeliness (referring both to the period covered and the ability to reduce the time-delay). While most of these determinants can be easily related to the basic advantages of process mining as discussed in the previous sections, a continuous monitoring or

auditing approach is required in order to outperform the traditional monitoring or auditing techniques on time-delay related timeliness (see subsequent section). Due to the fact that the whole population of transactions can be efficiently inspected, the **sufficiency of the evidence** can be optimal. This latter is also related to section 1220.A1 of the International Standards for the Professional Practice of Internal Auditing (Standards) [97] and AS 15 paragraph 7.

A high persuasiveness of the evidence provided by a stakeholder with a control function, unlocks **opportunities for cooperation between different types of controllers** [4]. Since the external auditor must always assume the sole responsibility for the audit opinion, the conclusions described in the internal auditor’s working papers need to be well founded and credible. Process mining as a methodology for compliance analysis may result in credible conclusions based on extensive testing. Moreover, a detailed documentation of possible issues about specific business cases can be obtained. While it remains crucial for the external auditor to perform some tests for him- or herself, e.g. to verify whether the right analyses were correctly performed, they can rely to a certain extent on internal audit work performed with process mining techniques. Cooperation between external and internal auditors can result in important advantages such as a higher coverage of both the audit universe and the actual testing and consequently a lower overall detection risk. Note that the mentioned coverage deals with both the sample size and the number of different tests. As process mining may enable the assessment of a full population of transactions, the expansion of coverage in this collaboration setting will primarily come from the latter option. Moreover, the available resources (both in terms of available auditors and knowledge) can be optimally allocated. Comparably, management monitoring and (internal) auditing activities can be complementary.

10.6. Future Work: Continuous Monitoring and Auditing

Traditionally, an important time-delay can be observed between the occurrence of important business events and the audit report due to the **periodic nature** of most monitoring and auditing models [5]. In the process mining based monitoring and audit models (introduced in section 8) this periodic nature and the related time-delay can also be observed. As a result of this delay, the **information contained in the management and audit report might become less useful or beneficial** for its user and therefore significantly affects his/her ability to make well-grounded business decisions [8].

Both continuous monitoring (implemented by management) and continuous auditing focus on reducing this time-delay by providing reporting/assurance **simultaneously with, or a short period of time after**, the occurrence of events related to the subject under investigation [17]. Consequently, continuous monitoring and auditing systems may unlock interesting opportunities; e.g. timely meeting regulatory requirements, promptly identifying irregularities or enhancing a stakeholder’s ability to make decisions.

Developing continuous auditing and monitoring models based on process mining can be interesting future work. The architectural methodology that could be used for implementing continuous auditing with process mining techniques is based on a **monitoring control layer** (MCL) [118]. The continuous monitoring or auditing component based on the MCL architecture would consist of adapted process mining techniques, which are using the event streams of the information system as main input [114]. Additionally, the continuous monitoring or auditing component could make use of the historic information recorded in the event log and all data available in the external data sources (e.g. human

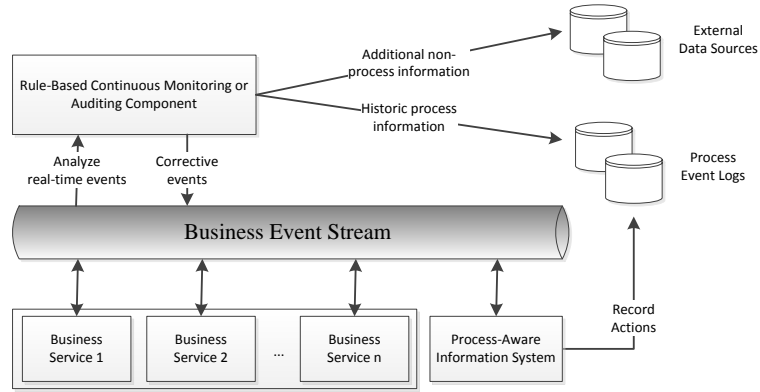


Figure 11: Continuous monitoring and auditing architecture

resources data or customer data). The architecture is schematically presented in figure 11. The main advantage of this architecture (in the auditing context) over its main rival the embedded audit modules (EAM) is its ability to operate independently of the information systems that it monitors. This architecture therefore allows the reinforcement of the separation of concerns between the management of an organization (responsible for the information system) and the auditor as presented in section 10.4.

11. Conclusion & Outlook

In this paper we proposed an applicability framework for process mining in the context of risk management and compliance checking. The framework aims at providing both the much needed business foundation for this subarea of process mining research and a clear guidance for future process mining projects in the control functions setting. Therefore we analyzed the different positions of three distinctive dimensions, i.e. process mining techniques, control functions and control function activities. We identified the process mining techniques that could add value to risk management and compliance checking. Improvements such as the conceptual advanced rule-based approach were presented.

Additionally, the scope for process mining in GRC was broadened beyond internal auditors. The control function dimension includes the management, the internal audit department, the external auditor and the audit committee as stakeholders that could benefit from process mining support in their GRC activities.

These GRC activities were grouped into three broad categories (risk identification & assessment, control activities and activities related to the generation and communication of information) which form the third dimension. Combining the three dimensions resulted in proposals for the effective use of process mining support to the control function activities.

Furthermore, an evaluation of the use of process mining for risk management and compliance checking activities has been provided. In conclusion, the use of process mining techniques in control functions supports different stakeholders in pursuing absolute assurance, in acquiring deep insights, in maintaining the required independence and in

improving the audit effectiveness and efficiency. While the potential added value might be clear, several technical challenges remain future research. Focus will be placed on the development of a continuous monitoring and auditing approach based on process mining techniques. Additionally, we will look for improvements of the existing process discovery and visualization techniques that allow for the construction of comprehensible models based on realistic characteristics of an event log.

Acknowledgements

We would like to thank the KU Leuven research council for financial support under grant OT/10/010: Business Process Mining: New Techniques and Evaluation Metrics and the Flemish research council for financial support under the Odysseus grant B.0915.09.

References

- [1] R. Agrawal, D. Gunopulos, and F. Leymann. Mining process models from workflow logs. *Advances in Database Technology EDBT'98*, pages 467–483, 1998.
- [2] R. Agrawal, C. Johnson, J. Kiernan, and F. Leymann. Taming compliance with sarbanes-oxley internal controls using database technology. In *Proceedings of the 22nd International Conference on Data Engineering*, pages 92–92. IEEE, 2006.
- [3] A. Alves de Medeiros, A. Weijters, and W. Van Der Aalst. Genetic process mining: a basic approach and its challenges. In *Business Process Management Workshops*, pages 203–215. Springer, 2006.
- [4] A.A. Arens, R.J. Elder, and M.S. Beasley. *Auditing and assurance services: An integrated approach*. Pearson Education, 2005.
- [5] International Auditing and Assurance Standards Board. *Handbook of international auditing, assurance, and ethics pronouncements*. International Federation of Accountants, 2010.
- [6] J. Bang-Jensen and G.Z. Gutin. *Digraphs: theory, algorithms and applications*. Springer Verlag, 2010.
- [7] Auditing Standards Board. Codification of auditing standards and procedures. Technical report, American Institute of Certified Public Accountants (AICPA), 1972.
- [8] ISACA Standards Board. Continuous auditing: Is it fantasy or reality? *Information Systems Control Journal*, 5, 2002.
- [9] C.E. Brown and I. Solomon. Auditor configural information processing in control risk assessment. *Auditing: A Journal of Practice and Theory*, 9(3):21–26, 1990.
- [10] F. Caron and J. Vanthienen. An exploratory approach to process lifecycle transitions from a paradigm-based perspective. *Enterprise, Business-Process and Information Systems Modeling*, pages 178–185, 2011.
- [11] F. Caron and J. Vanthienen. Applications of business process analytics and mining for internal control. *ISACA Journal*, 4:44, 2012.
- [12] F. Caron, J. Vanthienen, and B. Baesens. Comprehensive rule-based compliance checking and risk management with process mining. *Decision Support Systems*, Conditionally accepted.
- [13] F. Caron, J. Vanthienen, and B. Baesens. Rule-based business process mining: Applications for management. In *Management Intelligent Systems*, volume 171, pages 273–282, 2012.
- [14] F. Caron, J. Vanthienen, J. Weerdt, and B. Baesens. Advanced care-flow mining and analysis. In *Business Process Management Workshops*, pages 167–168. Springer, 2012.
- [15] F. Casati, S. Castano, M. Fugini, I. Mirbel, and B. Pernici. Using patterns to design rules in workflows. *IEEE Transactions on Software Engineering*, 26(8):760–785, 2000.
- [16] F. Chesani, P. Mello, M. Montali, F. Riguzzi, M. Sebastianis, and S. Storari. Checking compliance of execution traces to business rules. In *Business Process Management Workshops*, pages 134–145. Springer, 2009.
- [17] Wood Committee. Research report: continuous auditing. Technical report, Canadian Institute of Chartered Accountants & American Institute of Certified Public Accountants, 1999.
- [18] J.E. Cook and A.L. Wolf. Discovering models of software processes from event-based data. *ACM Transactions on Software Engineering and Methodology*, 7(3):215–249, 1998.

- [19] J.E. Cook and A.L. Wolf. Software process validation: quantitatively measuring the correspondence of a process to a model. *ACM Transactions on Software Engineering and Methodology*, 8(2):147–176, 1999.
- [20] COSO. Enterprise risk management - integrated framework. Technical report, Committee of Sponsoring Organizations of the Treadway Commission, 2004.
- [21] B. Curtis, M.I. Kellner, and J. Over. Process modeling. *Communications of the ACM*, 35(9):75–90, 1992.
- [22] G.S. Dallas. *Governance and Risk: an Analytical Handbook for Investors, Managers, directors, and stakeholders*. International Marine/Ragged Mountain Press, 2004.
- [23] H. de Beer. The LTL checker plugins: A reference manual. Technical report, Eindhoven University of Technology, 2004.
- [24] A.K.A. de Medeiros, W.M.P. van der Aalst, and C. Pedrinaci. Semantic process mining tools: core building blocks. In *16th European Conference on Information Systems*, pages 1953–1964. Citeseer, 2008.
- [25] A.K.A. de Medeiros, B.F. van Dongen, W.M.P. van der Aalst, and A. Weijters. Process mining: extending the α -algorithm to mine short loops. Technical report, Eindhoven University of Technology, 2004.
- [26] R.S. Debreceeny, G.L. Gray, J.J.J. Ng, K.S.P. Lee, and W.F. Yau. Embedded audit modules in enterprise resource planning systems: implementation and functionality. *Journal of Information Systems*, 19:7, 2005.
- [27] P.J. Denning. A new social contract for research. *Communications of the ACM*, 40(2):132–134, 1997.
- [28] Detection and Prevention of Fraud Task Force. Client acceptance and continuance procedures for audit clients, aicpa practice alert no. 94-3. Technical report, American Institute of Certified Public Accountants (AICPA), 1994.
- [29] R. Dijkman, M. Dumas, B. Van Dongen, R. Kaarik, and J. Mendling. Similarity of business process models: Metrics and evaluation. *Information Systems*, 36(2):498–516, 2011.
- [30] H.M. Ferreira and D.R. Ferreira. An integrated life cycle for workflow management based on learning and planning. *International Journal of Cooperative Information Systems*, 15(4):485–505, 2006.
- [31] The IIA Research Foundation. Information technology controls, global technology audit guide 3: Continuous auditing: Implications for assurance, monitoring, and risk assessment. Technical report, The Institute of Internal Auditors, 2005.
- [32] A. Ghose and G. Koliadis. Auditing business process compliance. *Service-Oriented Computing-ICSOC 2007*, pages 169–180, 2007.
- [33] C. Giblin, S. Müller, and B. Pfitzmann. From regulatory policies to event monitoring rules: Towards model driven compliance automation. *IBM Research Report. Zurich Research Laboratory*, 2006.
- [34] S. Goedertier, J. De Weerd, D. Martens, J. Vanthienen, and B. Baesens. Process discovery in event logs: An application in the telecom industry. *Applied Soft Computing*, 11(2):1697–1710, 2011.
- [35] S. Goedertier, D. Martens, J. Vanthienen, and B. Baesens. Robust process discovery with artificial negative events. *The Journal of Machine Learning Research*, 10:1305–1340, 2009.
- [36] S. Goedertier, C. Mues, and J. Vanthienen. Specifying process-aware access control rules in sbvr. *Advances in Rule Interchange and Applications*, pages 39–52, 2007.
- [37] S. Goedertier and J. Vanthienen. Compliant and flexible business processes with business rules. In *7th Workshop on Business Process Modeling, Development and Support (BPMDs'06) at CAiSE'06*, pages 94–104, 2006.
- [38] S. Goedertier and J. Vanthienen. Designing compliant business processes with obligations and permissions. In *Business Process Management Workshops*, pages 5–14. Springer, 2006.
- [39] G. Governatori and Z. Milosevic. Dealing with contract violations: formalism and domain specific language. In *Proceedings of the International Enterprise Distributed Object Computing Conference*, pages 47–57, 2005.
- [40] G. Governatori and S. Sadiq. The journey to business process compliance. *Handbook of Research on BPM*, pages 426–454, 2009.
- [41] S.M. Groomer and U.S. Murthy. Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems*, 3(2):53–70, 1989.
- [42] G. Guizzardi. Ontological foundations for structural conceptual models. 2005.
- [43] C. Gunther and W. van der Aalst. Fuzzy mining-adaptive process simplification based on multi-

- perspective metrics. *Business Process Management*, pages 328–343, 2007.
- [44] T. Halpin. Object-role modeling (ORM/NIAM). *Handbook on Architectures of Information Systems*, pages 81–103, 2006.
- [45] C. Harland, R. Brenchley, and H. Walker. Risk in supply networks. *Journal of Purchasing and Supply Management*, 9(2):51–62, 2003.
- [46] J. Herbst. A machine learning approach to workflow management. In *Proceedings of the 11th European Conference on Machine Learning*, pages 183–194. Springer, 2000.
- [47] A.R. Hevner, S.T. March, J. Park, and S. Ram. Design science in information systems research. *Mis Quarterly*, 28(1):75–105, 2004.
- [48] R. Hightower. *Internal controls, policies and procedures*. John Wiley & Sons Inc, 2008.
- [49] IIA. Position statement: The role of internal audit in enterprise-wide risk management. Technical report, The Institute of Internal Auditors, 2004.
- [50] J.E. Ingvaldsen and J.A. Gulla. Preprocessing support for large scale process mining of SAP transactions. In *Proceedings of the 2007 International Conference on Business Process Management*, pages 30–41. Springer, 2007.
- [51] Natovich J. Business process management systems: The internal control perspective. *ISACA Journal*, 2009.
- [52] R.P. Jagadeesh Chandra Bose and W.M.P. van der Aalst. Process diagnostics using trace alignment: opportunities, issues, and challenges. *Information Systems*, 2011.
- [53] M. Jans, N. Lybaert, and K. Vanhoof. Internal fraud risk reduction: Results of a data mining case study. *International Journal of Accounting Information Systems*, 11(1):17–41, 2010.
- [54] M. Jans, N. Lybaert, K. Vanhoof, and J.M. van der Werf. A business process mining application for internal transaction fraud mitigation. *Expert Systems with Applications*, 38(10):13351–13359, 2011.
- [55] G. Kassem and C. Rautenstrauch. Problem of tracing workflow instances in ERP-systems. In *International Business Information Management Conference*, pages 123–131, 2005.
- [56] M. Keegan. Audit committee handbook. Technical report, HM Treasury, 2007.
- [57] B. Kogut. “designing global strategies: profiting from operational flexibility”. *Readings in International Business*, The MIT Press, Cambridge, MA, pages 195–213, 1993.
- [58] J.R. Kuhn Jr and S.G. Sutton. Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems*, 24(1).
- [59] V. Kumar, R. Pollanen, and B. Maheshwari. Challenges in enhancing enterprise resource planning systems for compliance with sarbanes-oxley act and analogous canadian legislation. *Management Research News*, 31(10):758–773, 2008.
- [60] J.M. Küster, K. Ryndina, and H. Gall. Generation of business process models for object life cycle compliance. In *Proceedings of the 5th international conference on Business process management*, pages 165–181. Springer-Verlag, 2007.
- [61] K. Langfield-Smith. Management control systems and strategy: a critical review. *Accounting, organizations and society*, 22(2):207–232, 1997.
- [62] Y. Liu, S. Muller, and K. Xu. A static compliance-checking framework for business process models. *IBM Systems Journal*, 46(2):335–361, 2007.
- [63] E.M. Madigan, C. Petulich, and K. Motuk. The cost of non-compliance: when policies fail. In *Proceedings of the 32nd annual ACM SIGUCCS fall conference*, pages 47–51. ACM, 2004.
- [64] R.S. Mans, M.H. Schonenberg, M. Song, W.M.P. Aalst, and P.J.M. Bakker. Application of process mining in healthcare—a case study in a dutch hospital. *Biomedical Engineering Systems and Technologies*, 25:425–438.
- [65] J. Mendling, H.A. Reijers, and W.M.P. van der Aalst. Seven process modeling guidelines (7pmg). *Information and Software Technology*, 52(2):127–136, 2010.
- [66] J. Mendling, H.M.W. Verbeek, B.F. van Dongen, W.M.P. van der Aalst, and G. Neumann. Detection and prediction of errors in EPCs of the SAP reference model. *Data & Knowledge Engineering*, 64(1):312–329, 2008.
- [67] H. Mintzberg. *Structures in Fives: Designing Effective Organizations*. Prentice Hall, 1992.
- [68] M. Montali. Declarative process pining. *Specification and Verification of Declarative Open Interaction Models*, pages 343–365, 2010.
- [69] P.G. Moore. *The business of risk*. Cambridge University Press, 1983.
- [70] Association of Certified Fraud Examiners. Report to the nations on occupational fraud and abuse: 2012 global fraud study. Technical report, ACFE, 2012.
- [71] K. Peffers, T. Tuunanen, M.A. Rothenberger, and S. Chatterjee. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77,

- 2007.
- [72] M. Pesic. *Constrained-based workflow management systems: Shifting control to users*. PhD thesis, Eindhoven University of Technology, 2008.
 - [73] M. Pesic, M.H. Schonenberg, N. Sidorova, and W.M.P. Van Der Aalst. Constraint-based workflow models: Change made easy. In *Proceedings of the 2007 OTM Confederated international conference on the move to meaningful internet systems*, pages 77–94. Springer-Verlag, 2007.
 - [74] M. Pesic and W.M.P. van der Aalst. A declarative approach for flexible business processes management. In *Business Process Management Workshops*, pages 169–180. Springer, 2006.
 - [75] K.H.S. Pickett. *The internal auditing handbook*. Wiley, 2010.
 - [76] N. Pissinou, R.T. Snodgrass, R. Elmasri, I.S. Mumick, M.T. Ozsu, B. Pernici, A. Segef, B. Theodoulidis, and U. Dayal. Towards an infrastructure for temporal databases. *Sigmod Record*, 23(1):35–51, 1994.
 - [77] R. Prez-Castillo, B. Weber, J. Pinggera, S. Zugal, I. Garca-Rodrguez de Guzmán, and M. Piatini. Generating event logs from non-process-aware systems enabling business process mining. *Enterprise Information Systems*, 5(3):301–335, 2011.
 - [78] J. Recker, M. Rosemann, P. Green, and M. Indulska. Do ontological deficiencies in modeling grammars matter? *Management Information Systems Quarterly*, 35(1):57–79, 2011.
 - [79] M. Reichert and P. Dadam. Adept flexsupporting dynamic changes of workflows without losing control. *Journal of Intelligent Information Systems*, 10(2):93–129, 1998.
 - [80] R.G. Ross. *Principles of the business rule approach*. Addison-Wesley Professional, 2003.
 - [81] M. Rossi and M.K. Sein. Design research workshop: a proactive research approach. *Action Research*, 2005(01.02. 2004):1–20, 2003.
 - [82] A. Rozinat. *Process mining: conformance and extension*. PhD thesis, PhD thesis, Eindhoven University of Technology, Eindhoven, 2010.
 - [83] A. Rozinat and W.M.P. van der Aalst. Conformance testing: Measuring the fit and appropriateness of event logs and process models. In *Business Process Management Workshops*, pages 163–176. Springer, 2006.
 - [84] A. Rozinat and W.M.P. van der Aalst. Conformance checking of processes based on monitoring real behavior. *Information Systems*, 33(1):64–95, 2008.
 - [85] V. Rubin, C. Gunther, W.M.P. van der Aalst, E. Kindler, B. van Dongen, and W. Schafer. Process mining framework for software processes. *Software Process Dynamics and Agility*, pages 169–181, 2007.
 - [86] S. Sadiq, G. Governatori, and K. Namiri. Modeling control objectives for business process compliance. *Business Process Management*, pages 149–164, 2007.
 - [87] S.W. Sadiq, M.E. Orłowska, and W. Sadiq. Specification and validation of process constraints for flexible workflows. *Information Systems*, 30(5):349–378, 2005.
 - [88] J.R. Schermerhorn Jr. *Management*. Wiley, 2010.
 - [89] H. Schonenberg, R. Mans, N. Russell, N. Mulyar, and W. Aalst. Process flexibility: A survey of contemporary approaches. *Advances in Enterprise Engineering I*, 10:16–30, 2008.
 - [90] H. Schonenberg, R. Mans, N. Russell, N. Mulyar, and W.M.P. Van der Aalst. Towards a taxonomy of process flexibility. In *Proceedings of the CAiSE*, volume 8, pages 81–84, 2008.
 - [91] I.E.A. Segers. Investigating the application of process mining for auditing purposes. Master’s thesis, Technische Universiteit Eindhoven, 2007.
 - [92] H.A. Simon. *The sciences of the artificial*. the MIT Press, 1996.
 - [93] M. Song, C.W. Gunther, and W.M.P. Aalst. Trace clustering in process mining. In *Business Process Management Workshops*, pages 109–120. Springer, 2009.
 - [94] M. Song and W.M.P. van der Aalst. Towards comprehensive support for organizational mining. *Decision Support Systems*, 46(1):300–317, 2008.
 - [95] L.F. Spira and M. Page. Risk management: the reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4):640–661, 2003.
 - [96] S. Sutton, R. Young, and P. Mckenzie. An analysis of potential legal liability incurred through audit expert systems. *Intelligent Systems in Accounting, Finance and Management*, 4:191–204, 1994.
 - [97] Standards The Institute of Internal Auditors and Guidance. International standards for the professional practice of internal auditing (standards). Technical report, The Institute of Internal Auditors, 2010.
 - [98] D. Tschritzis. *The dynamics of innovation*. Copernicus Books, New York, 1998.
 - [99] C.J. Turner, A. Tiwari, R. Olaiya, and Y. Xu. Process mining: from theory to practice. *Business Process Management Journal*, 18(3):493–512, 2012.

- [100] W.M.P. van Aalst, K.M. Van Hee, J.M. van Werf, and M. Verdonk. Auditing 2.0: Using process mining to support tomorrow's auditor. *Computer*, 43(3):90–93, 2010.
- [101] W. Van der Aalst, T. Weijters, and L. Maruster. Workflow mining: Discovering process models from event logs. *IEEE Transactions on Knowledge and Data Engineering*, 16(9):1128–1142, 2004.
- [102] W.M.P. van der Aalst. Business alignment: Using process mining as a tool for delta analysis and conformance testing. *Requirements Engineering Journal*, 10(3):198–211, 2005.
- [103] W.M.P. van der Aalst. Process-aware information systems: Design, enactment, and analysis. *Wiley Encyclopedia of Computer Science and Engineering*. Wiley & Sons, Inc, 2008.
- [104] W.M.P. van der Aalst. *Process Mining*. Springer, 2011.
- [105] W.M.P. van der Aalst, H.T. De Beer, and B.F. van Dongen. Process mining and verification of properties: An approach based on temporal logic. *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE*, 3760/2005:130–147.
- [106] W.M.P. van der Aalst and C.W. Gunther. Finding structure in unstructured processes: The case for process mining. In *Proceedings of the 7th International Conference on Application of Concurrency to System Design*, pages 3–12. IEEE, 2007.
- [107] W.M.P. van der Aalst, H.A. Reijers, A.J.M.M. Weijters, B.F. van Dongen, A.K. Alves de Medeiros, M. Song, and H.M.W. Verbeek. Business process mining: An industrial application. *Information Systems*, 32(5):713–732, 2007.
- [108] W.M.P. Van der Aalst and M. Song. Mining social networks: Uncovering interaction patterns in business processes. *Business Process Management*, pages 244–260, 2004.
- [109] W.M.P. van Der Aalst, A.H.M. Ter Hofstede, B. Kiepuszewski, and A.P. Barros. Workflow patterns. *Distributed and parallel databases*, 14(1):5–51, 2003.
- [110] W.M.P. van der Aalst and B. Van Dongen. Discovering workflow performance models from timed logs. *Engineering and Deployment of Cooperative Information Systems*, 2480/2002:107–110.
- [111] W.M.P. van der Aalst, B. van Dongen, C. Gunther, R. Mans, A. de Medeiros, A. Rozinat, V. Rubin, M. Song, H. Verbeek, and A. Weijters. ProM 4.0: Comprehensive support for real process analysis. *Petri Nets and Other Models of Concurrency-ICATPN 2007*, pages 484–494, 2007.
- [112] W.M.P. Van der Aalst, B.F. Van Dongen, C. Gunther, A. Rozinat, H.M.W. Verbeek, and A. Weijters. ProM: the process mining toolkit. In *Proceedings of the International Conference on Business Process Management*, pages 1–4, 2009.
- [113] W.M.P. van der Aalst, B.F. van Dongen, J. Herbst, L. Maruster, G. Schimm, and A. Weijters. Workflow mining: a survey of issues and approaches. *Data & Knowledge Engineering*, 47(2):237–267, 2003.
- [114] W.M.P. van der Aalst, K. van Hee, J.M. van der Werf, A. Kumar, and M. Verdonk. Conceptual model for on line auditing. *Decision Support Systems*, 50, 2010.
- [115] W.M.P. van der Aalst and A. Weijters. Process mining: a research agenda. *Computers in Industry*, 53(3):231–244, 2004.
- [116] M. van Giessel and M.H. Jansen-Vullers. Process mining in sap r/3. *Master's thesis, Eindhoven University of Technology, Eindhoven*, 2004.
- [117] R. Van Gog and T.M. Van Engers. Modeling legislation using natural language processing. In *2001 IEEE International Conference on Systems, Man and Cybernetics*, volume 1, pages 561–566. IEEE, 2001.
- [118] M.A. Vasarhelyi, M.G. Alles, and A. Kogan. Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, 1(1):1–21, 2004.
- [119] G. Wagner. Rule modeling and markup. *Reasoning Web*, pages 251–274, 2005.
- [120] A. Weijters and JTS Ribeiro. Flexible heuristics miner (fhm). In *Computational Intelligence and Data Mining (CIDM), 2011 IEEE Symposium on*, pages 310–317. IEEE, 2011.
- [121] A. Weijters and W.M.P. van der Aalst. Rediscovering workflow models from event-based data using little thumb. *Integrated Computer Aided Engineering*, 10(2):151–162, 2003.
- [122] A. Weijters, W.M.P. van der Aalst, and A.K.A. de Medeiros. Process mining with the heuristics miner-algorithm. *Technische Universiteit Eindhoven, Tech. Rep. WP*, 166, 2006.
- [123] M. zur Muehlen and M. Rosemann. Workflow-based process monitoring and controlling? technical and organizational issues. In *Proceedings of the 33th Hawaii International Conference on System Sciences*, page 6032. Published by the IEEE Computer Society, 2000.
- [124] M. zur Muehlen and M. Rosemann. Integrating risks in business process models. In *Proceedings of 16th Australasian Conference on Information Systems*, 2005.