# Conceptualizing business process violations

Sebastian Dunzer[1,*], Annina Liessmann[1], Matthias Stierle[2] and Martin Matzner[1]

[1]Friedrich-Alexander-Universität Erlangen-Nürnberg, Fürther Str. 248, 90429 Nürnberg, Germany
[2]Datalane BV, Hoornwerk 1, 5264 PL Vught,The Netherlands

**Abstract**

Process analysts seek to gain insights into process execution to continuously improve their business processes. Business process deviation analysis can prove useful in identifying process improvements. However, differentiating between relevant and irrelevant deviations poses challenges. This is due to commercial process mining software flagging a high number of process instances as deviations from process definitions (e.g., process models). Against this background, we define and conceptualize business process violations that indicate undesired behavior. This paper defines business process violations based on regulatory business process compliance. Furthermore, this paper conveys a conceptual model connecting business process violations, the process definition they violate, and their organizational setting. We structure these components in ten dimensions of business process violations. The conceptual model and dimensions were developed and evaluated based on real-world examples provided by a German software vendor. Our conceptualization provides the vocabulary and raises awareness to discuss deviations' important aspects that delineate violations.

**Keywords**

business process deviations, business process violation, process analysis, conformance, compliance

## 1. Introduction

Organizations define and improve business processes to satisfy their customers' demands [1, 2]. Business processes can be defined formally—e.g., in process models [1], business rules [3]—and informally—e.g., in textual descriptions [4]. However, employees deviate from business processes in practice [5, 6]. Merit can be found in deviations in some cases [7, 8]. Employees discover improved methods of executing processes, or they react to a situation to achieve customer satisfaction [8, 9, 10]. However, if executions deviate from vital process requirements, harmful consequences can arise, including penalties and dissatisfied customers [6, 11]. Such deviations violate requirements spanning wider than an organization's process definition. Process requirements stem from within (e.g., operative requirements) and outside an organization (e.g., laws, regulations) [12, 13]. Organizations partly derive business process definitions from such requirements. As a consequence, process requirements are included implicitly in process definitions.

Checking process instances for their conformance to process definitions is one of the three constitutive types of process mining [14]. Surveys of process mining users and software providers identified transparency-related issues as a main incentive for using process mining [15]. Business process management (BPM) and process mining research has proposed an extensive arsenal of techniques, and tools for detecting deviations [7, 16, 17]. As conformance checking consultants, we believe that we as a community can develop a more effective toolbox by sharpening our fundamental concepts. The core problem with the status-quo is the techniques' focus on accurately detecting deviations between process data and models, whereas BPM practitioners are interested in problematic deviations [1, 6, 18]. We coin this type of deviation as violation. Conformance checking in companies frequently results in numerous deviations, as Section 2 shows. This is attributed to conformance checking, which assumes that process models encompass a complete business process. However, certain parts of processes may not be included

*PLC - Processes, Laws and Compliance workshop, in conjunction with ICPM 2024, October 14, 2024, Lyngby, Denmark*
*Corresponding author.
sebastian.dunzer@fau.de (S. Dunzer); annina.liessmann@fau.de (A. Liessmann); m.stierle@datalane.nl (M. Stierle); martin.matzner@fau.de (M. Matzner)
0000-0001-5229-1864 (S. Dunzer); 0000-0002-3542-0481 (A. Liessmann); 0000-0001-5938-1125 (M. Stierle); 0000-0001-5244-3928 (M. Matzner)

in the process models that are utilized. Process analysts are hardly supported in identifying violations among deviations. Therefore, academia and practice need a conceptual foundation to effectively identify violations. Accordingly, this paper proposes a conceptualization of business process violations (Section 4). We believe the demand for controlling process violations is a key practical driver for process analysis, especially, conformance checking, and it is far-fetched to consider every deviation a violation.

We conceptualize business process violations in this paper:

1. We extend the view on business process violations beyond process definitions towards their requirements to distinguish undesired from undefined behavior (Section 2). Rather than deviating from a process definition [19], a violation infringes a requirement.
2. Section 3 presents a concise overview of notions revolving around process deviations workarounds, anomalies, and non-compliance.
3. We define violations along the dimensions: definition level, requirement, execution, context, time, organization, dependency, restorability, awareness, and planned (Section 4).
4. We evaluate the definition and conceptual-model based on real-world examples provided by a German software vendor (Section 5).
5. We distinguish violations from terms used in related BPM-research streams (Section 6).

Additionally, we contribute to practice. Process owners and analysts can use the conceptualization to identify blind spots in their analyses, assess their capabilities regarding analysis, and find an entry point for process improvements. To outline its relevance, a motivating example from a practitioner's viewpoint shows difficulties which process analysts face when they assess deviations.

## 2. Motivating Example

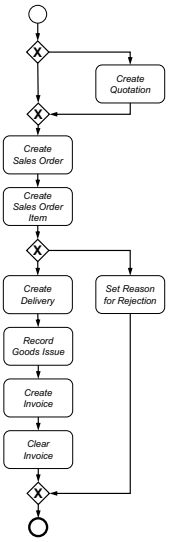
Process adherence is a topic that is naturally coming up in our discussions with industry about how to create value from process data. However, the understanding of process adherence differs a lot across different stakeholders and companies. Process adherence can be strictly conforming to a process model or executing a sequence of activities, not necessarily explicit in the process model, to achieve a process goal. For audits, compliance is the major focus to avoid fines and other liabilities.

This becomes apparent in process analysis projects. Commercial process mining software detects numerous deviations by comparing process definitions (i.e., process models or rules in natural language) with event data. However, once process experts are confronted with these deviations, they express no urgency to take actions regarding most deviations identified (e.g., "it should not be done like that, but it is not really a problem"). For some cases, the process definitions need to be fine-tuned, (e.g., "this can happen, but only in specific cases"). Defining all possible exceptions is a tedious, and to some extent, impossible task.

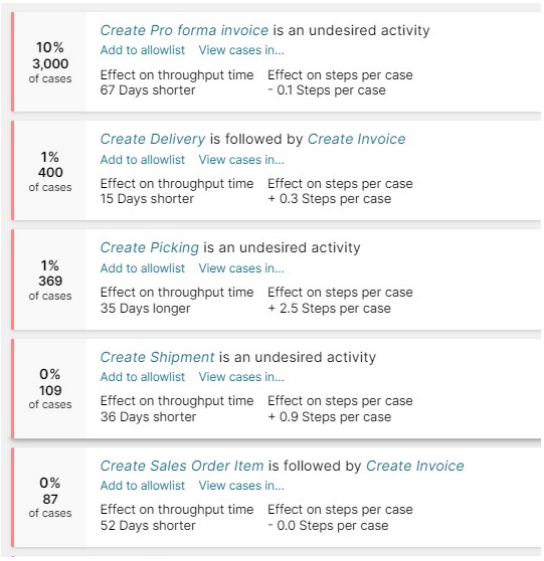
The following scenario illustrates this issue. Figure 1a shows a simplified BPMN model of a sales process. This model is compared against an *SAP* data set using *Celonis's* conformance checking software[1]. Figure 1b contains a part of the results (top five deviations).

The most common deviation in Figure 1b is the creation of a pro forma invoice. It is not represented in the BPMN model, but occurs if a customer requests it. Although creating a pro forma invoice leads to some effort, unwanted consequences do not arise. Another deviation is shown for creating a delivery after creating the invoice. A reason could be that a second delivery was created because of an incomplete first delivery. Likewise, customers may be invoiced before sending a delivery, either intended as payment in advance, or unintended as accounting is not aware that the goods have not been shipped. Consequently, it is difficult to assess if a deviation is a violation by looking at the BPMN model.

[1] www.celonis.com




(a) Exemplary business process model and notation (BPMN) model for a sales process.




(b) Results for conformance check with SAP data with BPMN model from Figure 1a.

**Figure 1:** Applying conformance checking in commercial process mining software.

# 3. Background

To establish a conceptual model for business process violations, literature on definitions and classifications of deviations and its associated concepts serves as a foundation. Moreover, we consider BPM-streams related to risk management, compliance, and non-compliance to constrict conceptualizing violations.

## 3.1. Deviations, Workarounds, and Anomalies

Conceptualizing violations in the context of business processes requires examining related concepts, such as deviations, workarounds, and anomalies. Therefore, we outline the definitions along with characteristics proposed in previous research.

Business process deviations are characterized as process behavior which differs from its process definition [19], such as process models [7, 20], business rules [3], and other definitions [21]. Process definitions tend to omit exceptions to keep process models concise [5]. Hence, deviating behavior is inevitable in real-world business processes because exceptions occur and workers depend on their freedom to react situationally [6, 19].

Workarounds are related to deviations in BPM [22]. They are described as "[...] deviations from defined business processes that are carried out in the employees' performances of routines in a work system" [22, p. 1]. Misusing information technology (IT) systems against their designed purpose constitutes the top-down perspective on workarounds. In contrast, the bottom-up perspective promotes workarounds as a source of innovation. Like deviations, workarounds can be considered a positive and negative phenomenon [23]. Workaround characterizations are composed of multi-perspective patterns including swapped activities, violated responsibilities, and manipulated data [8].

With the increasing adoption of process mining, the data-centric perspective on business processes gained importance. Anomalies in event logs represent deviations in real-world process executions from a data-centric perspective [24]. Research refers to anomalies if an observation of a process execution deviates from the *normal* observation [24]. Normal observations fulfill requirements regarding their frequency and compliance with a data generation process. Hence, anomalies can be noise (e.g., mistaken recording of an observation), data generation mistakes (e.g., wrong attribute column), and misbehavior [24]. Two anomaly-classification approaches can be differentiated—model-based and

data-based [7]. From the model-based perspective, a formal definition of anomalies includes the fitness between an appropriate process model and an event log [25]. The model-based perspective resembles process deviations by definition. In contrast, clustering-based and data-based approaches determine anomalies based on, for example, their likelihood [26]. Additionally, research yields patterns—e.g., skip, insert, rework—to characterize control-flow anomalies [27].

### 3.2. Compliance and Risk Management

Violations constitute undesired behavior, possibly breaking requirements spanning wider than an organization. Compliance and risk management in BPM are concerned with legal, regulatory and operational non-compliant behavior. Therefore, this stream of research contributes to conceptualizing violations by extending the view on risk mitigation and fraud prevention mechanisms.

Business process violations are typically associated with business process compliance—i.e., non-compliant behavior [11, 28]. The term violation originates from regulatory non-compliance. Compliance itself can be found in many facets, including legal compliance, regulatory compliance, and compliance with internal guidelines [29]. BPM research enlightens three perspectives to ensuring compliance in business processes: (1) design-time, (2) run-time and (3) auditing [30]. Additionally, management frameworks guide maintaining compliance in organizations [30]. Non-compliant practices incorporate several risks, including fraud and malicious damage [31]. Fraud can manifest in deviating and non-compliant behavior referring to a defined process. To qualify as fraud, employees deliberately act in a non-compliant manner intending to achieve personal or organizational benefits [32]. In the set of fraudulent behavior, process-based fraud can be identified using deviation-detection mechanisms [33]. Fraud detection and classifications search for patterns in data comprising, for example, control-flow, resources, time, and data [33].

Many laws, regulations, and other potential sources of non-compliance are known when designing business processes. Therefore, organizations implement mitigation strategies for violations to increase their business processes' resilience. Risk-aware business process models allow for counteracting violating process instances [34]. Whenever non-compliant behavior occurs during process executions, these models do not break. Instead, they mitigate emerging issues, or recover a compliant state [34]. This stream of literature indicates that non-compliant and harmful behavior can be planned for in process definitions.

## 4. Conceptualizing Business Process Violations

Against this background, we conceptualize business process violations, inspired by the terminologies revolving around deviations and compliance. Before we elaborate on the different dimensions and characteristics of business process violations, we define business process violations and propose a conceptual model.

### 4.1. Defining Business Process Violations

A *violation* is defined as "an action that breaks or acts against something, especially a law [...]" according to the *Cambridge Dictionary* [35]. This notion is akin to non-compliance in BPM [30]. To clarify, violations can be defined as undesired actions, behavior, and events that disrupt a process requirement, which can be part of a business process definition. Process definitions range from detailed procedural process models (e.g., pharmaceutical quality assurance) to unstructured textual instructions [21, 36, 37]. Process requirements originate from different sources including laws, regulatory agencies, internal guidelines. Organizations want to adhere to process requirements for different reasons [2]; for example, legal compliance [30], strategic alignment (e.g., cost leadership), governance (e.g., transparency), and operations [38].

To violate a process requirement, an agent (i.e., systems, workers, teams) performs prohibited behavior according to a process requirement while executing the related business process. An agent can be

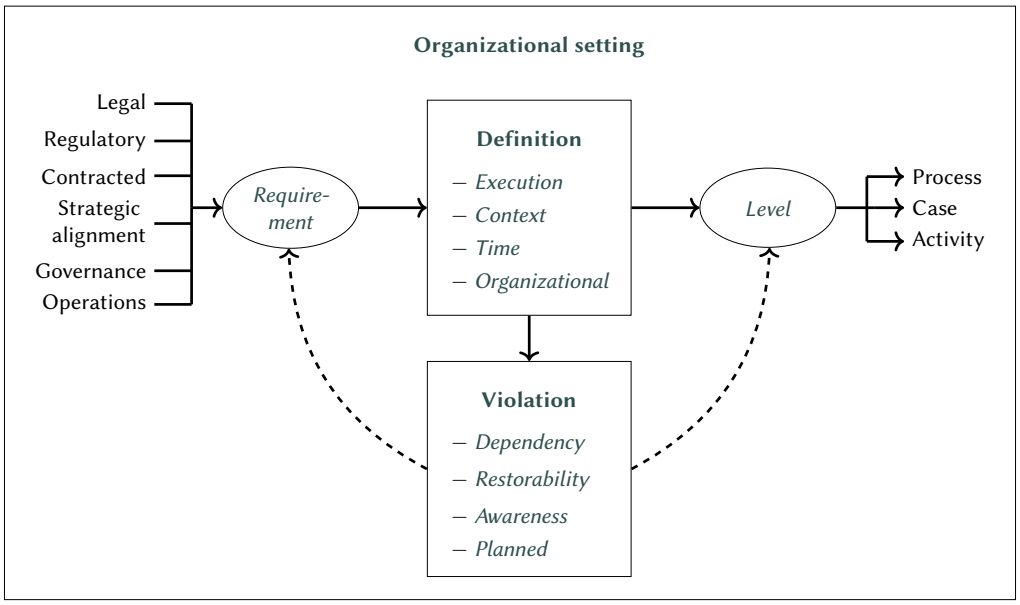



**Figure 2:** Conceptual model of business process violations.

aware or unaware of violating a process requirement [32, 33]. Consequently, a violation can be caused deliberately and accidentally [39]. Agents can instigate countermeasures to recover a process execution from a violation, whereby process definitions can provide mitigation strategies, or an agent works out countermeasures ad hoc [34]. Depending on their severity, violations can interrupt business process execution [40].

Three components describe a violation: (1) its organizational setting, (2) its process definition, and (3) its characteristics. Each of these components is characterized in different dimensions. Figure 2 depicts the resulting conceptual model of business process violations. Ten dimensions delineate a violation in total: The organizational setting of a violation comprises the process (1) *requirement* (e.g., legal requirements), and the definition (2) *level* (i.e., business process, case, activity). The context within which a violation occurs, both at the definition level and its requirement, can provide an indication of its severity. Process definitions preset the boundaries that agents must remain within during process execution. A process definition encompasses four dimensions to execute a business process: (3) it may regulate the control-flow of process *execution*, (4) stipulate *context* factors of executions, (5) define *time*-bound constraints, and (6) prescribe *organizational* duties and responsibilities. Four dimensions characterize a specific violation: (7) its *dependency* on previous events, (8) its *restorability*, (9) its causing agent's *awareness*, and (10) if it is *planned* for.

The relationships in the model arise from the nature of process requirements and definitions. Business process execution must adhere to requirements that account for an organization. These requirements can originate from within and outside an organization. They are embodied in a process definition that affects different levels of business process execution, ranging from business process to activity execution. Therefore, a violation affects the requirement and the definition level.

## 4.2. Organizational Setting

As depicted in the conceptual model (see Figure 2), a violation impacts the organizational setting regarding the *requirement* and definition *level*. Both dimensions and their respective characteristics are summarized in Table 1.

**Requirement.** The *requirement* dimension is related to a process definition's origin. Process definitions can stem from various internal and external requirements an organization has to, should, or can adhere to. A violation of a definition means in turn a violation of a requirement. This can be a legal,

**Table 1**
Organizational setting dimensions and respective characteristics' descriptions.

| Dim. | Characteristic | Description | Example |
|---|---|---|---|
| Requirement | Legal | The definition ensures compliance with rules and regulations governed and enforced by an authority. | GDPR compliance |
| | Regulatory | The definition is in place to comply with external standards that the organization decided to follow. | ISO 9001 |
| | Contracted | The definition is designed to meet contractual obligations an organization has with other entities. | Service-level agreement |
| | Strategic alignment | The definition is in place to ensure business processes are aligned to an organization's strategy. | Cost leadership |
| | Governance | The definition is in place to ensure adherence to internal guidelines. | Maverick buying |
| | Operations | The definition is in place to ensure that operations run efficiently. | Efficient resource utilization |
| Definition level | Process | A violation infringes a process definition designed for all cases. | Process model |
| | Case | A violation infringes a definition which accounts for specific cases. | Case condition |
| | Activity | A violation infringes work instructions given to perform a certain activity. | Work instruction |

regulatory or contractual obligation as well as an organization's strategic alignment, governance, and operations. A legal source implies following a binding set of rules and regulations, which are governed by an authority [13]. An organization has to abide these rules and regulations in all its operations. For example, the compliance with GDPR is a European regulation applying to all organizations that collect personal data in the European Union (EU). Violating GDPR can result in substantial fines. Next to legal sources, industry regulations (e.g., ISO) and standards can represent a set of requirements for process definitions. A violation of industry standards can lead to a certification suspension or withdrawal. An organization also has contractual obligations that it needs to fulfill, like service-level agreements. Additionally, organizations set requirements themselves concerning strategic alignment, governance, and operations. This entails requirements derived from a corporate strategy, internal guidelines, and operational procedures. These types of requirements, including reaching objectives such as minimizing costs, risk, and time or maximizing quality and flexibility, can be the source of a specification.

**Definition level.** Process definitions are designed based on process requirements and applicable to different *levels* [24, 33]. These levels can be considered as different perspectives of a requirement. On the process level, process definitions include process models and textual descriptions [41]. A violation of a specification on process level could be a sequence not represented in the process model and a sequence indicating an exception. Definitions on case level consider a subset of cases sharing specific characteristics. A violation of case-level definitions can be, for example, infringing specific requirements for a customer as part of the order-to-cash process. The last definition level is activity, including work instructions. Violations on the activity level can be, for example, the wrong resource performing the work, or the work itself being erroneous.

## 4.3. Process Definition

Next to the organizational setting, the process definition is broken down into four dimensions: *execution*, *context*, *time*, *organizational*. An execution agent should follow these definitions. Table 2 specifies the

**Table 2**
Process definition dimensions and respective characteristics' descriptions.

| Dim. | Characteristic | Description | Example |
|---|---|---|---|
| Execution | Precedence | An execution requires a specific preceding execution. | Mandatory sequence not followed |
| | Parallelism | An execution should (not) be parallelized. | Sequential instead of parallel execution |
| | Detour | An execution detours to a wrong path in a process. | Wrong decision leads to wrong sequence |
| | Insertion | An execution performs additional, unspecified actions. | Unspecified loops |
| | Absence | A required execution of an entity is not performed at all. | Execution missing |
| | Erroneous | The work conducted within an activity or case has errors. | Human mistake in execution |
| Context | Falsify context | An execution leads to an undesired change in context. | A supplier's address is copied into the delivery document instead of the buyer's address. |
| | Falsify execution | An undesired change in context leads to an incorrect execution. | An incorrect delivery document results in a delivery to a wrong address. |
| Time | Duration | An execution has to be completed in a specified period. | Assembling a product takes longer than specified. |
| | Delay | An execution has to pause for some time. | After coating a product, the product needs to cure for two hours. |
| | Deadline | An execution has to be completed at a specific time. | A service request must be answered within five business days. |
| | Point in time | An execution has to be completed at a specific point in time. | A delivery should take place at a specified delivery date. |
| Organizational | Wrong resource | An agent cannot perform the execution. | An agent lacks the permission to place an order. |
| | Wrong duty | An agent could perform the execution, but should not. | Four-eyes principle performed by a single agent. |

dimensions and their characteristics with an example.

**Execution.** The *execution* dimension comprises all characteristics of violations related to the sequence of steps to implement the definition [27, 28]. First, the definition requires an execution sequence of entities, that is, precedence. For example, a product needs to be packaged before it is sent to the customer. Second, the indeterminate absence (or existence) of parallelism in an execution can violate a definition. Although two entities should be performed in parallel, they are not, potentially increasing execution time. Third, triggering a wrong path after evaluating a condition incorrectly is a detour violation. Fourth, an entity might be repeated unnecessarily, or other unspecified entities are performed. The insertion of such entities violates a definition. Fifth, an entity specified can be absent from an execution (e.g., a missing activity). The last definition violation in the execution dimensions concerns the specific steps within an entity. Errors and mistakes lead to wrong outcomes of an entity, such as saving a document in a wrong location.

**Context.** Besides the implementation of steps, a definition can include details on process, case, and activity context [33]. Context refers to additional data that is required to execute a process. Wrong context (input) can either lead to an incorrect execution or can be the result of an incorrect execution (output). For example, while creating a delivery document, the addresses of the buyer and supplier are mixed up and copied incorrectly, falsifying the context. The erroneous document as input of the next activity results in a delivery to the wrong address. This falsifies the execution.

**Time.** Another dimension of the process definition is *time* [8, 24, 33]. A time violation can occur in terms of duration, deadline, point in time, and delay. A duration violation is committed once a specified period has passed without completing the execution. On an activity level, this means that the work instructions are not finished within a timeframe, for example, the assembly of a product. In contrast to duration, a delay imposes a requirement on the minimum idle time. A freshly coated product might need a certain time to cure. Deadline and point in time violations both relate to a date, which can be specified dynamically during execution. While a deadline signifies the time an execution must be completed at the latest, a point in time refers to a time-frame in which the execution must take place or finish. For example, a service request should be answered within five business days is a dynamically created deadline. However, the delivery of a product at a specified delivery date is a point in time. Delivering too early or too late is both considered a violation of a point in time definition.

**Organizational.** Process definitions can include requirements for *organizational* aspects [33]. The organizational dimension can be structured into three characteristics. A violation occurs if the executing agent cannot execute the definition or if he can, but should not, execute the definition. In the former case, wrong resource, the agent might not have the required permission, for example in an IT system. In the latter case, the executing agent might have the required permissions; however, there are other duty-specific requirements in the definition to be respected. For example, two different agents need to be involved in the execution.

## 4.4. Violation

A violation can be described along the dimensions: *dependency*, *restorability*, *awareness*, and *planned*. Table 3 summarizes the characteristics belonging to these dimensions and provides examples to explain each characteristic.

**Dependency** The *dependency* dimension relates to the procedural circumstances related to a violation. Violations can be independent, dependent on another execution, or interdependent on executions outside its organization. Independent violations arise when human errors are involved; for instance, mistyping bank account details in a form. Whenever there is an error in how to perform an activity and the required data is available, a violation occurs independently. Dependent violations occur when static case conditions within an organization are triggered during the execution of a process. For example, after a customer has placed an order, the customer should receive the delivery within the next three business days, but the organization misses this date. Interdependent violations relate to executions which are executed outside the organization. For instance, a customer sets a desired delivery date later than at the order placement. Hence, it is not known before the customer triggered a change in the case context. If the organization delivers earlier or later, a violation occurred interdependently.

**Restorability.** The second dimension related to business process violations is their *restorability*. Violations can be recoverable, repairable, or irreparable. A recoverable violation can be neutralized by taking appropriate countermeasures; for example, a cancelled duplicated order. In contrast, countermeasures cannot mitigate the effects of an irreparable violation on a business process execution. For instance, a worker sends sensitive customer data to a wrong recipient—i.e. a GDPR infringement. Once the data is underway, the damage has occurred and cannot be fixed. In between irreparable and recoverable violations, there are violations whose effects can be mitigated at a certain cost. A missing order of supplies for a production process can still be placed. However, by that time, the production of a good may be delayed, leading to contractual penalties, dissatisfied customers and production rescheduling.

**Awareness.** A violation's *awareness* characteristic differentiates between harmful intention and accidental behavior resulting in violations [32]. If an executing agent is aware of violating a process requirement and violates it deliberately, this can be an indicator for fraud. In such cases, execution agents may or may not strive for personal or organizational benefits by violating a binding process requirement. Unaware violations can occur because process definitions to follow might be unenforced, unknown, or unclear to executing agents. In response, the agents might have established routines ignoring the definition [9, 23].

**Table 3**
Violation dimensions and respective characteristics' descriptions.

| Dim. | Characteristic | Description | Example |
|---|---|---|---|
| Dependency | Independent | A violation occurs independently of any other execution. | An employee enters incorrect bank account information in a form. |
| | Dependent | A violation is linked to another execution within the organization. | An employee receives and enters incorrect bank account information of a customer from another department. |
| | Interdependent | A violation is linked to external interdependencies. | A customer changes payment details and the change is not considered in imminent direct debits. |
| Restorability | Recoverable | A violation's effects can be undone by instigating countermeasures. | An employee places a purchase order with the wrong quantity of an item, but can still change it by contacting the supplier. |
| | Repairable | A violation's effects can be mitigated by instigating countermeasures. | A purchase order has not been placed in time and can still be placed at the cost of a delayed delivery to a customer, including fines. |
| | Irreparable | A violation's effects cannot be undone. | An employee reveals customer data to a third party. |
| Awareness | Aware | An agent is aware of violating a process definition. | An employee wants to disclose information and chooses to send it to the wrong recipient deliberately. |
| | Unaware | An agent is unaware of violating a process definition. | An employee does not know that the recipient address of an e-mail is wrong. |
| Planned | Planned | A violation is part of a process definition. | A process definition contains risk mitigation scenarios. |
| | Unplanned | A violation is not part of a process definition. | A process model only contains the desired path. |

**Planned.** Lastly, violations can be *planned* for in process definitions to handle their potential consequences [34]. Planned violations are exceptions from the desired behavior which are explicitly incorporated in a process definition. If they occur, escalation or mitigation procedures are in place. On the contrary, unplanned violations are not accounted for in a process definition. Such violations represent deviations from a process model [7].

## 5. Evaluation

After having outlined the definition, conceptual model, and characteristics of violations, we demonstrate the suitability of this conceptualization based on real-world examples of violations and other types of deviations. We evaluated the definition and characteristics of violations in collaboration with the German software company *MonCorp*[2]. The company operates in the area of IT monitoring and employs 300 workers. *MonCorp* has a dedicated BPM department. One of their business process managers, who held the position for five years, helped to develop and evaluate the violation definition and characteristics. She provided 20 real-world process requirements, reported potential violations, and participated in discussions. The provided process requirements and violations originate from different organizational functions, including accounting, finance, IT, and sales. Following on from our motivating example (cf. Section 2), we elaborate on three real-life requirements and violations regarding the order-to-cash (O2C) process in accounting.

[2]The company's name is altered due to confidentiality.

*MonCorp* provided examples that deviate from process definitions, but do not constitute violations. To obtain a tax exemption as a US-based customer for purchasing *MonCorp's* services, an exemption certificate must be available before issuing an invoice; otherwise the customer has to pay the taxes. In the best-case scenario, the certificate is available before issuing an invoice to the customer. However, in some cases, the certificate is unavailable at the time of the order. If the certificate is received later and needs to be added to an invoice, *MonCorp's* team reimburses the original invoice and creates another invoice for the customer without taxes. While this procedure takes more time and infringes the process's definition, the company considers this a workaround rather than a violation. Customers may not have the certificate available, but service delivery is required. In these cases, although not in the process definition, this represents a desired behavior to still achieve customer satisfaction. Thus, it does not fulfill the criteria to qualify as a violation. The second example originates from the legal environment. If a country is internationally embargoed (e.g., by the European Union), no goods and services may be delivered there and invoices may not be issued. However, when an aid organization operating in an *embargoed* country requested one of *MonCorp's* services, it had to be delivered and an invoice needed to be created. The company considers this a deviation and perhaps a workaround, but not a violation. The actions complied with the legal requirements, however, infringed the process definition since system constraints were bypassed to allow for service delivery and invoice creation.

The first violated O2C process requirement concerns charging value-added taxes on invoices. If a European customer has provided their value-added tax (VAT) ID, it has to be added to the customer's profile. The automatic invoice creation without a VAT ID entry leads to wrongly created invoices, rescinded transactions and a restart of the process. *MonCorp* considers forgetting to enter a VAT ID in cases where the customer is European as a violation. This violation is characterized by the dimensions *definition level* (case), *requirement* (legal), *execution* (absence), *context* (falsify context), *dependency* (independent), *restorability* (repairable), *awareness* (unaware), and *planned* (planned).

The second legal requirement regarding invoicing is that the delivery and invoice date match. A typical violation provided by *MonCorp* is redating an invoice which deviates from a process-level definition. This becomes problematic in audits and can lead to fines. This violation is characterized in the dimensions *definition level* (process), *requirement* (legal), *execution* (erroneous), *context* (falsify context), *dependency* (dependent), *restorability* (irreparable), *awareness* (aware), and *planned* (unplanned).

Third, partners can achieve certain partner levels. Depending on the level, partners can redeem discounts and are invited to *MonCorp's* events and fares. The company provided an example of a violation, where customers received multiple partner levels. As consequences, these customers were invited to events where their partner level was insufficient, and they were granted additional discounts resulting in high losses because of their added up partner level. This violation is characterized by the following dimensions: *definition level* (case), *requirement* (operations), *execution* (insertion), *context* (falsify execution), *dependency* (interdependent), *restorability* (repairable), *awareness* (unaware), and *planned* (unplanned).

As shown, the conceptual model and characteristics of violations help to classify violations. In addition, the characterization allows for deriving countermeasures for certain violations. If a violation occurs multiple times, *MonCorp* may reconfigure their systems based on the characterization. For example, *MonCorp* could automatically check for duplicate entries in partner levels. Furthermore, the business process manager stated that the conceptual model and characteristics raise the awareness of those aspects that influence and delineate violations.

## 6. Discussion

Following our definition and characteristics of business process violations, the question, if they are a foundational concept of BPM, remains open. After distinguishing violations conceptually from deviations and other related concepts, we outline our contributions and future research opportunities.

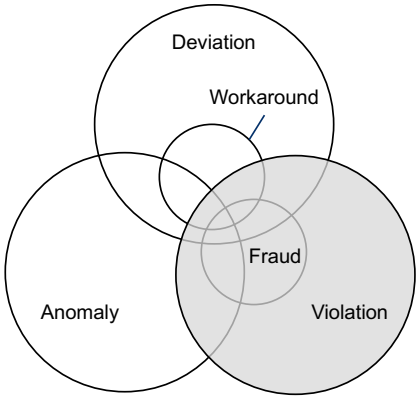



**Figure 3:** Relation between violation, fraud, deviation, workaround, and anomaly.

## 6.1. Distinguishing Violations

Violations are closely related to the notions of deviations, workarounds, anomalies, and fraud. Additionally, the term itself arises from non-compliance regarding regulatory compliance. Approaches to determine deviations from a process definition can be characterized as model-based approaches [7]. These approaches find deviations by comparing normative or descriptive behavior encoded in a process definition with process executions [18]. In contrast to violations, deviations solely represent behavior not accounted for in the process definition, without considering whether the behavior is desired or undesired. Workarounds are a subset of deviations, carried out as an employee's work routine [22] and are not defined as part of the process. They can be considered negative or positive [9]. A workaround can be a violation if it represents an undesired action or behavior infringing a process requirement. However, a workaround can in turn also facilitate a process requirement (i.e., desired behavior).

Approaches to determine anomalies, cluster-based approaches, assume a data-centric perspective by detecting anomalies in process execution data [7]. An anomaly fails to meet specific characteristics in terms of frequency, or does not fit a probability distribution [24]. Even though the behavior is infrequent, it might not necessarily be undesired or violating a process requirement.

Violation and fraud both place emphasis on undesired behavior in process executions. Undesired behavior can stem from violating laws, rules, regulations, and organizational policies [35, 42]. This undesired behavior might not be explicitly reflected in process definitions. While fraud violates the process definition, it can be characterized as a deliberate act intended to obtain a benefit [33]. Since fraud always involves undesired behavior, all kinds of fraud can be considered a violation. On the contrary, not all violations are frauds.

The various relations between deviation, workaround, anomaly, fraud, and violation are depicted in Figure 3. Based on this distinction, it becomes clear, that violations are not necessarily deviations, workarounds, or anomalies. This should be considered when designing systems to check for violations.

## 6.2. Contributions and Future Research

We set out to investigate the difference between relevant and irrelevant deviations in process analysis projects in practice. Commercial analysis methods reveal numerous deviations and aggravate finding relevant deviations. Soon it became apparent, that deviating from foundational process requirements derived from, for instance, operative or strategic objectives, determine a deviation's relevance for further examination. In business process compliance, non-compliant behavior is referred to as violations. We argue for expanding violations beyond regulatory compliance, also taking requirements stemming from operations, corporate strategy and governance into account. This notion allows for conceptualizing what practice is searching for, when they analyze their processes using deviation detection methods (e.g., conformance checking):

1. We define business process violations as undesired actions, behavior, or events infringing a

process requirement which may or may not be part of a process definition (e.g., process model).
2. We provide and evaluate a conceptual model linking the three components organizational setting, process definitions, and violations to conceptualize the latter. We describe these components in ten dimensions: definition level, requirement, execution, context, time, organization, dependency, restorability, awareness, and planned.
3. We differentiate violations from deviations, workarounds, anomalies, and fraud.

Our conceptualization of violations opens up opportunities for future research. The conceptual model and its dimensions call for further empirical validation. The model could further be refined and extended based on resulting insights. An opportunity for future research arises from the link between process requirements and process definitions. Another type of empirical research design could scrutinize to what extent process definitions in practice include process requirements derived from different sources. Design-time compliance research can provide initial reference points on quantifying this relationship in field and case studies [30, 31]. Furthermore, to assist process analysts in determining the relevant deviations, an algorithmic research setup could develop a violation relevance metric.

## 7. Conclusion

This paper originates in the different understanding of business process deviations in practice and academia. Practitioners require insights into problematic process execution. Current commercial methods, tools, and techniques, however, identify numerous and mostly irrelevant deviations. Instead, practitioners strive to identify and eliminate problematic deviations, breaking operative or legal requirements. In contrast, research defines deviations as behavior, which is not expressed within a process definition. A multitude of techniques, methods, and algorithms are concerned with identifying deviations. Such deviations can be very useful when organizations want to detail and refine their process definitions. However, most deviation analysis projects focus on identifying potential candidates for process improvements. A look into BPM research reveals an eclectic number of concepts related to deviations—i.e. anomalies, workarounds, compliance, and risk. Consolidating these different streams into business process violations resembles what organizations are searching for when they analyze deviations using industry-standard conformance checking. Business process violations represent undesired actions, behavior, or events that can be characterized in different dimensions. We pledge for process analysis and mining that incorporates the connection between process definitions, their requirements and the violating process executions.

## References


[1] W. Van der Aalst, Business process management: a comprehensive survey, International Scholarly Research Notices 2013 (2013).

[2] M. Indulska, P. Green, J. Recker, M. Rosemann, Business process modeling: Perceived benefits, in: Conceptual Modeling-ER 2009: 28th International Conference on Conceptual Modeling, Gramado, Brazil, November 9-12, 2009. Proceedings 28, Springer, 2009, pp. 458–471.

[3] K. Kluza, G. J. Nalepa, A method for generation and design of business processes with business rules, Information and Software Technology 91 (2017) 123–141.

[4] J. Sànchez-Ferreres, A. Burattin, J. Carmona, M. Montali, L. Padró, L. Quishpi, Unleashing textual descriptions of business processes, Software and Systems Modeling 20 (2021) 2131–2153.

[5] J. Swinnen, B. Depaire, M. J. Jans, K. Vanhoof, A Process Deviation Analysis – A Case Study, in: F. Daniel, K. Barkaoui, S. Dustdar (Eds.), Business Process Management Workshops, volume 99, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 87–98.

[6] M. Jans, M. G. Alles, M. A. Vasarhelyi, A field study on the use of process mining of event logs as an analytical procedure in auditing, The Accounting Review 89 (2014) 1751–1773.

[7] G. Li, W. Van der Aalst, A framework for detecting deviations in complex event logs, Intelligent Data Analysis 21 (2017) 759–779.

[8] S. Weinzierl, V. Wolf, T. Pauli, D. Beverungen, M. Matzner, Detecting temporal workarounds in business processes–a deep-learning-based method for analysing event log data, Journal of Business Analytics 5 (2022) 76–100.
[9] S. Alter, A workaround design system for anticipating, designing, and/or preventing workarounds, in: International Workshop on Business Process Modeling, Development and Support, Springer, 2015, pp. 489–498.
[10] S. Alter, Theory of workarounds, Communications of the Association for Information Systems 34 (2014) 55.
[11] A. Awad, M. Weske, Visualization of compliance violation in business process models, in: S. Rinderle-Ma, S. Sadiq, F. Leymann (Eds.), Business Process Management Workshops, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 182–193.
[12] M. Rosemann, J. Recker, C. Flender, Contextualisation of business processes, International Journal of Business Process Integration and Management 3 (2008) 47–60.
[13] S. Höhenberger, D. M. Riehle, P. Delfmann, From legislation to potential compliance violations in business processes-simplicity matters., in: ECIS, 2016, p. ResearchPaper188.
[14] W. Van der Aalst, A. Adriansyah, A. K. A. De Medeiros, F. Arcieri, T. Baier, T. Blickle, J. C. Bose, P. Van Den Brand, R. Brandtjen, J. Buijs, et al., Process mining manifesto, in: Business Process Management Workshops: BPM 2011 International Workshops, Clermont-Ferrand, France, August 29, 2011, Revised Selected Papers, Part I 9, Springer, 2012, pp. 169–194.
[15] Deloitte, Delivering Value with Process Analytics | Process mining adoption and success factors, Technical Report, Deloitte, 2021. URL: https://www2.deloitte.com/de/de/pages/finance/articles/global-process-mining-survey-2021.html.
[16] P. Felli, A. Gianola, M. Montali, A. Rivkin, S. Winkler, Cocomot: conformance checking of multi-perspective processes via smt, in: Business Process Management: 19th International Conference, BPM 2021, Rome, Italy, September 06–10, 2021, Proceedings 19, Springer, 2021, pp. 217–234.
[17] S. Weinzierl, S. Zilker, S. Dunzer, M. Matzner, Machine learning in business process management: A systematic literature review, Expert Systems with Applications (2024) 124181.
[18] S. Dunzer, M. Stierle, M. Matzner, S. Baier, Conformance checking: a state-of-the-art literature review, in: Proceedings of the 11th international conference on subject-oriented business process management, 2019, pp. 1–10.
[19] M. Monashev, M. Krčál, J. Mendling, Deviation from Standards and Performance in Knowledge-Intensive Processes: Evidence from the Process of Selling Customized IT Solutions, in: C. Di Francescomarino, A. Burattin, C. Janiesch, S. Sadiq (Eds.), Business Process Management, Lecture Notes in Computer Science, Springer Nature Switzerland, Cham, 2023, pp. 430–446.
[20] M. A. Ellatif, E. M. Shaaban, M. A. Amin, Detecting Deviations in Business Processes Using Process Mining, in: 2019 14th International Conference on Computer Engineering and Systems (ICCES), IEEE, Cairo, Egypt, 2019, pp. 49–54.
[21] A. Ottensooser, A. Fekete, H. A. Reijers, J. Mendling, C. Menictas, Making sense of business process descriptions: An experimental comparison of graphical and textual notations, Journal of Systems and Software 85 (2012) 596–606.
[22] V. Wolf, D. Beverungen, Conceptualizing the impact of workarounds–an organizational routines' perspective, in: Proceedings of the 27th European Conference on Information Systems (ECIS), 2019, pp. 1–12.
[23] N. Röder, M. Wiesche, M. Schermann, H. Krcmar, Toward an ontology of workarounds: A literature review on existing concepts, in: 2016 49th Hawaii international conference on system sciences (HICSS), IEEE, 2016, pp. 5177–5186.
[24] J. Ko, M. Comuzzi, A Systematic Review of Anomaly Detection for Business Process Event Logs, Business & Information Systems Engineering 65 (2023) 441–462.
[25] F. Bezerra, J. Wainer, W. Van der Aalst, Anomaly Detection Using Process Mining, in: T. Halpin, J. Krogstie, S. Nurcan, E. Proper, R. Schmidt, P. Soffer, R. Ukor (Eds.), Enterprise, Business-Process and Information Systems Modeling, volume 29, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, pp. 149–161.

[26] K. Böhmer, S. Rinderle-Ma, Multi-perspective Anomaly Detection in Business Process Execution Events, in: C. Debruyne, H. Panetto, R. Meersman, T. Dillon, E. Kühn, D. O'Sullivan, C. A. Ardagna (Eds.), On the Move to Meaningful Internet Systems: OTM 2016 Conferences, volume 10033, Springer International Publishing, Cham, 2016, pp. 80–98.
[27] T. Nolle, S. Luettgen, A. Seeliger, M. Mühlhäuser, BINet: Multi-perspective business process anomaly classification, Information Systems 103 (2022).
[28] M. Weidlich, H. Ziekow, J. Mendling, O. Günther, M. Weske, N. Desai, Event-Based Monitoring of Process Execution Violations, 2011.
[29] D. Schumm, F. Leymann, Z. Ma, T. Scheibler, S. Strauch, Integrating Compliance into Business Processes, in: Multikonferenz Wirtschaftsinformatik, volume 2010, 2010, p. 421.
[30] M. Hashmi, G. Governatori, H.-P. Lam, M. T. Wynn, Are we done with business process compliance: state of the art and challenges ahead, Knowledge and Information Systems 57 (2018) 79–133.
[31] R. Lu, S. Sadiq, G. Governatori, Measurement of Compliance Distance in Business Processes, Information Systems Management 25 (2008) 344–355. doi:10.1080/10580530802384613.
[32] M. Jans, J. M. Van Der Werf, N. Lybaert, K. Vanhoof, A business process mining application for internal transaction fraud mitigation, Expert Systems with Applications 38 (2011) 13351–13359.
[33] B. Omair, A. Alturki, Taxonomy of Fraud Detection Metrics for Business Processes, IEEE Access 8 (2020) 71364–71377.
[34] S. Suriadi, B. Weiß, A. Winkelmann, A. H. ter Hofstede, M. Adams, R. Conforti, C. Fidge, M. La Rosa, C. Ouyang, A. Pika, et al., Current research in risk-aware business process management—overview, comparison, and gap analysis, Communications of the Association for Information Systems 34 (2014) 52.
[35] C. Dictionary, Violation, 2024. URL: https://dictionary.cambridge.org/dictionary/english/violation.
[36] L. Quishpi, J. Carmona, L. Padró, Extracting Annotations from Textual Descriptions of Processes, in: D. Fahland, C. Ghidini, J. Becker, M. Dumas (Eds.), Business Process Management, volume 12168, Springer International Publishing, Cham, 2020, pp. 184–201.
[37] H. Van Der Aa, H. Leopold, H. A. Reijers, Dealing with Behavioral Ambiguity in Textual Process Descriptions, in: M. La Rosa, P. Loos, O. Pastor (Eds.), Business Process Management, volume 9850, Springer International Publishing, Cham, 2016, pp. 271–288.
[38] M. Rosemann, T. De Bruin, Towards a business process management maturity model, in: ECIS 2005 proceedings of the thirteenth European conference on information systems, Verlag and the London School of Economics, 2005, pp. 1–12.
[39] N. Van Beest, H. Groefsema, A. Cryer, G. Governatori, S. C. Tosatto, H. Burke, Cross-instance regulatory compliance checking of business process event logs, IEEE Transactions on Software Engineering (2023).
[40] S. Bassil, S. Rinderle, R. Keller, P. Kropf, M. Reichert, Preserving the context of interrupted business process activities, in: Enterprise Information Systems VII, Springer, 2006, pp. 149–156.
[41] L. Nake, S. Kuehnel, L. Bauer, S. Sackmann, Towards identifying gdpr-critical tasks in textual business process descriptions, in: INFORMATIK 2023 - Designing Futures: Zukünfte gestalten, Gesellschaft für Informatik e.V., Bonn, 2023, pp. 1895–1908.
[42] A. Elgammal, O. Turetken, W.-J. Van Den Heuvel, M. Papazoglou, Root-Cause Analysis of Design-Time Compliance Violations on the Basis of Property Patterns, in: P. P. Maglio, M. Weske, J. Yang, M. Fantinato (Eds.), Service-Oriented Computing, volume 6470, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 17–31.