

# Integrating IT Security Aspects into Business Process Models: A Taxonomy of BPMN Extensions

Leonard Nake<sup>1</sup>

<sup>1</sup> Martin Luther University Halle-Wittenberg, Universitaetsring 3, 06108 Halle (Saale), Germany

## Abstract

Protecting themselves from IT security breaches is a crucial and cost-intensive task for the organizations of today. To achieve this, organizations implement bundles of IT security measures to secure their assets, which substantially influences their business processes. Therefore, aspects from the IT security domain must be integrated into business process models to adequately represent reality. There are various papers introducing extensions that integrate these aspects into the Business Process Model and Notation (BPMN) language. However, existing literature reviews are outdated and do not identify common characteristics among BPMN extensions that integrate IT security aspects. Based on the analysis of 18 papers that were identified during a structured literature review, this article develops a multi-dimensional taxonomy of BPMN extensions. This taxonomy identifies common characteristics and dimensions of the extensions and therefore gives a structured overview of the field and provides profound insights into the existing work.

## Keywords

IT security, BPMN extension, literature review, taxonomy

## 1. Introduction

Technological innovations, such as intelligent process automation or cloud computing, have drastically changed the business processes of companies in the last years and provided them with opportunities to develop competitive advantages. However, these innovations also introduce new security risks that need to be addressed. Technologies and other organizational assets must be protected from attacks aiming to access sensitive information, change the data in information systems, and disrupt the normal operations of information systems [1]. It is typically not sufficient to implement isolated IT security measures for single assets as complex bundles of interdependent measures are required. Because of this, IT security measures have a substantial influence on the business processes of organizations [2]. Hence, aspects of this highly influential IT security domain that are addressed with such measures should be integrated into business process models for them to adequately represent reality.


Because of this need to integrate IT security aspects into business process models, many extensions for Business Process Model and Notation (BPMN), which is the de facto standard modeling language for business process models, have been introduced. While these extensions have similarities to one another, each approaches the problem from a different angle and therefore defines different concepts to integrate IT security aspects. For instance, there are approaches that extend BPMN with the necessary attributes to perform risk assessments [3, 4] while other approaches extend it with administrative control policies such as the separation of duty [5]. While there are papers that conduct literature reviews in this field [6, 7], they are outdated as many extensions have been published since their publications. Additionally, they do not identify common characteristics among the identified BPMN extensions. Therefore, this article aims to firstly identify the latest and relevant BPMN extensions in the field and secondly


---

CIISR 2023: 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research, co-located with the 18th International Conference on Wirtschaftsinformatik (WI 2023), September 18, 2023, Paderborn, Germany

✉ leonard.nake@wiwi.uni-halle.de (L. Nake)

ORCID  0000-0001-8324-5641 (L. Nake)

 © 2023 Copyright for this paper by its authors.  
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

create a taxonomy to identify the characteristics and dimensions of the different extensions to give a structured analysis of the existing literature and show research gaps. I raise the following research question to address this problem:

*What are the dimensions and characteristics of BPMN extensions that integrate IT security aspects into business process models?*

To address the research question, I base the research design of the literature review on the method proposed by vom Brocke et al. [8]. The taxonomy creation is based on the method proposed by Nickerson et al. [9]. The contribution of this article is the new domain knowledge introduced through the literature review, on the one hand, and through the rigorous creation of the taxonomy, on the other hand. This paper is structured in the following way: In section 2, the related research relevant to this topic is discussed. The research design is explained in section 3 in detail. Section 4 describes the taxonomy that was created from the identified BPMN extensions. Section 5 is a further discussion of the findings of the literature review and the creation of the taxonomy. Section 6 concludes this article.

## **2. Related Research**

The related research of my paper can be divided into two types. Considering the first type, there are two publications that conduct reviews of BPMN extensions that integrate IT security aspects into business process models in some way. In their research, Maines et al. [7] analyze BPMN-security extensions to create a cyber security ontology. Although this might seem quite similar to my research, it is quite different. Maines et al. [7] focus on extensions that provide BPMN-security instead of IT security in general. Therefore, the identified literature as well as the goal of the research is not the same. For instance, the identified literature that extends BPMN to conduct risk assessments [10, 11] are not considered in the ontology. Additionally, Maines et al. [7] create an ontology instead of a taxonomy and their research was done in 2015, which means that several newer BPMN extensions could not be considered in their research.

Other closely related research is the paper of Leitner et al. [6]. The authors conduct a literature review of security aspects in BPMN and provide an overview of the identified concepts in combination with the extended BPMN elements. This paper is the most similar to my research and the identified concepts are still relevant today, which is why it was analyzed during the first iteration of creating the taxonomy. However, the literature review was done in 2013. Since then, many new BPMN extensions have been published. Therefore, a new literature review was necessary to identify all relevant extensions. Additionally, my paper has the goal to create a taxonomy from the identified BPMN extensions by using the well-known method developed by Nickerson et al. [9] to identify common characteristics among the extensions.

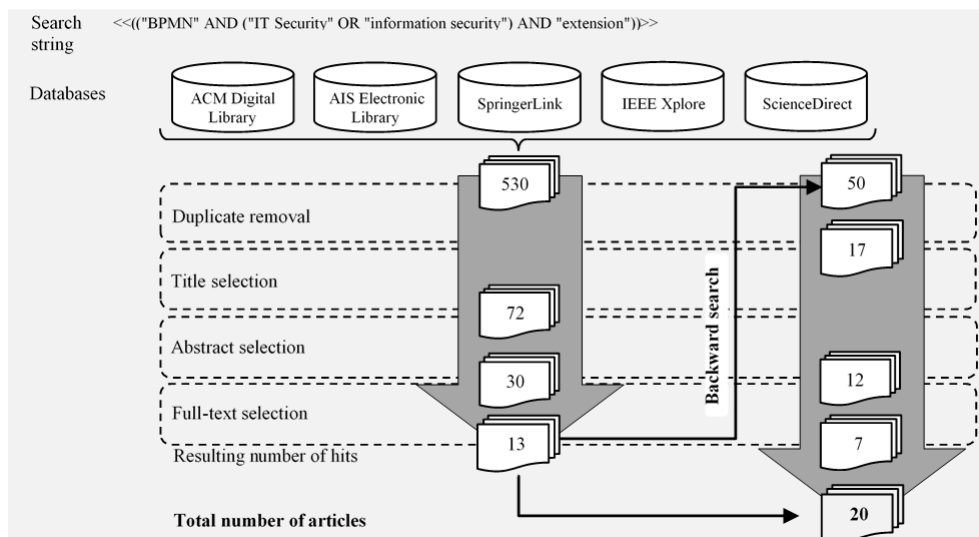
The literature identified during my literature search is the second type of related research. It is analyzed in the following sections.

## **3. Research Method**

### **3.1. Structured Literature Review**

This study aims to create a taxonomy of existing BPMN extensions that integrate IT Security aspects into business process models and therefore needs to identify the relevant literature. To achieve this, I conducted an exhaustive but selective structured literature review [12] and followed the methodological guidelines of Webster & Watson [13] as well as vom Brocke et al. [8]. In their research, vom Brocke et al. [8] define five steps necessary for a structured literature review. As the first step the review scope has to be defined. For my review, I defined the scope as articles that introduce or discuss BPMN extensions that deal with IT Security in some way. These articles must be published between 2013 and 2023 as older papers were already identified in the

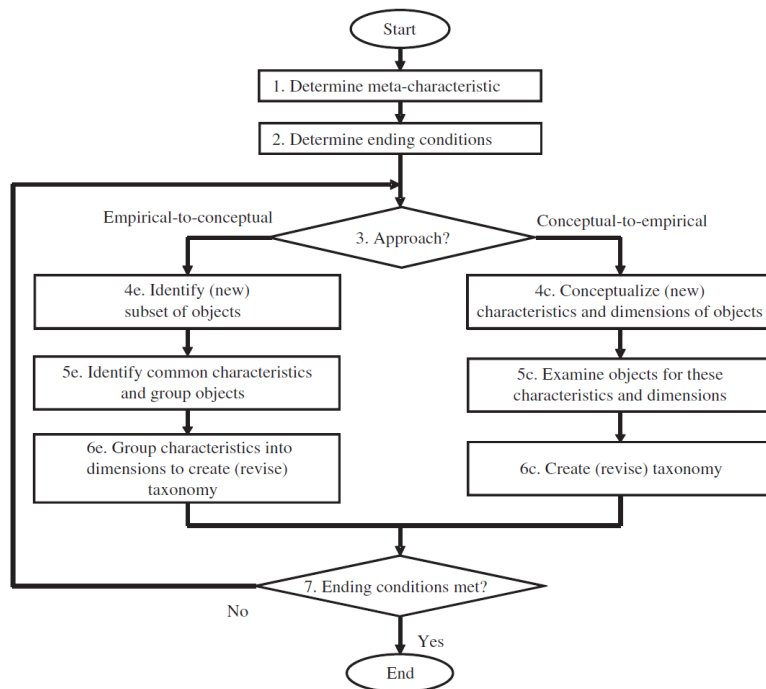
work of Leitner et al. [6], must be in English, and must be published in established scientific databases (ACM Digital Library, AIS Electronic Library, SpringerLink, IEEE Xplore, ScienceDirect). The second step is to conceptualize the topic. This work focuses on BPMN extensions since BPMN is the de facto standard language for modeling business processes. I also researched definitions and synonyms for IT Security. The third step is the actual literature search. The search string ("BPMN" AND ("IT Security" OR "information security") AND "extension") that was used to search full texts of articles resulted in 530 hits over the five databases. Then, the titles of the publications were analyzed which led to a drastic reduction in the number of hits (see Figure 1). After analyzing the abstracts and full text, there were 13 relevant articles left. We excluded articles that do not introduce or discuss BPMN extensions dealing with IT Security aspects but use other modeling languages or do not have IT Security as a main focus. As proposed by Webster & Watson [13], we then conducted a backward search which resulted in 7 additional papers after removing duplicates and analyzing the abstracts as well as the full texts. This led to a total number of 20 articles. Of these 20 publications, 18 introduced or improved relevant BPMN extensions and 2 articles reviewed the topic (see section 2). The fourth step is the analysis and synthesis of the identified literature. To achieve this, a taxonomy is developed in section four. Finally, in the last step, a research agenda has to be developed. This is done by discussing possibilities for future research in section six.



**Figure 1:** Literature Search Process

### 3.2. Development of Taxonomies in Information Systems

After identifying the relevant literature, I created a taxonomy following the widely used method for taxonomy development in information systems from Nickerson et al. [9]. The method consists of seven steps as shown in figure 2. The first step is to define a meta-characteristic that is based on the purpose, the users, and the expected use of the taxonomy. All characteristics must be logical consequences of this meta-characteristic. The second step is to determine the ending conditions for the taxonomy development. Then, one of two approaches has to be selected. The conceptual-to-empirical approach focuses on the conceptualization of dimensions and characteristics without examining the actual objects. This means that the creation of dimensions and characteristics is based on the researcher's notions about how the objects are similar and dissimilar. In the empirical-to-conceptual approach, a researcher has to identify a set of objects for the classification. Then, the researcher analyses these objects to find common characteristics and dimensions among them. Both approaches lead to the creation of a taxonomy that has to be evaluated considering the ending conditions. If all ending conditions are met the taxonomy development ends. If not all ending conditions are met, more conceptual-to-empirical or empirical-to-conceptual iterations have to be conducted.



**Figure 2:** Taxonomy Development Method by Nickerson et al. [9]

Nickerson et al. [9] proposed 13 ending conditions that have to be met. There are eight objective ending conditions (all objects examined, no objects/dimensions/characteristics split or merged in the last iteration, at least one object under every characteristic, no new dimensions/characteristics in the last iteration, each dimension/characteristic is unique, and each combination of characteristics is unique) and five subjective ending conditions (concise, robust, comprehensive, extendible, and explanatory). I describe the development of my taxonomy in the next section.

#### 4. Taxonomy of BPMN Extensions Integrating IT Security Aspects into Business Process Models

The creation of the taxonomy required 3 iterations until all ending conditions were met. The first conducted iteration was conceptual-to-empirical. In this iteration, I analyzed a literature review about security aspects in BPMN [6] to conceptualize dimensions and characteristics from the discussion of the literature in this article as a first step. Then, other theoretical work about the topic was consulted to gain insights into possible dimensions and characteristics. The other two iterations were empirical-to-conceptual. During these iterations, the 18 identified articles were analyzed to identify common characteristics. After the second iteration, three dimensions were discarded as they did not provide meaningful insights. Also, the dimension domain specificity had to be added since articles that introduced domain specific attributes differed significantly from more generic IT security attributes. While conducting the third iteration, all ending conditions were met. Neither dimensions nor characteristics changed during this iteration although all objects found during the literature search were classified. The resulting taxonomy is concise, robust, comprehensive, extendible, and explanatory and does not consist of repetitive characteristics or dimensions. It consists of five dimensions with 30 characteristics that are described in section 4.2. Of the five dimensions, only the domain specificity has mutually exclusive characteristics. This is a deliberate decision to make the taxonomy more concise and useful.

## 4.1. Meta-Characteristic

A meta-characteristic acts as the basis for the choice of characteristics so that each characteristic logically follows the previously defined meta-characteristic [9]. Since our taxonomy is aimed at researchers and practitioners that want to integrate IT security aspects into their business processes, we want to give a practical overview instead of going too far into the technical details of each extension. Hence, I define the meta-characteristic of the taxonomy as: 'characteristics of IT Security aspects and their extended BPMN elements defined in the identified BPMN extensions from a functionality perspective'.

## 4.2. Dimensions and Characteristics

The first dimension **risk assessment** includes articles that extend BPMN by aspects needed for conducting security risk assessments [4, 10, 11]. The characteristics are the security aspects used to perform these risk assessments. Reliability in this context is the counterpart to the failure probability. Papers extend BPMN with this value to include the probability of a security incident [3]. Risk objective describes the maximum value of acceptable risk in a business process [11]. Risk information is the risk value of a process or task based on the values of reliability and asset value [3]. Vulnerabilities as a characteristic means that the paper extends BPMN with information about vulnerabilities of a business process, for example, an insecure communication protocol [11]. The Asset value corresponds to the value that an asset represents for the organization [3]. While these characteristics are all part of the risk assessment, it makes sense to include them as separate characteristics in the taxonomy because the papers differ in the way they perform the assessment. Additionally, other BPMN extensions can integrate only some of the aspects into the business processes. For instance, Altuhhov et al. [14] introduced an annotation called "vulnerability point" to mark vulnerable assets, such as data objects or tasks.

The dimension **task execution rules** is comprised of rules about the execution of tasks. Separation of duty means that a task cannot be executed by a single person but has to be executed by at least two persons. The binding of duty dictates that several tasks have to be executed by the same person [15, 16]. The third characteristic is the rule non-delegation which means that a task can only be executed by assigned users [17].

The dimension **security goal** is built on the RMIAS reference model developed in the work of Cherdantseva & Hilton [18] and is referenced frequently in the different articles. It involves the following characteristics:

Authenticity describes the ability of a system to verify identity and establish trust in a third party as well as in the provided information [18]. The analyzed BPMN extensions try to implement this principle in different ways. For instance, Salnitri et al. [19] impose that the identity or authenticity of a user has to be verified in activities by requiring executors to have a minimum level of trust or by banning anonymous users from executing activities. Authenticity is also defined for data objects. Using the extension makes it possible to prove the genuineness of the data object by proving that the data was not modified by unauthorized parties or by proving the identity of the entity who generated or modified it. Salnitri et al. [19] give the example of a visa as a data object that is marked with an authenticity annotation that specifies the security mechanisms TLS (Transport Layer Security) and X.509 to be used in order to guarantee the integrity of the visa data.

Availability means that a system needs to ensure that all its components are available and functional when they are required [18]. One instantiation of availability found in the literature tries to ensure that critical resources are always available to process participants. If a requested resource is not available the system has to maintain backups from which the respective data object can be retrieved so that it is always available for the user [20].

Accountability describes a system's ability to hold users accountable should they perform harmful actions [18]. One of the ways how accountability is achieved in business process models is described in the work of Argyropoulos et al. [20]. In their extension, only process participants

with appropriate permissions can access resources or perform certain activities if they are authorization constrained.

Auditability means that a system needs to monitor all actions performed by actors in the system in a way that it cannot be bypassed [18]. There are different ways to implement auditability in business process models. For activities, it can be made possible to save all the actions performed by the executor of an activity. For data objects, it can be made possible to keep track of all actions concerning the data object, such as write, read, or store. For a message flow, it can be made possible to save all the actions performed during the communication [21].

Confidentiality is a system's ability to make information only accessible to authorized users [18]. One way to guarantee confidentiality is introduced by Pullonen et al. [22]. Their extension allows for the encryption and decryption of data in so-called privacy-enhancing technology tasks. It uses a data input and a public key to generate a ciphertext that can be decrypted with the respective secret key.

Integrity describes the ability of a system to ensure completeness, accuracy as well as the absence of unauthorized modifications in its components [18]. One example of an implementation of integrity in a business process model using a BPMN extension is to compare the system's copy of data to the original by data validation techniques if the data object in the business process model is integrity-constrained [20].

Non-repudiation means that a system needs to have the ability to prove the occurrence or non-occurrence of events and the participation or non-participation of parties in this event [18]. An example of non-repudiation in a business process model is described by Salnitri et al. [21]. For activities, the execution and non-execution of an activity can be made provable. For message flows, it can be made verifiable if a message flow was used or not used.

Privacy is a system's duty to obey privacy legislation. The system needs to enable individuals to control their personal information if feasible [18]. Privacy can be introduced to business process models by specifying that activities or data objects must be compliant with privacy legislation and should therefore let users control their own data [19].

The dimension **domain specificity** has the characteristics generic and domain specific and it describes whether the BPMN extension contains attributes that do not only implement generic IT security aspects but also domain specific aspects. Most BPMN extensions introduce generic concepts that exclusively implement IT security aspects into the business process model. However, there are exceptions in the identified literature. For instance, in addition to similar IT security aspects Ramadan et al. [17] introduce annotations for anonymity, undetectability, unlinkability, unobservability, and fairness for including data-minimization and fairness in the business process model. Köpke et al. [22] introduce annotations for enforceability and privacy in their model-driven approach to designing secure smart contracts.

The dimension **extended BPMN element** describes which of the existing BPMN elements were extended by each extension. It consists of the characteristics Activity, Event, Gateway, Pool, Message Flow, Data Object, Process, Subprocess, and Other that refer to the elements defined in the BPMN language. All extensions extended activities in some way and many extended data objects. Other BPMN elements were extended more rarely. The decision about which element is extended depends on the goal of each extension. For instance, Varela-Vaca et al. [4, 10, 11] decided to integrate most of their parameters by extending pools since they see the business process inside a pool as the main asset that needs assessment for their approach.

<b>Risk Assessment</b>	Reliability (5)	Risk Objective (5)	Risk Information (5)
	Vulnerabilities (4)	Asset Value (5)	None (12)
<b>Task Execution Rules</b>	Separation of Duty (5)		Binding of Duty (5)
	Non-delegation (3)		None (13)
<b>Security Goal</b>	Accountability (8)	Auditability (6)	Authenticity (10)
	Confidentiality (10)	Integrity (11)	Availability (11)
	Non-repudiation (7)	Privacy (8)	None (5)
<b>Domain Specificity</b>	Domain Specific (3)		Generic (15)
<b>Extended BPMN Element</b>	Activity (18)	Event (4)	Gateway (3)
	Pool (6)	Message Flow (7)	Data Object (12)
	Process (2)	Subprocess (2)	Other (6)

**Table 1:** Taxonomy of BPMN Extensions for Integrating IT Security Aspects

## 5. Discussion

Table 1 shows the final taxonomy. The small numbers in brackets show how many of the BPMN extensions fulfill each characteristic. If an extension integrates the respective IT security aspect it is counted into this number. The classification of the papers shows that most BPMN extensions are generic, meaning that they do not introduce domain specific but general IT security aspects. Most extensions perform no risk assessment but introduce annotations and execution logic into the business process model to achieve the security goals defined in [18]. Some extensions implement task execution roles. For example, some require tasks to be executed by at least two persons. While the BPMN elements that are extended differ in the different articles, all of them extend activities in some way.

There is a clear distinction in the identified literature between risk-oriented BPMN extensions and security goal-oriented extensions. The former focus on implementing security risk-related data into the business process model to perform calculations for a risk assessment. The latter focus on annotating and regulating BPMN elements to achieve security goals during the execution of the business process itself. The risk-oriented extensions are defined by Varela-Vaca et al. [4, 10, 11] and Cardoso et al. [3, 23]. While they aim for similar goals, there are differences. Varela-Vaca et al. [4, 10, 11] extend BPMN to assess the conformance of IT security properties in business process models by adding new calculations and model logic. Cardoso et al. [3, 23] focus on extending BPMN using the standard to perform quantitative risk assessment. Among the security goal-oriented extensions the most used language is SecBPMN [19]. On the one hand, it was refined by the authors themselves [5, 21]. On the other hand, several other publications referenced SecBPMN and augmented it with other aspects [17, 22]. Extensions built on the SecBPMN language are the only objects that fulfill all characteristics of the security goal as well as the task execution rules dimension. Therefore, it seems to be the standard extension in the field. Still, many authors published their own extensions to address the specific problems of their research fields [24–27]. The taxonomy shows that there seem to be research gaps in the field. The most

obvious one is that the risk-oriented extensions barely apply security goal-oriented concepts and vice versa. Naturally, it is possible to implement extensions from both groups at the same time but this would mean that the concepts do not influence each other. In reality, changes in the business process model caused by security goal-oriented concepts could influence the risk of the underlying business process. To integrate IT security aspects holistically it could be beneficial to consider both orientations. Therefore, it could be an interesting research objective to combine the two groups in a new extension.

## 6. Conclusion

In this research, I conducted a rigorous, structured literature review that led to the identification of 18 papers introducing BPMN extensions that integrate IT security aspects into business process models and two papers that review such extensions. Then, I created a multidimensional taxonomy from these 18 papers to answer my research question. I derived five dimensions and 30 characteristics of BPMN extensions that integrate IT security aspects that are explained in detail in section 4.2. However, there are limitations to this research that need to be considered. I followed well-known methods for the literature review as well as for the taxonomy creation to guarantee scientific rigor and maximize the objectivity of the research. Nevertheless, the results of this research are influenced by subjective decisions. Firstly, the literature review was done in only five scientific databases and the exclusion of papers is subjective to a certain extent. Additionally, the selection of the search string used in the literature search is partly subjective. However, I experimented with different synonyms (for example, expansion and augmentation as synonyms for extension) to analyze and improve the search results. Secondly, the actual creation of the taxonomy with all its dimensions and characteristics is a subjective process. Therefore, it is possible that other researchers would have developed other characteristics and dimensions. Despite these limitations, I believe that this work provides useful insights for scientists and practitioners.

This paper makes the following scientific contributions. The developed taxonomy can be used as a basis for further research about BPMN extensions that integrate IT security aspects. It provides knowledge about the relevant literature and can be used to classify new extensions. Additionally, the taxonomy structures the research field by deriving common characteristics and dimensions and shows research gaps, such as the observation that there are no extensions that combine the risk-oriented and the security goal-oriented view, which could be necessary for integrating a holistic combination of IT security aspects into the business processes of an organization. Therefore, it is possible to derive new BPMN extensions from the taxonomy. This research also has implications for practice. It allows practitioners to get an overview of existing BPMN extensions and their implemented IT security aspects and therefore provides them with insights that can help when choosing an extension that addresses their respective needs.

## Acknowledgements

The project on which this study is based was funded by the German Federal Ministry of Education and Research under grant number 16KIS1331. The responsibility for the content of this publication lies with the author.

## References

- [1] M. Z. Gunduz, and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, 2020, doi: 10.1016/j.comnet.2019.107094.
- [2] S. Kühnel, S. Sackmann, S. Trang, I. Nastjuk, T. Matschak, L. Niedzela, and L. Nake, "Towards a Business Process-based Economic Evaluation and Selection of IT Security Measures," CEUR Workshop Proceedings 2966, CEUR-WS.org 2021, pp. 7-21.



- [3] P. Cardoso, A. Respício, and D. Domingos, “riskaBPMN - a BPMN extension for risk assessment,” *Procedia Computer Science*, vol. 181, pp. 1247–1254, 2021, doi: 10.1016/j.procs.2021.01.324.
- [4] Á. J. Varela-Vaca, L. Parody, R. M. Gasca, and M. T. Gómez-López, “Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Models,” *IEEE Access*, vol. 7, pp. 26448–26465, 2019, doi: 10.1109/ACCESS.2019.2901408.
- [5] M. Salnitri, E. Paja, and P. Giorgini, “Maintaining Secure Business Processes in Light of Socio-Technical Systems' Evolution,” in *2016 IEEE 24th International Requirements Engineering Conference workshops: Proceedings : 12-16 September 2016, Beijing, China*, Beijing, China, 2016, pp. 155–164.
- [6] M. Leitner, M. Miller, and S. Rinderle-Ma, “An Analysis and Evaluation of Security Aspects in the Business Process Model and Notation,” in *2013 International Conference on Availability, Reliability and Security*, 2013.
- [7] C. L. Maines, D. Llewellyn-Jones, S. Tang, and B. Zhou, “A Cyber Security Ontology for BPMN-Security Extensions,” in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 1756–1763.
- [8] J. vom Brocke *et al.*, *Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process*. [Online]. Available: <https://www.alexandria.unisg.ch/handle/20.500.14171/75942>
- [9] R. C. Nickerson, U. Varshney, and J. Muntermann, “A method for taxonomy development and its application in information systems,” *European Journal of Information Systems*, vol. 22, no. 3, pp. 336–359, 2013, doi: 10.1057/ejis.2012.26.
- [10] A. J. Varela-Vaca, R. M. Gasca, and A. Jimenez-Ramirez, “A Model-Driven engineering approach with diagnosis of non-conformance of security objectives in business process models,” in *2011 Fifth International Conference on Research Challenges in Information Science (RCIS 2011): Gosier, [Guadeloupe], France, 19 - 21 May 2011 ; [proceedings, Gosier, France, 2011*, pp. 1–6.
- [11] A. J. Varela-Vaca, R. M. Gasca, and S. Pozo, “OPBUS: Risk-aware framework for the conformance of security-quality requirements in business processes,” in *Proceedings of the International Conference on Security and Cryptography*, 2011, pp. 370–374.
- [12] H. M. Cooper, “Organizing knowledge syntheses: A taxonomy of literature reviews,” (in En;en), *Knowledge in Society*, vol. 1, no. 1, pp. 104–126, 1988, doi: 10.1007/BF03177550.
- [13] J. Webster, and R. T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” *MIS Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002. [Online]. Available: <http://www.jstor.org/stable/4132319>
- [14] O. Altuhhov, R. Matulevičius, and N. Ahmed, “An Extension of Business Process Model and Notation for Security Risk Management,” *International Journal of Information System Modeling and Design (IJISMD)*, vol. 4, no. 4, pp. 93–113, 2013. [Online]. Available: <https://ideas.repec.org/a/igg/jisimd0/v4y2013i4p93-113.html>
- [15] A. D. Brucker, I. Hang, G. Lückemeyer, and R. Ruparel, “SecureBPMN,” in *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, New York, NY, USA, 2012.
- [16] W. Labda, N. Mehandjiev, and P. Sampaio, “Modeling of privacy-aware business processes in BPMN to protect personal data,” in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, Gyeongju Republic of Korea, 2014, pp. 1399–1405.
- [17] Q. Ramadan, D. Strüber, M. Salnitri, J. Jürjens, V. Riediger, and S. Staab, “A semi-automated BPMN-based framework for detecting conflicts between security, data-minimization, and fairness requirements,” *Softw Syst Model*, vol. 19, no. 5, pp. 1191–1227, 2020, doi: 10.1007/s10270-020-00781-x.
- [18] Y. Cherdantseva and J. Hilton, “A Reference Model of Information Assurance & Security,” in *2013 Eighth International Conference on Availability, Reliability and Security (ARES 2013): Regensburg, Germany, 2 - 9 [i.e. 2 - 6] September [2013 ; proceedings ; including workshops*, Regensburg, Germany, 2013, pp. 546–555.

- [19] M. Salnitri, F. Dalpiaz, and P. Giorgini, "Modeling and Verifying Security Policies in Business Processes," in *Lecture Notes in Business Information Processing*, vol. 175, *Enterprise, business-process and information systems modeling: 15th International Conference, BPMDS 2014, 19th International Conference, EMMSAD 2014, held at CAiSE 2014, Thessaloniki, Greece, June 16-17, 2014 ; Proceedings*, I. Bider, Ed., Heidelberg: Springer, 2014, pp. 200–214.
- [20] N. Argyropoulos, H. Mouratidis, and A. Fish, "Enhancing secure business process design with security process patterns," (in En;en), *Softw Syst Model*, vol. 19, no. 3, pp. 555–577, 2020, doi: 10.1007/s10270-019-00743-y.
- [21] M. Salnitri, F. Dalpiaz, and P. Giorgini, "Designing secure business processes with SecBPMN," *Softw Syst Model*, vol. 16, no. 3, pp. 737–757, 2017, doi: 10.1007/s10270-015-0499-4.
- [22] J. Köpke, G. Meroni, and M. Salnitri, "Designing secure business processes for blockchains with SecBPMN2BC," *Future Generation Computer Systems*, vol. 141, pp. 382–398, 2023, doi: 10.1016/j.future.2022.11.013.
- [23] P. B. Cardoso, D. Domingos, and A. Respício, "Contributions for risk assessment of IoT-aware business processes at different granularity levels," *Procedia Computer Science*, vol. 192, pp. 991–1000, 2021, doi: 10.1016/j.procs.2021.08.102.
- [24] M. E. A. Chergui and S. M. Benslimane, "A Valid BPMN Extension for Supporting Security Requirements Based on Cyber Security Ontology," in *Lecture Notes in Computer Science*, vol. 11163, *Model and data engineering: 8th International Conference, MEDI 2018, Marrakesh, Morocco, October 24–26, 2018 : proceedings*, E. H. Abdelwahed, L. Bellatreche, M. Golfarelli, D. Méry, and C. Ordonez, Eds., Cham: Springer, 2018, pp. 219–232.
- [25] P. Pullonen, R. Matulevičius, and D. Bogdanov, "PE-BPMN: Privacy-Enhanced Business Process Model and Notation," in *Lecture Notes in Computer Science*, vol. 10445, *Business Process Management: 15th international Conference, BPM 2017 Barcelona, Spain, September 10-15, 2017 ; proceedings*, J. Llinás, G. Engels, and A. Kumar, Eds., Cham: Springer, 2017, pp. 40–56.
- [26] P. Pullonen, J. Tom, R. Matulevičius, and A. Toots, "Privacy-enhanced BPMN: enabling data privacy analysis in business processes models," *Softw Syst Model*, vol. 18, no. 6, pp. 3235–3264, 2019, doi: 10.1007/s10270-019-00718-z.
- [27] K. S. Sang, and B. Zhou, "BPMN Security Extensions for Healthcare Process," in *The 15th IEEE International Conference on Computer and Information Technology (CIT 2015), the 14th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2015), the 13th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2015), the 13th IEEE International Conference on Pervasive Intelligence and Computing (PICom 2015): CIT/IUCC/DASC/PICom 2015 : proceedings : 26-28 October 2015, Liverpool, United Kingdom, LIVERPOOL, United Kingdom, 2015*, pp. 2340–2345.

# Appendix

Object	Risk Assessment					Task Execution Rules				Security Goal								Domain Specificity		Extended BPMN Element												
	Reliability	Risk Objective	Risk Information	Vulnerabilities	Asset Value	None	Separation of Duty	Binding of Duty	Non-delegation	None	Accountability	Auditability	Authenticity	Availability	Confidentiality	Integrity	Non-repudiation	Privacy	None	Domain Specificity	Generic	Activity	Event	Gateway	Pool	Message Flow	Data Object	Process	Subprocess	Other		
Brucker et al. 2012						X	X			X										X		X										
Varela-Vaca et al. 2019	X	X	X	X	X						X									X	X	X				X						
Varela-Vaca et al. 2011a	X	X	X	X	X						X									X	X	X				X						
Varela-Vaca et al. 2011b	X	X	X	X	X						X									X	X	X				X						
Cardoso et al. 2021a	X	X	X	X	X						X									X	X	X				X						
Cardoso et al. 2021b	X	X	X	X	X						X									X	X	X				X						
Saintri et al. 2014						X					X									X	X	X				X						
Saintri et al. 2016						X	X				X									X	X	X				X						
Saintri et al. 2017						X	X	X			X									X	X	X				X						
Pullonen et al. 2017						X					X									X	X	X				X						
Pullonen et al. 2019						X					X									X	X	X				X						
Argyropoulos et al. 2020						X					X									X	X	X				X						
Saintri et al. 2017						X					X									X	X	X				X						
Ramadan et al. 2020						X					X									X	X	X				X						
Altuhov et al. 2013				X							X									X	X	X				X						
Labda et al. 2014						X					X									X	X	X				X						
Sang & Zhou 2015						X	X				X									X	X	X				X						
Chergui et al. 2018						X					X									X	X	X				X						
Köpke et al. 2023						X	X		X		X									X	X	X				X						