

Dimensions of Accountability in Inter-organizational Business Processes

Matthias Buchinger
fortiss GmbH
buchinger@fortiss.org

Peter Kuhn
fortiss GmbH
pkuhn@fortiss.org

Dian Balta
fortiss GmbH
balta@fortiss.org

Abstract

Inter-organizational business processes are the basis of a globalized, highly dynamic, and digitalized world, enabling faster and cost-effective transactions. At the same time, they raise business vulnerabilities. A particular vulnerability is linked to the substantiation of trust between actors in dynamic business relationships, as trust affects interdependencies and complexity. An approach to address this vulnerability is the introduction of accountability mechanisms. Extant research suggests that accountability enables revealing causality and a transparent allocation of responsibilities for each process step. Thereby, corresponding actors can judge upon misbehavior and verify trust claims. Unfortunately, a thorough understanding of accountability and its dimensions accountability in the context of IBP is still missing. To address this gap, we develop a framework with dimensions of accountability. We demonstrate the resulting framework in an industrial supply chain case and derive implications for theory and practice.

1. Introduction

Globalization, digitalization, and the growing need for efficiency and effectiveness in established collaborative production and business structures drive a profound change. This change occurs in the dynamics of how activities are performed in organizations and how organizations interact with each other [1, 2]. In this context, an inter-organizational view on business processes gains increasing importance [3, 4].

Inter-organizational business processes (IBP) depict the creation process of value in products or services through the involved organizations. IBP can be defined as “an organized group of joined activities carried out by two or more organizations to achieve a common business objective” [3]. They enable companies to transact faster and more cost-effectively while achieving better quality [5].

At the same time, an IBP can be fragile and lead to business vulnerabilities [6], as several hazards show, for example in the food industry [7].

A constituent factor influencing the increase of vulnerabilities is that an IBP is often dependent on **trust** in dynamic business relations between different actors [8]. Typically, a long-term business relationship and the right economic circumstances are needed to establish trust [9]. Since relationships in IBP are increasingly short-term, this poses a challenge for the actors in an IBP to continue collaboration despite a mutual lack of trust [8].

A potential approach to tackling trust’s challenge towards minimizing vulnerabilities is based on **accountability** [10]. Accountability enables “the uncovering of causes for events and helps understand who or what is responsible for these events” [11]. By increasing this understanding, accountability can increase trust and thus improve situations where an IBP cannot be based on a long lasting collaboration.

However, so far the scope of accountability in the context of IBP is not sufficiently understood (cf. e.g. [11–14]). Given this conceptual shortcoming, this paper addresses the research question: **What is the scope of accountability facilitating to substantiate trust in the context of IBP?**

To address this question, we describe challenges to establishing trust in IBP and develop a framework of relevant dimensions of accountability. We structure the framework along the management, business process, and technical layers. We demonstrate the framework in an industrial supply chain case and conclude with a discussion about implications for theory and practice.

2. Theoretical Background

2.1 Inter-Organizational Business Processes

A radical change of the characteristics of trade occurred during the 20th century, away from simple physical distribution of goods and raw material towards a highly individually adopted and efficient management of product-flows across multiple echelons [15]. This development of supply chain management was driven by

the increasing awareness of the advantages regarding efficiency and cost reduction through collaborative relationships beyond specialized organization within a value chain [16, 17].

Along with this development, also the work in organizations changed dramatically. Business process management (BPM) was developed to improve how work in production and office can be done more efficiently by laying focus on improving processes in organizations [18].

Especially since the 1990s, with the growing number of external business relationships and dependencies of internal processes from external interconnections, the business processes of collaborating organizations need to be more and more aligned across organizational boundaries [17]. Following this development and internal BPM, mapping and controlling an IBP became an essential and complex task [17].

IBP is defined as “*an organized group of joined activities carried out by two or more organizations to achieve a common business objective*” [3]. IBP incorporates the concept of supply chain, but is not limited to physical goods, but also includes purely databased collaboration, e.g. in the provision of services.

An IBP can be considered on three different layers [3, 19, 20]. On the **management layer**, the strategic goals of an IBP are set, and a valuable perspective on collaborating with other organizations is taken. On the **business process layer**, the processes and interactions are designed and optimized with process modeling techniques. On the **technical layer**, the development and deployment of concrete artifacts are considered. Such artifacts include, for example, systems necessary for the execution of the IBP [19, 20].

Besides the potential benefits like faster, more cost-effective production with better quality [5], IBP can also lead to business vulnerabilities [6]. A recent example is the massive problem in the automotive industry regarding the procurement of semiconductors, triggered by the Covid19 pandemic and other circumstances. Different challenges must be considered to counteract such vulnerabilities, like the alignment of complex interdependent internal and external processes [4], the combination of different process logics and terminologies, and responsibilities and confidentiality issues [17]. Moreover, in an IBP, by definition, at least two organizations have the control over the execution of specific actions in the overall process [3, 21]. This distribution of control, often across sectoral and even national borders [8], leads to uncertainty for the single organizations, as they become dependent on the actions of others.

In order for an IBP to be established despite these vulnerabilities, trust between the involved parties is required [8, 21, 22]. Trust can be defined as “*the willingness to assume that a partner will bear the vulnerability*

stemming from the acceptance of risk” [8]. Poppo et al. [9] examined that the expectation of continuity plays a critical, a common past a supporting role in generating inter-organizational trust. Especially in cases where trust is mainly based on economic considerations and the expectation that future returns of the collaboration outweigh the gains from self-interested behavior for all parties, a long time horizon is required [9].

Therefore, building trust is especially challenging in today’s highly dynamic world. In many cases, collaborative business processes must be implemented in situations where trust is lacking [8, 10]. One increasingly discussed possibility of improving such situations and building a more solid foundation for trust, despite just economic considerations or the existence of a long lasting collaboration, is the substantiation of trust through accountability [10, 23, 24].

2.2 Accountability in the Context of IBP

Although research studied accountability in multiple domains, a generally acknowledged definition of accountability in the context of IBP is lacking [11–14], as extant research shows. Existing definitions are often bound to a particular context and focus on management or technology perspectives (cf. e.g. [14]). Furthermore, the boundaries to terms like traceability (cf. e.g. [7]) or responsibility (cf. e.g. [25]) are blurred.

In the context of IBP, several essential features of accountability are described in the literature

Assignable responsibilities: Accountability means a transparent assignment and ownership of responsibilities for actions, decisions, products, and policies, legitimizing certain expectations about established results between members in a community, as well as for the obligation to be answerable for possible consequences [1, 12, 26, 27].

Distributed obligations: Accountability means, that obligations and business goals can be distributed across business units with different roles and capabilities while maintaining transparent responsibilities, activities, and relations [12, 28, 29].

Rules and agreements: Accountability manifests as rules and agreements controlling authorities and giving certainty about the legitimacy of expectations between community members [12, 30].

Judgment: Accountability implies that some actors have the right to judge other actors whether they have fulfilled their responsibilities in light of defined rules, and to impose sanctions if the responsibilities have not been met [31].

Managing complex situations: Accountability means that within complex task environments where multiple, diverse, and conflicting expectations arise, responsibilities and obligations keep manageable [30].

Verification: Accountability means a mechanism exists to verify whether or not an obligation has been satisfied in a predefined and transparent way [28, 32].

Concerning these features, we define accountability in the context of IBP as follows. **Accountability** is the transparent assignment and ownership of responsibilities based on rules and agreements about the expected results and obligation, facilitating to judge whether all parties have fulfilled their responsibilities and impose sanctions if not, thereby enabling distributing business goals across multiple organizations. To this end, accountability provides the possibility to verify that the obligations have been satisfied by all parties enabling to manage a complex situation where multiple, diverse, and conflicting expectations exist.

Accountability enables in IBP to assess whether all parties have fulfilled their responsibilities through transparent assignment and assumption of responsibilities, based on rules and agreements on expected outcomes and commitments, and to impose sanctions in the event of non-fulfillment. Accountability allows business objectives to be distributed across multiple organizations, even in complex situations with different and conflicting expectations.

3. Research Approach

We follow a qualitative analysis approach to explorative research. We aim at developing a descriptive artifact –an analysis framework– as a theory for analyzing [33]. Our research approach is rooted in the paradigm of pragmatism [34]. We studied the findings through an argumentative-deductive analysis [35], which comprised literature study and case studies, which include empirical data gathering and analysis as well as concept and prototype development.

We choose this approach in accordance with [34, 36] for two reasons. On the one hand, the authors were involved in dialogical action during seminars jointly conducted with practice partners in their role as scientific advisors and student supervisors [37]. This allowed for an in-depth study of 23 cases. On the other hand, we aim at the development of a theory-based artifact combining interpretation of work [38] as well as practical inquiry [34], which also involved developing technical artifacts to evaluate the feasibility of our arguments through prototyping [39, 40] for each of the cases under study.

3.1 Literature study

We conducted a systematic literature review based on Webster and Watson [41]. To avoid a cold start problem as described by Levy and Timothy [42], initially, we conducted a broad, unstructured literature search in

Google Scholar for highly cited papers about trust, accountability, and IBP.

The input of these papers was used to expand the search to multiple databases including, literature in the area of computer science and information systems, as our focus on the implementation of accountability in IBP lies in these two research fields. Through a broad search, we got a comprehensive overview regarding relevant scientific literature not confined to one research methodology, one set of journals, or one geographic region [41]. For the extended search, we focused on the terms accountability respectively accountable and business process.

In total, we found 274 potentially relevant papers in the five databases from Scopus, the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE), ScienceDirect (SD) and Web of Science (WoS).

Following the structured guidelines for the effective screening of scientific papers described from Petersen et al. [43] and Faber et al. [44], we analyzed these papers in multiple iterations. At first, we excluded papers for which the title and the keywords did not indicate that they addresses accountability in the context of business processes while also considering related wordings. In the next step, we read the abstracts of the remaining 46 papers. We once more extracted papers considering the criteria described above as well as additionally such with no explicit reference to an inter-organizational context. Again, we also took an abstract mentioning of the inter-organizational context through wordings like “multiple interacting parties” and “distributed business processes” into account. From the 21 remaining papers, we had full-text access to 14. Finally, after analyzing these papers, we found that all were relevant and beneficial for our topic. Conducting a forward and backward search [41] in these papers brought two additional papers, resulting in 16 relevant papers for accountability substantiating trust in IBP.

3.2. Case studies and exemplary framework application

We studied cases, developed in the period 2017 to 2020 across different industries and domains as part of a master’s seminar conducted by Fortiss and the Chair of Information Systems at the TU Munich.

For each case, empirical data was gathered and analyzed, a concept and prototype development we developed. The empirical data includes data and documents provided by the organization and its partner in each case under study, interviews, workshops, meeting minutes, existing information systems, and business process documentation. The concept development involves a stake-

holder needs analysis, a feasibility evaluation for a technology-enabled IBP, and a technical architecture design for the future information system. The prototype development involves implementing of core components that emphasize the need for a technical mechanism to address accountability.

For demonstration purposes, we apply the developed framework in an industrial supply chain case for IBP. The use case focuses on a small manufacturing company (COMP) in Germany, which produces safety-critical components, among others for the aerospace industry. The information regarding the use case and the application of the framework are taken from three reports as well as additional company internal documents and unstructured interviews with experts from the company as well as actors along the supply chain.

4. Trust Challenges in IBP

The Economist Intelligence Unit [10], states that collaborations are often built on trust between the partners. This is why a thorough verification of the trustworthiness of potential partners and the general standards of trust in inter-organizational businesses play an essential role for successful IBP.

As stated above, “trust is a likely outcome of prior history for parties engaged in frequent transactions in which learning occurs and expectation of continuity arises” [9].

This and other factors like unequal power relations and an environment with fast changing processes and partners can lead to situations where an IBP must be initiated and implemented although trust is lacking [8].

We identified the following challenges for IBP in tackling trust vulnerabilities between involved actors:

Lack of contextual understanding [45]: IBP often takes place in an international context. This is a challenge for organizations if they “*lack local knowledge and embeddedness in the networks of local relationships*”[45], which can cause higher expenses for the organization in the IBP. Through the missing knowledge and network, central requirements for establishing of trust in the other parties in this context are missing.

The reputation of Corporate Social Responsibility [46, 47] **and sustainability** [48]: Social responsibility and sustainability are becoming more important in society. As a result, and through the tightening of national and international regulations, they are also becoming increasingly crucial for the reputation and success of companies. In IBP, the monitoring of corporate social responsibility and sustainability is often difficult and more of a risk, as the malfunctioning of an organization can have adverse effects on all involved parties. Reputation regarding social responsibility and sustainability is thereby also highly interconnected to trust since

it is a kind of trust from the customer in the integrity of the OEM and its capability to control his partners in IBP. Moreover, the challenge of increasing vulnerabilities through interdependencies of an organization is affected by trust since this vulnerability is only accepted if there is trust in the honesty of the other partners.

Interdependencies and complexity [48–50]: Through IBP, the interdependencies of the organization from other organizations increase significantly, which leads to vulnerabilities if the partners do not fulfill their tasks as agreed on or, if needed, competencies are no longer accessible after the termination of cooperation. These interdependencies also increase the complexity since a detailed time, information, and dependency management is needed across multiple organizations.

Concluding these findings, the main challenge to tackle in IBP is the substantiation of trust to build a more solid foundation for trust than just economic considerations or the existence of a long-lasting collaboration. An increasingly discussed approach, therefore, is accountability [10, 23, 24].

5. Dimensions of Accountability in IBP

IBP can be analyzed at three levels [3, 19, 20], the management, business process, and technical layer. At these three levels, we have identified nine dimensions that influence accountability in IBP, as shown in Figure 1. The focus of the identified dimensions is on an organizational rather than an individual view.

At the **management layer**, strategic goals are defined and the expected added value from a collaboration with other organizations is considered.

Compliance: One aim of accountability is allowing to “*verify compliance according to evidence in a provable and undeniable way*” [23]. Compliance is ensuring that “*business processes, operations, and practice are in accordance with a prescribed and/or agreed set of norms*” [51]. From a management layer view, compliance is a dimension affiliated in two respects with accountability. First, all organizations have specific roles to follow derived, e.g. from legal regulations, they have to be compliant with and for which they are held accountable (from the state or customers) in a broader context [28]. As in IBP, the collaborating organizations can be distributed over multiple countries and industries, and possibly each organization could have to be compliant to other regulations. These specific regulations must be considered for developing the regulatory framework for an IBP so that this IBP is compliant with the regulations required from the different organization.

Second, accountability enables the control of the compliance of all parties in an IBP to the defined regulatory framework [23]. “*The importance of compliance has dramatically increased over the last few years for*

businesses in several industry sectors” [51]. Examples of compliance roles stemming from legal regulations, regulatory bodies, or standards are Sarbanes-Oxley, Basel II and ISO9000 [28, 51].

Control is a dimension for accountability in IBP since only parties with control over a specific process can be held accountable for the condition of this process [1, 29, 30]. Thereby we define the term control as the capability of an organization to bringing a certain condition in a process step on its own [1]. To achieve accountability, it is necessary that each organization delimit its control area, so that it is transparent for which process step the organization can be responsible for. This delimitation has to be done on a management level.

Regulatory Framework: Accountability is rights-driven and needs a regulatory framework, which defines the requirements, goals, and completion criteria, for

which satisfaction a party is accountable and by which to judge the completion of the process in a verifiable way [1, 12, 23, 31]. The regulatory framework is the instrument to govern an IBP and consists of a set of “*arrangements and agreements between supply chain actors*” [52]. The bases for this framework are the compliance regulations and the liabilities of each organization. The regulatory framework is not one single collaboration contract closed by all parties. Instead, it arises from multiple contracts between partners in the process chain or even informal arrangements based on trust, commitment, and reputation [52]. It is thereby strongly dependent on the structure of the IBP. For that reason, to contemplate the regulatory framework of a whole IBP, it is necessary to consider all involved parties. The conditions for the regulatory framework of an IBP are thereby determined on a management level.

	Dimensions	Central Question	Artefacts
Management Layer	Compliance	To which compliance regulations are the parties accountable?	E.g. Sarbanes-Oxley, Basel II and ISO9000
	Control	Who has the control in each process-step to determine the output?	Inter-organizationally accepted delimitation of the control capabilities over the single process steps
	Regulatory Framework	Is there a clear regulatory framework for the IBP that defines the requirements, goals, and completion criteria for each party?	E.g. BMW Group Supplier Sustainability Standard, Airbus Sustainable supply chain regulations
Business Process Layer	Responsibilities	Which actors have which obligations regarding output and manner of completion for the specific process steps?	Inter-organizationally accepted stakeholder diagram
	Dependencies	Which dependencies exist between process-steps and organizations?	Inter-organizationally accepted stakeholder diagram
	Data collection points	At which points in the IBP must data be collected or process steps adopted to make the process traceable?	Process flow diagram in BPMN with relevant data and data-sources to implementation accountability
Technical Layer	Identity Management	How are all organizations in the IBP uniquely and authoritatively identifiable?	E.g. signatures on documents, stamps, digital signatures, public & private key encryption
	Reconstructable Traceability	Can the downstream path of the product be traced during and after production based on recorded information?	E.g. Archived documents, Blockchain systems
	Verification	How can be verified that all parties fulfill their tasks as agreed?	E.g. Audits, independent inspections, Blockchain systems

Figure 1: Framework of nine dimensions of accountability on the different layers of IBP (Own depiction)

Responsibilities: To achieve accountability, clear responsibilities for the defined regulations must be specified, e.g. who is responsible for delivering which sub-results of the process [6, 26, 32]. A clear definition of responsibility is dependent on the reference context [53]. In IBP, we consider the obligation for an unique process step assigned to one specific actor [1, 30]. This dimension is allocated to the business process layer, as at this layer, all single process steps are contemplated. Thereby, relevant input and output criteria for each step can be defined. The organization liable for a specific process step is then responsible for ensuring that given

the correct input, the result of that step meet the agreed output criteria [26]. Moreover, responsibility is not only be delimited to providing the agreed output. Still, it may also encompass executing the process step in an agreed way if defined in the regulatory framework. Responsibilities are highly interlinked with the dependencies between the parties [25].

Dependencies: Accountability in IBP requires a clear understanding of the dependencies between the process steps and the partners as they can affect an organization’s ability to fulfill its responsibilities [26]. Dependencies are thereby “*conditions deemed outside of*

the scope of the process but critical to the completion of the process” [26]. They describe in IBP the importance of input or output for an organization and its actions and the extent to which it is controlled by other parties [54]. Dependencies are considered at the business process layer as making them explicitly known in the business process design can help better manage risks and expectations in IBP [26]. Moreover, they have to be contemplated over organization borders since they always concern at least parties. The number of dependencies is crucial for the complexity of an IBP and clear accountability in it and should be minimized [26].

Data collection points: One further dimension relevant to enabling accountability and trust in IBP is identifying data collection points in the process [1]. Data collection points are spots in the IBP where data must be raised to enable tractability and accountability throughout the process. It is relevant to analyze, which data is needed to achieve accountability and where this data is produced. If not all needed data can be gathered in the IBO, specific steps of the process need to be adopted.

At the **technical layer**, the development and deployment of specific artifacts are considered. Such artifacts include, for example, systems necessary for the execution of the IBP [19, 20].

Identity Management: Identity management is an essential dimension because only if all parties involved in a specific IBP can be uniquely and authoritatively identifiable, they can be held accountable for their actions [23, 32, 55]. Thereby “*accountability is a concept to make the system accountable and trustworthy by binding each activity to the identity of its actor*” [23]. In conclusion, identity management in IBP means that each action can be unambiguously assigned to one unique organization known from its partners. As identity management again is distributed between the organizations, it also has to be considered over organization borders. Since in an inter-organization context a trustworthy determination of identities can be complex [55], identity management today is realized chiefly through IT systems and digital identities, through which organizations get authenticated in an IBP [32]. Therefore, we mainly consider identity management on the technical layer. An intensively discussed approach for a digital identity management solution in IBP is cryptographic digital signatures [28]. These are mainly investigated in blockchain technologies as the basis for a trustable platform with reliable access and identity management [32, 55].

Reconstructable Traceability: To enable accountability by enlightening and assigning violations of the defined regulatory framework to the responsible party, the whole process must be traceable [28, 56] and reconstructable. Traceability, also “*referred to as the ability*

to track and trace information” [57], is the “*ability to follow the downstream path of a product along the supply chain*” [52]. In contrast, reconstructability refers to the ability of accessing product-related records regarding what, how, where, why, and when specific processes were performed in the process chain [52]. This means that to obtain reconstructable traceability, the completion of all process steps must be tracked, and an immutable record must be stored. Since this is accomplished through diverse IT systems like ERP systems and throughout the whole IBP, reconstructable traceability is also considered at the technical layer and over organization borders.

Verification: Accountability in an IBP is only achievable if the involved organizations also have verification mechanisms. Verification is understood as examining that the other parties fulfill the tasks they are responsible for as agreed in the regulatory framework [23]. Through verification, the parties in a collaboration can ensure that the IBP is compliant to their specific regulations. Therefore, the parties also need to have control over the evidence to prove misconduct [23]. Since this can be achieved through reconstructable traceability, also verification is considered at the technical layer. However, as each organization in an IBP has to have the ability of verification regardless of the support of the partners, it must be situated in an organizational context.

6. Demonstration and Discussion

6.1 Case Overview

A rather simplified depiction of the IBP for COMP is shown in Figure 2. The IBP includes multiple parties at different tiers. For demonstration purposes, we consider one party per tier and only three tiers in the manufacturing process, although in reality, there exist multiple organizations in several tiers. COMP is a tier 2 supplier (supplier T2).

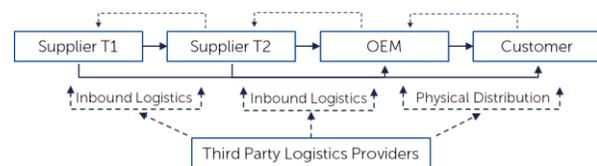


Figure 2: Simplified depiction of the general IBP in the use case (Own depiction)

The overall process starts with the ordering of a product from the customer at the OEM. Thereby the product characteristics are defined, often in multiple discussion rounds. The confirmation, along with the requirements, CAD models, and terms & conditions documents, is dispatched to the customer once the order is

confirmed. The tier 2 supplier initiates the requirements planning for raw material, components, tools, equipment and assesses risks and opportunities. Afterward, he places orders for the raw materials and the components. The respective two parties, tier 1 and tier 2 suppliers need to agree on the order specification details, including the price, expected delivery date, quality, etc.

Once the raw materials and components are ready, the tier 1 suppliers ship them to the tier 2 supplier, including quality documents and additional material on request. Upon receiving the materials, the tier 2 supplier reviews the shipment's quality and verifies the documents.

All details are saved in the ERP system, and, in case of incongruity, a complaint is raised to the respective tier 1 supplier. The raw materials and components are used to manufacture the product for the OEM. It is tested with in-house, fully automated test machines. The details of the manufacturing and the results of the testing are also stored in the ERP system.

Afterward, the order is labeled and shipped together with the agreed documents. The logistics company involved in the shipment is notified in case of special delivery conditions. Upon receiving the shipment, the OEM inspects the product and the documents, and if satisfied, initiates the payment or raises a complaint.

6.2 Application of the Framework

We exemplify the framework's application by describing first the particular trust challenges in the IBP of the case. The lack of contextual understanding for COMP concerns tier 1 supplier. For particular products, COMP has quality requirements for raw material, since potential product complains have to be analyzed back to a raw material batch. Lack of local knowledge limits the dynamics of business relationships with T1 suppliers since verifying the claims regarding requirement fulfillment for the raw material is very resource intensive.

In terms of corporate social responsibility and sustainability, COMP does not have specific requirements. It relies on information provided by its tier 1 suppliers, which it forwards to OEM and/ or customers.

The interdependence between the actors in the supply chain is high since COMP is a manufacturer of specific products that can hardly be sourced or replaced by another actor. At the same time, COMP has particular requirements for its tier 1 suppliers. Moreover, COMP provides OEM and customers with concrete guidelines for product use and care, which is crucial for sustaining the proper product quality over time. These interdependencies increase the complexity of the IBP since claims regarding COMP products has to be defined and verified over a period, in some cases even by third parties (e.g. certification bodies or assessors).

Concerning the rather general trust challenges, the developed framework provides an approach for a more detailed analysis and deriving potential measures to overcome the latter (cf. Figure 3).

	Dimensions	Artefacts
Management Layer	Compliance	DO-254: Design Assurance Guidance for Airborne Electronic Hardware
	Control	Contract with OEM
	Regulatory Framework	Terms & conditions documents (possibly with requirements, CAD models, ...) which are exchanged between the organizations
Business Process Layer	Responsibilities	Derived from OEM contract and distributed to suppliers in a hierarchical manner
	Dependencies	Depending on the particular role and tasks of each actor.
	Data collection points	Structured documents as forms and certificates along the business process as an interface between actors
Technical Layer	Identity Management	Signatures on documents, online access via shared link to documents
	Reconstructable Traceability	Document archiving
	Verification	External audits based on technical methods and control of archived documents

Figure 3: Exemplarily application of the accountability framework (Own depiction)

Compliance: Dependent on the OEM (customer) and its industry, different compliant regulations must be fulfilled. For instance, the most relevant norm in the aerospace industry is DO-254 regarding design criteria for airborne electronic hardware.

Control: Typically, the IBP is hierarchically controlled by the OEM, i.e. the suppliers from all tiers have to comply with the contractual conditions and provide evidence of their fulfilment.

Regulatory Framework: In this case, the regulatory framework is not a specific document with validity across all organizations but terms and conditions negotiated and agreed upon between the respective organization and its supplier.

Responsibilities: The responsibilities are derived from the contract. At the same time, the OEM tries to keep a manageable complexity of the interdependencies by enforcing his direct suppliers to manage the responsibilities of their suppliers from a lower tier.

Dependencies: Depending on the particular role and tasks of each actor. The dependencies involved exchanging information regarding the product and its quality guarantees. Typically, full transparency exists only between two directly interacting parties, resulting in limited transparency along the entire supply chain.

Identity Management: Identity management is still represented by signatures on documents. However,

this causes increased risks, e.g. due to defective, counterfeit products, which are difficult to identify. A more digital approach applied by COMP is to share unique document links with its suppliers based on their role in the supply chain. Still, this approach does not apply to OEM or customers. They typically have their information systems and still rely on signed paper documents (potentially, with attachments as a digital document).

Reconstructable Traceability: In case of an accident, the source must be traced back through the documents exchanged with the product. However, the entirety of the documents is only partially exchanged due to privacy aspects. For that reason, complete traceability based on the documents requires the involvement of several parties, which in turn increases complexity and error-proneness

Verification: Verification is conducted mainly by audits of the single parties in the IBP and in case of an accident by controlling the documents distributed over the single parties. A continuing verification is very resource-intensive and is currently mastered by excelling in information shared along the business process and quality management techniques. Still, claims are verified in detail only in case of a complaint. In such a case, a third-party auditor might even apply technical methods to verify product quality according to predefined specifications.

From an overall perspective, the case shows a clear need for a holistic approach to accountability throughout all layers. For instance, if changes to the management layer occur, only workarounds are available to translate the changes to the business process and technology layer. Starting from the technical layer, it is crucial to be able to introduce novel technology tools to upper layers and to as many actors as possible along the IBP to gain the highest benefits in terms of efficiency.

7. Conclusion

In this paper, we present a framework with nine dimensions specifying the scope of accountability on the different layers of IBP, as a first step towards substantiating trust in IBP.

We give an overview and definition of IBP and the importance of trust in this context as well as of accountability. Furthermore, we define particular challenges of implementing trust in such processes and how the concept of accountability can substantiate trust.

Based on a literature study and an analysis of case studies, we develop a framework of dimensions at the different layers of IBP relevant for the implementation of accountability in this context. Finally, we demonstrate the framework in an exemplary supply chain case in the manufacturing industry.

Although several different sources were analyzed for the development of the framework, limitations regarding its general applicability exist. First, both types of sources, the literature study and analysis of case studies from a seminar are of theoretical nature. Furthermore, we only selected publications considering an inter-organizational context. For that reasons, the presented dimensions should be further evaluated and possibly extended through an extension of the literature study and especially through interviews and investigations in practices. Second, to utilize the findings of this paper, further characteristics of the dimensions and possibilities for a methodical analysis and adoption of the dimensions in IBP cases towards the implementation of accountability should be considered in future work.

Despite these limitations, we believe that our research is valuable for theory and practice as the framework is a first step towards a structured implementation of accountability in IBP. The framework can be used to discuss and confront current approaches for accountability in IBP and shows that future research is needed in the different dimensions. Practitioners can apply it to conduct an initial analysis of their current level of accountability in an IBP context and to derive general room and measures for improvement.

10. References

- [1] Baldoni, M., C. Baroglio, R. Micalizio, and S. Tedeschi, "Accountability and responsibility in business processes via agent technology", in Proceedings of the Workshop on Experimental Evaluation of Algorithms for Solving Problems with Combinatorial Explosion, Workshop on Experimental Evaluation of Algorithms for Solving Problems with Combinatorial Explosion (RCRA 2018), Oxford, UK. 2018.
- [2] Min, H. and G. Zhou, "Supply chain modeling: past, present and future", *Computers & Industrial Engineering*, 43, 2002, pp. 231–249.
- [3] Bouchbout, K. and Z. Alimazighi, "Inter-Organizational Business Processes Modelling Framework", in Proceedings II of the 15th East-European Conference on Advances in Databases and Information Systems (ADBIS '11), J. Eder, M. Bielikova, and A.M. Tjoa, Editors, ADBIS '11, Vienna, Australia. 2011. CEUR-WS.org.
- [4] Liu, C., Q. Li, and X. Zhao, "Challenges and opportunities in collaborative business process management: Overview of recent advances and introduction to the special issue", *Information Systems Frontiers*, 11(3), 2009, pp. 201–209.
- [5] Norta, A., P. Grefen, and N.C. Narendra, "A reference architecture for managing dynamic inter-organizational business processes", *Data & Knowledge Engineering*, 91, 2014, pp. 52–89.
- [6] Baldoni, M., C. Baroglio, O. Boissier, R. Micalizio, and S. Tedeschi, "Engineering multiagent organizations by accountability and responsibility", in Proceedings of the 5th Collaborative European Research Conference (CERC

- 2019), 5th Collaborative European Research Conference, Darmstadt, Germany. 2019. CEUR-WS.org.
- [7] Corallo, A., M.E. Latino, and M. Menegoli, "A Business Process Modelling Approach for Supporting Traceability in Food Industry", in Proceedings of the 8th International Conference on Industrial Technology and Management, Cambridge, United Kingdom. 2019. IEEE.
- [8] Vangen, S. and C. Huxham, "Nurturing Collaborative Relations", *The Journal of Applied Behavioral Science*, 39(1), 2003, pp. 5–31.
- [9] Poppo, L., K.Z. Zhou, and S. Ryu, "Alternative Origins to Interorganizational Trust: An Interdependence Perspective on the Shadow of the Past and the Shadow of the Future", *Organization Science*, 19(1), 2008, pp. 39–55.
- [10] Economist Intelligence Unit, "The role of trust in business collaboration: An Economist Intelligence Unit briefing paper sponsored by Cisco Systems", *The Economist*, 2008.
- [11] Kaciánka, S. and A. Pretschner, "Understanding and Formalizing Accountability for Cyber-Physical Systems", in Proceedings of 2018 IEEE International Conference on Systems, Man, and Cybernetics, International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan. 2018. IEEE.
- [12] Dubnick, M.J. and J.B. Justice, "Accounting for accountability", in Annual Meeting of the American Political Science Association, APSA. 2004.
- [13] Parmigiana, A., R.D. Klassen, and M.V. Russo, "Efficiency meets accountability: Performance implications of supply chain configuration, control, and capabilities", *Journal of Operations Management*, 29, 2011, pp. 212–223.
- [14] Kaciánka, S. and A. Pretschner, "Designing Accountable Systems", in Fairness, Accountability, and Transparency (ACM FAccT) 2021. 2021.
- [15] Hou, H., S. Chaudhry, Y. Chen, and M. Hu, "Physical distribution, logistics, supply chain management, and the material flow theory: a historical perspective", *Information Technology and Management*, 18(2), 2017, pp. 107–117.
- [16] Rattray, R., "Defining supply chain management: a historical perspective and practical guidelines", *Industrial Management & Data Systems*, 99, 1999, pp. 11–17.
- [17] Legner, C. and K. Wende, "The Challenges Of Inter-Organizational Business Process Design – A Research Agenda", 15th European Conference on Information Systems (ECIS) 2007. - St. Gallen, Switzerland, 2007.
- [18] Dumas, M., M. La Rosa, J. Mendling, and H.A. Reijers, *Fundamentals of Business Process Management*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- [19] Huemer, C., P. Liegl, R. Schuster, H. Werthner, and M. Zapletal, "Inter-organizational systems: From business values over business processes to deployment", in 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies, 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies (DEST), Phitsanuloke, Thailand, 26.02.2008 - 29.02.2008. 2008. IEEE.
- [20] Adam, O., S. Zang, C. Hammer, M. Jerrentrup, and S. Leinenbach, "A Collaboration Framework for Cross-enterprise Business Process Management", First International Conference on Interoperability of Enterprise Software and Application, Geneva, 2005.
- [21] Muller, M., S.R. Garzon, M. Rosemann, and A. Kupper, "Towards Trust-Aware Collaborative Business Processes: An Approach to Identify Uncertainty", *IEEE Internet Computing*, 24(6), 2020, pp. 17–25.
- [22] Seppänen, R., K. Blomqvist, and S. Sundqvist, "Measuring inter-organizational trust—a critical review of the empirical research in 1990–2003", *Industrial Marketing Management*, 36(2), 2007, pp. 249–265.
- [23] Yao, J., S. Chen, and D. Levy, "Accountability-Based Compliance Control of Collaborative Business Processes in Cloud Systems", in Security, Privacy and Trust in Cloud Systems, S. Nepal and M. Pathan, Editors. 2014. Springer Berlin Heidelberg: Berlin, Heidelberg.
- [24] Hall, A.T., D.D. Frink, and M.R. Buckley, "An accountability account: A review and synthesis of the theoretical and empirical research on felt accountability", *Journal of Organizational Behavior*, 38(2), 2017, pp. 204–224.
- [25] Baldoni, M., C. Baroglio, and O. Boissier, "Engineering Business Processes through Accountability and Agents", in Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems, AAMAS, Montreal, Canada. 2019. IFAAMAS.
- [26] Tseng, M.M., C.-J. Su, and M. Qin Hai, "Accountability Centered Approach to Business Process Reengineering", in Proceedings of the Thirty-First Hawaii International Conference on System Sciences, HICSS, Kohala Coast, HI, USA. 1998. IEEE.
- [27] van Bussel, G.-J., "Accountability and the Reconstruction of the Past", in ECIS 2011 Proceedings, The European Conference on Information Systems Management, Helsinki, Finland. 2011.
- [28] Breaux, T.D., A.I. Antón, and E.H. Spafford, "A distributed requirements management framework for legal compliance and accountability", *Computers & Security*, 28(1-2), 2009, pp. 8–17.
- [29] Baldoni, M., C. Baroglio, R. Micalizio, and S. Tedeschi, "Implementing Business Processes in JaCaMo+ by Exploiting Accountability and Responsibility", in Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems, AAMAS, Montreal, Canada. 2019. IFAAMAS.
- [30] Baldoni, M., C. Baroglio, O. Boissier, R. Micalizio, and S. Tedeschi, "Accountability and Responsibility in Multi-agent Organizations for Engineering Business Processes", in Engineering Multi-Agent Systems, L.A. Dennis, R.H. Bordini, and Y. Lespérance, Editors, 7th International Workshop, EMAS 2019, Montreal, QC, Canada. 2020. Springer International Publishing: Cham.
- [31] Grant, R.W. and R.O. Keohane, "Accountability and Abuses of Power in World Politics", *The American Political Science Review*, 99, 2005, pp. 29–43.
- [32] Felicetti, C., A. Furfaro, D. Saccà, M. Vatalaro, M. Lanuzza, and F. Crupi, "Making IoT Services Accountable: A Solution Based on Blockchain and Physically Unclonable Functions", in Internet and Distributed Computing Systems, R. Montella, A. Ciaramella, G. Fortino, A. Guerrieri, and A. Liotta, Editors, International Conference on Internet and Distributed Computing Systems,

- Naples, Italy. 2019. Springer International Publishing: Cham.
- [33] Gregor, S., "The Nature of Theory in Information Systems", *MIS Quarterly*, 30(3), 2006, pp. 611–642.
- [34] Goldkuhl, G., "Pragmatism vs interpretivism in qualitative information systems research", *European Journal of Information Systems*, 21, 2012, pp. 135–146.
- [35] Wilde, T. and T. Hess, "Forschungsmethoden der Wirtschaftsinformatik: Eine empirische Untersuchung", *Wirtschaftsinformatik*, 49, 2007, pp. 280–287.
- [36] Cole, R., S. Puroo, M. Rossi, and M. Sein, "Being Pro-active: Where Action Research Meets Design Research", *ICIS 2005 Proceedings*, 27, 2005.
- [37] Mårtensson, P. and A.s. Lee, "Dialogical action research at omega corporation", *MIS Quarterly*, 28, 2004, pp. 507–536.
- [38] Klein, H.K. and M.D. Myers, "A set of principles for conducting and evaluating interpretive field studies in information systems", *MIS Quarterly*, 23(1), 1999, pp. 67–93.
- [39] Naumann, J.D. and A.M. Jenkins, "Prototyping: the new paradigm for systems development", *MIS Quarterly*, 1982, pp. 29–44.
- [40] Chiasson, M. and A.S. Dexter, "System development conflict during the use of an information systems prototyping method of action research", *Information Technology & People*, 2001.
- [41] Webster, J. and R.T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review", *MIS Quarterly*, 26(2), 2002.
- [42] Levy, Y. and E.J. Timothy, "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research", *Informing Science Journal*, 9, 2006.
- [43] Petersen, K., R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering", in *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering*, 12th International Conference on Evaluation and Assessment in Software Engineering (EASE) (EASE), 26–27.06.2008. 2008.
- [44] Faber, A., M. Riemhofer, S.-V. Rehm, and G. Bondel, "A Systematic Mapping Study on Business Ecosystem Types", in *AMCIS 2019 Proceedings*, G. Rodriguez-Abitia and C. Ferran, Editors, AMCIS 2019 Conference. 2019.
- [45] Nachum, L., "Foreignness, multinationality and inter-organizational relationships", *Strategic Organization*, 8(3), 2010, pp. 230–254.
- [46] Maloni, M.J. and M.E. Brown, "Corporate Social Responsibility in the Supply Chain: An Application in the Food Industry", *Journal of Business Ethics* volume, 68, 2006, pp. 35–52.
- [47] Yawar, S.A. and S. Seuring, "Management of Social Issues in Supply Chains: A Literature Review Exploring Social Issues, Actions and Performance Outcomes", *Journal of Business Ethics*, 141, 2015, pp. 621–643.
- [48] Nuhoff-Isakhanyan, G., E.F. Wubben, and S. Omta, "Sustainability Benefits and Challenges of Inter-Organizational Collaboration in Bio-Based Business: A Systematic Literature Review", *Sustainability*, 307(8), 2016.
- [49] Casey, C., J. Li, and M. Berry, "Interorganizational collaboration in public health data sharing", *Journal of Health Organization and Management*, 30(6), 2016, pp. 855–871.
- [50] Hall, D.J., J.B. Skipper, B.T. Hazen, and J.B. Hanna, "Inter-organizational IT use, cooperative attitude, and inter-organizational collaboration as antecedents to contingency planning effectiveness", *The International Journal of Logistics Management*, 23(1), 2012, pp. 55–76.
- [51] Sadiq, S., G. Governatori, and K. Namiri, "Modeling Control Objectives for Business Process Compliance", in *Business Process Management*, G. Alonso, P. Dadam, and M. Rosemann, Editors. 2007. Springer Berlin Heidelberg: Berlin, Heidelberg.
- [52] Pant, R.R., G. Prakash, and J.A. Farooque, "A Framework for Traceability and Transparency in the Dairy Supply Chain Networks", *Procedia - Social and Behavioral Sciences*, 189, 2015, pp. 385–394.
- [53] van de Poel, I., "The Relation Between Forward-Looking and Backward-Looking Responsibility", in *Moral Responsibility: Beyond Free Will and Determinism*, N.A. Vincent, I. van de Poel, and J. van den Hoven, Editors. 2011. Springer Netherlands: Dordrecht.
- [54] Pfeffer, J. and G. Salancik, *The External Control of Organizations: A Resource Dependence Perspective*, Harper & Row, New York, 1978.
- [55] Furfaro, A., L. Argento, D. Sacca, F. Angiulli, and F. Fassetti, "An Infrastructure for Service Accountability based on Digital Identity and Blockchain 3.0", in *Proceedings of IEEE INFOCOM 2019, IEEE Conference on Computer Communications Workshops*, Paris, France. 2019. IEEE.
- [56] Zhang, Y., K.-J. Lin, and T. Yu, "Accountability in Service-Oriented Architecture: Computing with Reasoning and Reputation", in *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'06)*, IEEE International Conference on e-Business Engineering, Shanghai. 2006. IEEE.
- [57] Sunny, J., N. Undralla, and V. Pillai, "Supply chain transparency through blockchain-based traceability: An overview with demonstration", *Computers & Industrial Engineering*, 150, 2020.