Resource Policy Management using Access Control Model Enforcement in Business Processes

Paulo Sanchéz Lemos Alves

Instituto Superior Técnico, Lisboa, Portugal

January 2021

Abstract

Business processes are a core asset of corporations. They refer to how an organization is coordinated, to produce valuable products or services and determine the tasks and shape the work of every employee. Business Process Model and Notation (BPMN) is a standard available to model business processes with graphical representations. However, standards, such as BPMN are not thought and prepared to represent organizational policies related to the resources (i.e., people) of the organizations. This thesis proposes a BPMN framework, with the objective of having a better way for organizations to express their policies related to their resources or, informally, 'who can do what'. To capture this in business processes, access control models will be enforced to BPMN using the Atlas project as modeling tool. An access control model is a security technique to prevent unauthorized access to a system with the objective of achieving security. There are different types of access control models. In this thesis, the role-based access control (RBAC) and the attribute-based access control (ABAC) models are used. After implementing the BPMN framework in Atlas, a tool was developed for checking that every business process that uses the proposed framework is correct using a set of rules, and that will provide a system based on queries to support the actors and prevent non-compliant situations regarding the organizations' resource policies during the execution of the processes.

Keywords: Access control model, Attribute-based access control, Business process, BPMN, Role-based access control

1. Introduction

Authorization is present in every form of information technology and is concerned with how users can access resources in computer systems or, informally speaking, with *' who can do what'* [9]. We consider access control models as a way to offer the guarantee that only qualified users can gain access to what was assigned to them. Today, business process models (BPM) [5] are the core elements of an organization and refer to how an organization is coordinated and how its work is organized to produce valuable products or services. Business processes are defined as a collection of inter-related events, activities, and decision points that involve several actors [5].

There are different standards to express the business process of an organization, being one of the most used the Business Process Model and Notation (BPMN)[8]. Withal, such standards are not though to represent authorization constraints [15]. Integrating the domains of access control models and business process models empowers the enforcement of business process operation control [8], in specific, the business process compliance.

Business process compliance is the operation that centers on asserting the business processes are compliant to the regulations, standards and internal policies of an organization[6]. The non-compliance of the business processes can be considered a threat to the organization since it can damage the production of valuables (products and services). For instance, by making them more expensive to produce. Business process compliance normally demands an event-based behavior modeling that orchestrates the communication between actors and used resources (*e.g.*, information, time). However, most of the business processes compliance solutions consider that ex-dure is fully known, which does not always happens, and leads to organizations having an incomplete vision of the process [4].

To contribute with a solution for this problem, we propose the enforcement of an authorization approach based on access control models: integrate Attribute-Based Access Control (ABAC), and Role-Based Access Control (RBAC) with the specification of the BPMN [13], this way creating an expansion of the BPMN language. This will allow the specification of organization policies related to the 'who can do what' within the organizations' business process models; and the prevention of the non-compliance behavior by the actors involved in the tasks of the business processes.

1.1. Objectives

The organizational activity can be divided into three intervals in time: the ex-ante, the ex-dure, and the ex-post. Each of these intervals focuses on a particular phase of the business processes. The ex-ante is centered on what happens before the process starts functioning (i.e., this interval centers on the process modeling). This phase enables a common understanding and analysis of the business process. Hence, it is important to model correctly the business processes[1]. The next interval is the ex-dure and occurs during the execution of the business process. This interval has the objective of supporting the operation directly from the ex-ante model's definition. During this interval is where the mistakes and non-compliance can occur if the process is not clear and understood by the actors. Lastly, the ex-post focuses on what is going to happen after the execution of the process. In other words, the goal of the ex-post interval is to estimate the future behavior of the process from the available data from the past executions [7].

This thesis centers on the ex-ante. The main objective is to solve the problem of representing and operating exactly what was assigned to the actors of the organizations, to avoid non-compliance situations of the business processes and produce damage to the production of products and services of the organizations.

Therefore, the contributions of this work are the following:

- Propose a solution for representing resource policies in business processes.

- Integrate access control models in the BPMN meta-model.

- Implement the previous point in the Atlas project, a Link Consulting's tool[1] for modeling. However, because of Atlas not allowing inheritance relations between classes, an interpretation of the meta-model needs to be done first.

- Develop a tool for checking the correctness of business process and giving a system based on queries, that prevents the actors of executing business process instances that are non-compliant by using the concept *need-to-know* (i.e., allow actors to only be able to access the information that is his relevant to them).

- Apply the Rent-a-Car case study's business process to the presented solution to solve the problems that the organization is having based on the ex-post information; and show the obtained results.

Hence, the first part of the solution is related to the ex-ante interval since it refers to the modeling of the business processes, and the second part provides the tool that aims to support the actors during the execution. So, while the modeling of the business processes with access control models provides the distribution of the process' activities within the actors of the process and creates the set of logically related tasks and behaviors that organizations develop over time to produce specific business results [12]; the tool with the query system in combination with the diagram helps the actors comply to the process, and maintain a good process behavior, by showing them only the tasks that they what was assign to them in a given business process.

1.2. Organization of the Document

This work is organized as following. Section 2 presents the related works. Subsequently, section 3 designs the solution to integrate RBAC and ABAC with BPMN using Atlas, and the tool for checking business process along with a query system. Afterwards, section 4 the results of applying the solution to a business process. Finally, section 5 concludes the extended abstract, reflecting on the solution, and points to future work.

2. Related Work

In this chapter, a review of the literature on the subject is presented. It is centered on topics such as Business Process Compliance, Business Process, and Access Control Model Integration, giving special attention to the Role-based access control Model and Attribute-based access control model because they are the models used in this work. For that matter combinations of these keywords were searched in the following libraries: Google Scholar[2], in all the AIS eLibrary's repositories[3], and ACM Digital Library[4].

From the papers, it can be extracted, that there is a separation between business processes and security requirements, such as access controls. Mainly because the modeling languages, such as BPMN, were created to represent the flow, and the coordination of the business process when modeled. Thus, they do not have a representation of these types of requirements. Figure 1 shows an overview of the features of these papers. The

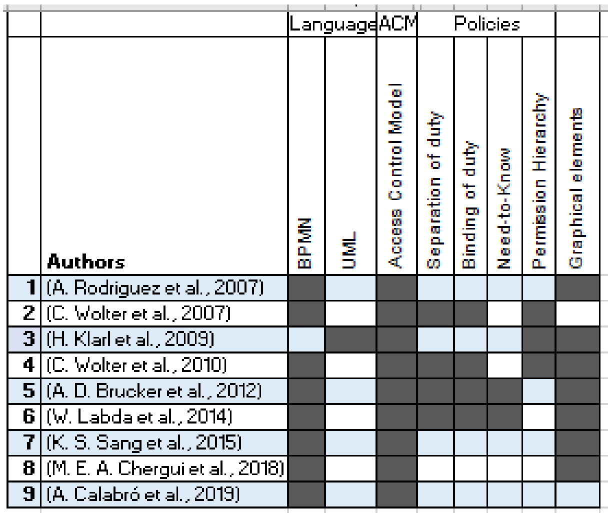
[1] www.linkconsulting.com/atlas/

[2] scholar.google.com/

[3] aisel.aisnet.org/

[4] dl.acm.org/

grey cells indicate the languages, access control model, policies, and other properties that each paper contains and solves (e.g., for A.Rodriguez et al., 2007 the paper uses BPMN, contains access control models in the solution, and uses graphical elements). The first two columns indicate the chosen language for implementing the solution. The following column indicates, if it is being use any access control mechanism in the paper. The next three columns indicate if the paper solves these security requirements with the solution presented. Lastly, the column *Graphical elements* points out if visual elements were added to the expansion of the language used in the solution.



		Language		ACM	Policies				
	Authors	BPMN	UML	Access Control Model	Separation of duty	Binding of duty	Need-to-Know	Permission Hierarchy	Graphical elements
1	(A. Rodriguez et al., 2007)	■		■					■
2	(C. Wolter et al., 2007)	■		■	■	■		■	
3	(H. Klarl et al., 2009)		■	■				■	■
4	(C. Wolter et al., 2010)	■		■	■	■		■	■
5	(A. D. Brucker et al., 2012)	■		■	■	■	■		■
6	(W. Labda et al., 2014)	■		■	■	■	■		■
7	(K. S. Sang et al., 2015)	■		■					■
8	(M. E. A. Chergui et al., 2018)	■		■					■
9	(A. Calabró et al., 2019)	■		■					

Figure 1: Overview of the related work

As it can be seen by the table the integration of security requirements, such as access control models, is an area of research relevant, since papers about the topic have been written and published from 2007 to 2019. Regarding access control models, the predominance of the papers only implements models based on roles, which limits the level of expressiveness in terms of organizational policies. The papers that also implement models based on attributes (i.e., they use ABAC) and explicitly say it are, [2] that applies ABAC in the specific context of General Data Protection Regulation (GDPR) compliance, using the advantage of Extensible Access Control Markup Language (XACML) to define ABAC policies. Lastly, [14], uses graphical elements for the representation of policies based on roles and attributes, being later applied to activities. However, the ABAC policies have a focus on representing the requirements of separation and binding of duty and because they are directly applied in activities and data objects this forces the definition of an ABAC policy in each activity, which withdraws the activity categorization that lanes do. Concerning graphical elements, most of the papers use extended visual representations for representing the needed requirements, however, this can obstructs the integration of the approaches in already existing business process modeling tools [3].

In conclusion, there are different proposed solutions for integrating security requirements into business processes, and each of them does it with an objective in mind, that go from a need to represent security requirements in BPMN; a need to represent identity management requirements in business process for service-oriented architectures; and also a need for a solution for compliance of the GDPR. Thus, the topic has a variety of areas of use and is still a relevant, as can be seen by the years of publications of papers in figure 1. In the developed solution of this work, BPMN is used as the language to expand and integrate access control models and to implement topics introduced by the papers, such as role hierarchies or the concept of the 'need-to-know'. The models chosen for the solution are RBAC, and ABAC, which contribute by giving more simplicity or more flexibility for representing organizational policies, respectively. Lastly, a tool was developed to check the business processes modeled regarding a set of rules defined by the expansion of the language; and give a query system that will provide actors a checklist that combine with the business process diagram will prevent non-complying behaviors related to the resource's policies of the organizations.

3. Solution

3.1. Theoretical Approach: BPMN Meta-model

Business processes are defined as a collection of inter-related events, activities, and decision points that involve several actors [5]. BPMN provides a graphical representation of the coordination and flow of business processes easy to understand by modelers and other viewers [15]. When extending the language it is important not to change the footprint of any existing flow element, such as events, activities, and gateways [15]. In other works, such as the ones presented in the previous section, some of the solutions consisted of adding new elements to represent security requirements, for instance, by adding symbols or using other visual elements to indicate the roles of RBAC models. The solution created in this work does not add new visual elements to represent access control models. However, new information will be added to BPMN elements that already existed. This was done because Atlas does not allow the creation of new visual elements and also with the objective of not interfering with the graphical representation of the language.

Figure 2, represents an interpretation of the BPMN meta-model with the extension to accept access control models. The green-colored entities in the diagram are the new elements added to the BPMN model. These correspond to the classes related to the access controls and do not have a visual representation when modeling. The idea behind it was to use the concept of Lane and enlarge his meaning. Lanes are partitions used to organize and categorize activities, normally representing internal roles or departments [13]. When lanes are defined in BPMN, they represent participants within the business process and "each of these participants is shown as a separate lane containing the activities performed by the participant in question" [5]. If the meaning of lanes is enlarge with the information provided by access control models, we will be able to define the what was assigned to each of the participants as well as the required permissions to access. Hence, in this thesis access control models are consider a type of lane where a permission is defined to access to the activities of the lane.

Concerning these permissions, notice that these have associated business functions, which represent lower-level activities in which there is a privilege, and that there are two types of permissions. This is because RBAC only needs to know about the roles of the actors that can allocate the tasks, and ABAC not only can accept roles, but also other information about the subject, the object, or the environment, allowing a finer level of granularity and create policies that are combinations of attributes [11]. The attributes considered for the ABAC model in this case were based from the National Institute of Standards and Technology's (NIST)[5]. These are:

- **Subject**:
  - **Certification:** Indicates official documents that the person has achieve.
  - **Division:** Indicates the departments or groups where the person belongs to.
  - **Email:** Indicates the different emails of a person.
  - **Training:** Indicates the skills that a person has.
  - **Role:** Indicates the different positions that a person has in a organization.
- **Object**:
  - **Project:** Indicates the projects that a person is involve in.
- **Environment**:
  - **Location:** Indicates the places where a person works.

Lastly, because events correspond to things that happen atomically, that is, they have no duration [5], and gateways have the objective of controlling the flow of the process through sequence flows [13]. They were not considered to have anything relevant to the access control models and solution, other than for modeling the processes.

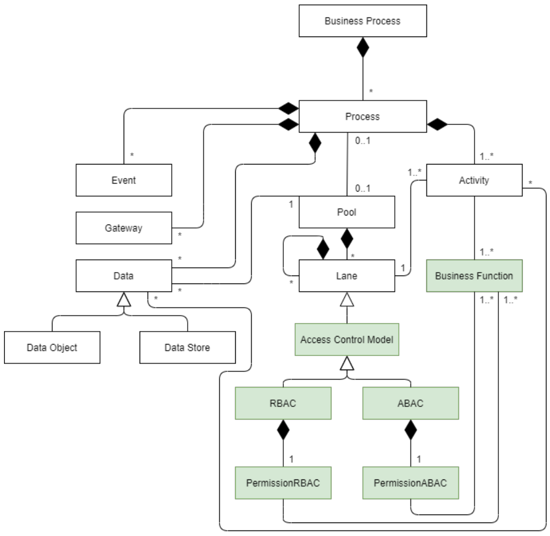


Figure 2: BPMN meta-model's expansion with access control models

3.2. Atlas: Metal-model Implementation

The developed solution consists of implementing the meta-model presented using the Atlas project and developing a tool that counts with a part for checking processes that use this new BPMN framework and with a query system to answer questions about the processes.

Atlas is a project that aims to endow organizations with a bigger capacity for managing and planning their IT. It is a solution for simplifying the process of creating and sustaining the IT architecture of the organizations. The functionalities of this tool used for this work are related to the modeling of business processes using BPMN and the Rest API that Atlas has. Atlas is powered by bpmn.io (bpmn.io/), a tool that allows the visualization and easy creation and edit of BPMN diagrams using BPMN 2.0.

Atlas functions all based on classes. The elements of the business process for Atlas are just instances of classes that are mapped to the BPMN elements. Therefore, for this work, two steps need to be done before modeling business processes. These are: create classes and objects, and map them to BPMN elements.

In terms of implementation, the meta-model is not exactly as represented in figure 2, because At-

[5] www.youtube.com/watch?v=cgTa7YnGfHA&feature=emb_title, Accessed = 03/11/2020

las does not have the inheritance relationship between classes. This caused the development of different approaches to better represent the relation, being the final result the figure 3. Because of this limitation of Atlas, what determines the type of access control model that is, are the permissions associated to the lane. If the lane is associated to a PermissionRBAC, then, the lane is RBAC; If the lane is associated to a PermissionABAC, then, the lane is ABAC.

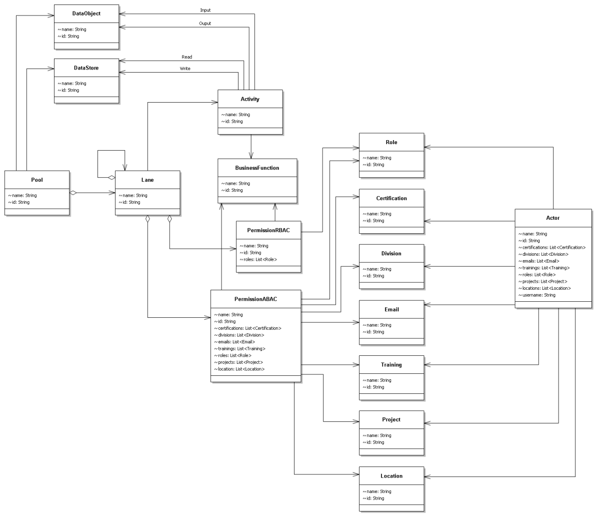


Figure 3: Class relation diagram in Atlas

3.3. Tool: Mapper, BusinessProcessChecker and Queries

The other part of this work consisted of the development of a tool using Java 1.8 for checking the business process and create a system based on queries that answered questions about the business processes that the actors of the process have, to help keep a correct behavior of the process.

The extension of the BPMN language caused the integration of new information to the already existing elements of the language. Therefore, it needs to be treated and given some more meaning. It was with this purpose that the tool was also developed. Figure 4 shows the relation between the classes of the created tool.

As it can be observed from the figure, there is a great part of the classes of the diagram equal to Atlas's class diagram from figure 3. The reason behind it, is that these classes are needed to map the information retrieved by the Atlas's API. The colored classes, on the other hand, are totally new and each one has a different objective and functionality. These are:

- **Manager:** This class has the goal of interacting with the other important modules (i.e., it manages all the operations). All the commands to execute are sent to the respective class through here, in order to be executed.
- **Mapper:** This class has the purpose of receiving the information of the Atlas API about a process modeled and creating the respective objects in Java.
- **BusinessProcessChecker:** Because there was created a BPMN framework, it is required to give meaning to everything new of the language. This resulted in the creation of rules. This class has the objective of verifying if these rules are respected in the business processes models that come from Atlas. These rules, if not satisfied, produce faults and warnings depending on the severity of the mistake. These rules are:
  - **Rules that produce faults:**
    - ⋆ A business function always must have at least one actor that can execute them.
    - ⋆ There must only be one permission per lane.
    - ⋆ If the lane is not parent-lane then it must have a permission.
    - ⋆ Every business function must be associated to a permission.
    - ⋆ The business function must be associated to a permission of the lane where his activity is modeled.
    - ⋆ Every data object and data store should be associated to the pool where they are modeled.
    - ⋆ An object lane that is parent-lane, must not have activities associated.
  - **Rules that produce Warning:**
    - ⋆ Data objects or data stores associated to a pool object should be used in the process.
- **Queries:** To implement the queries, a visitor pattern design, was used. The pattern allows easing the creation of queries when needed since it is only required to create a new class for a new query, and does not force to modify any part of the already created classes. The classes ShowAllProcessVisitor, ShowRelevantProcessVisitor, and ShowActivityVisitor represent each of the queries implemented.

4. Results

This sections centers in showing the results of the "**Show Business Process For Current User**" (i.e., ShowRelevantProcessVisitor class) and the "**Show Responsible For The Activity**" (i.e.,

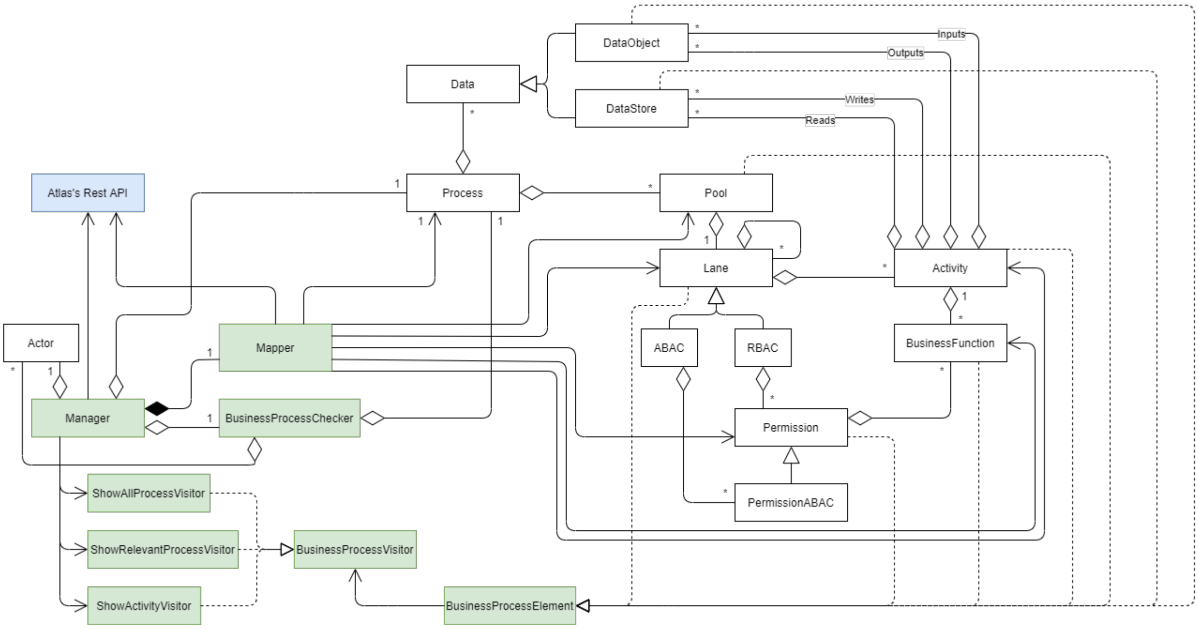


Figure 4: System's class diagram

ShowActivityVisitor class) queries for the *Rent-a-Car* business process of figure 5 adapted from the case study presented in [10]. The "**Business Process For Current User**" query, shows only the parts of the process relevant to the user that is logged in. When the query is executed, it uses the user's information and the permissions that each Atlas's lane has. Then it crosses the information, presenting only the activities (with their business functions) that the user has access to execute. Figure 6 shows the result for a user with the required permission of the lane Cars' Maintenance. The "**Show Actors of Activities**" query allows the user to search for activities to know the pool and lane where it is and the available actors that can execute his business functions. This query will be helpful when a determined activity is badly being executed. In these cases, there is a need to know as quickly as possible who are the actors responsible for the activity execution and correct it. An example of result is presented in figure 6.

5. Conclusions and Future Work

Today, business process models are the core elements of an organization and refer to how an organization is coordinated and how its work is organized to produce valuable products or services. When modeling business processes, policies that define the resources that can access and execute tasks or, informally speaking, with *' who can do what'*, are often not expressed. To solve this problem, we consider access control models as a way to offer the guarantee that only qualified users can gain access to tasks to execute them. To contribute with a solution for this problem, we propose the enforcement of an authorization approach based on access control models: integrate ABAC and RBAC with the specification of the BPMN, this way creating an BPMN framework. This will allow the specification of organizations' policies, related to resources, within the organizations' business process models, and prevention of the non-compliance behaviors by the actors involved in the tasks of the business processes.

Overall we believe that this line of work worth pursuing, and that what was develop in this work can be taken further in terms of the design of new control models to express better policies in BPMN, and in terms of more solutions for business process compliance. To improve the specification of policies, access control models that involve time should be implemented to represent policies, such as:

- "The car preparation team can only prepare cars at Depot from 9 am to 5 pm".

Regarding business process compliance solutions, queries that involve the sequence of tasks would be helpful for the actors too. A relevant query would be if given a name of an activity to the tool, let the actor know the next activity (as to the given as input) that they can execute. This is a helpful way for the actor to execute the process in more little steps. Lastly, all these queries (implemented in the work and the proposed in this section) could be implemented inside Atlas to allow a visual representation too. This way the actors would have a simplified version of the process with the parts that they are allow to execute with a visual representation.

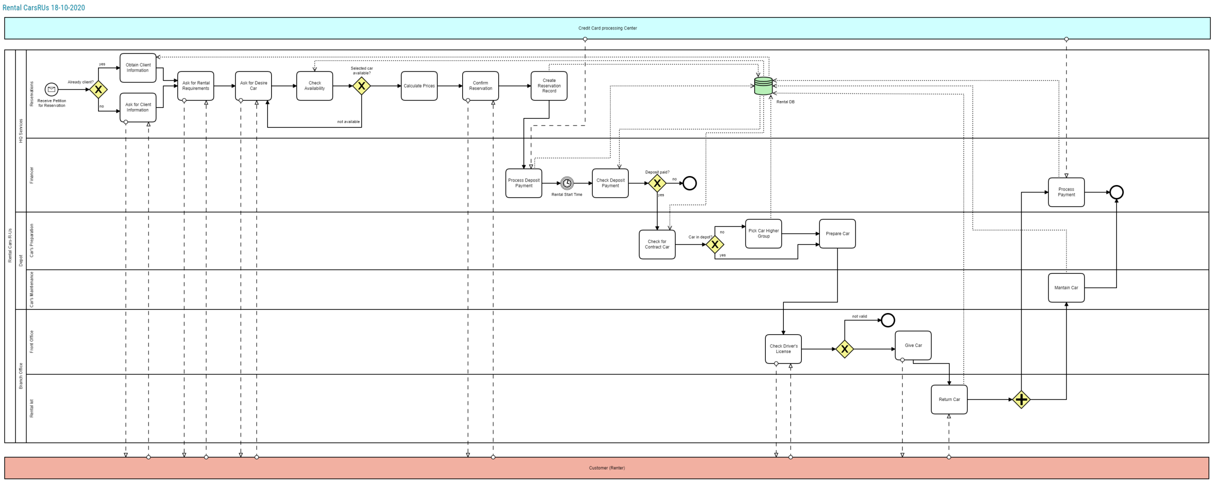
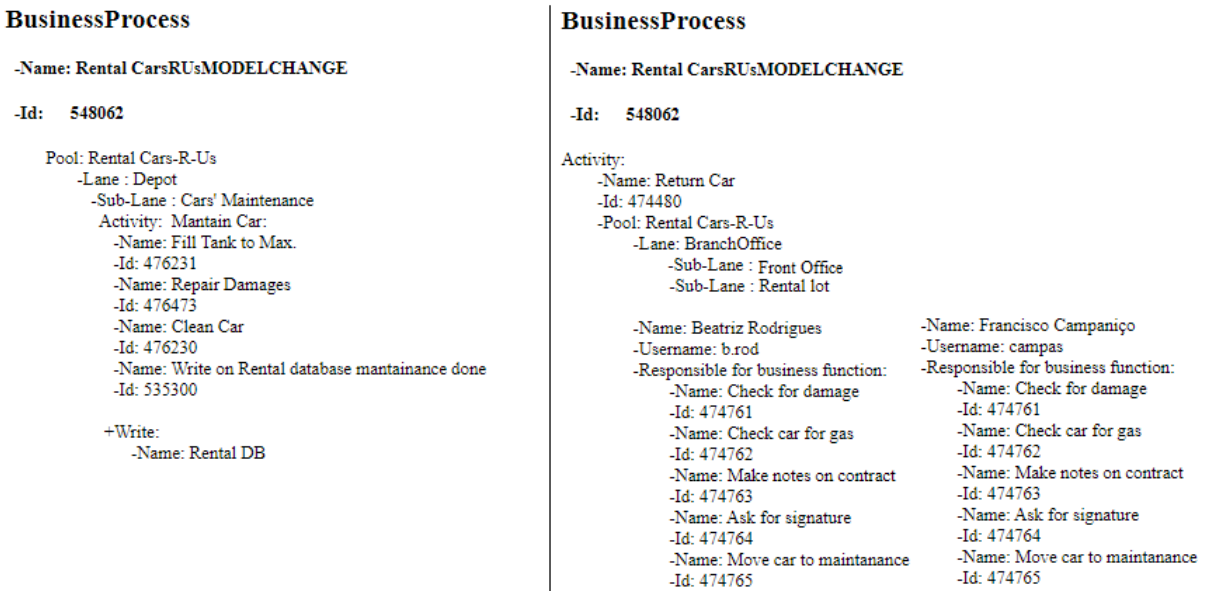


Figure 5: Rent-a-Car business process



BusinessProcess

-Name: Rental CarsRUsMODELCHANGE

-Id: 548062

Pool: Rental Cars-R-Us

-Lane : Depot

-Sub-Lane : Cars' Maintenance

Activity: Mantain Car:

-Name: Fill Tank to Max.

-Id: 476231

-Name: Repair Damages

-Id: 476473

-Name: Clean Car

-Id: 476230

-Name: Write on Rental database mantainance done

-Id: 535300

+Write:

-Name: Rental DB

BusinessProcess

-Name: Rental CarsRUsMODELCHANGE

-Id: 548062

Activity:

-Name: Return Car

-Id: 474480

-Pool: Rental Cars-R-Us

-Lane: BranchOffice

-Sub-Lane : Front Office

-Sub-Lane : Rental lot

-Name: Beatriz Rodrigues

-Username: b.rod

-Responsible for business function:

-Name: Check for damage

-Id: 474761

-Name: Check car for gas

-Id: 474762

-Name: Make notes on contract

-Id: 474763

-Name: Ask for signature

-Id: 474764

-Name: Move car to maintanance

-Id: 474765

-Name: Francisco Campaniço

-Username: campas

-Responsible for business function:

-Name: Check for damage

-Id: 474761

-Name: Check car for gas

-Id: 474762

-Name: Make notes on contract

-Id: 474763

-Name: Ask for signature

-Id: 474764

-Name: Move car to maintanance

-Id: 474765

Figure 6: "Show Business Process For Current User" result for "Paulo Alves" actor in *Rent-a-Car* business process (left) and "Show Actors of Activities" result for "Return Car" activity in *Rent-a-Car* business process (right)

References

[1] R. S. Aguilar-Saven. Business process modelling: Review and framework. *International Journal of production economics*, 90(2):129–149, 2004.

[2] A. Calabró, S. Daoudagh, and E. Marchetti. Integrating access control and business process for gdpr compliance: A preliminary study. In *ITASEC*, 2019.

[3] M. E. A. Chergui and S. M. Benslimane. A valid bpmn extension for supporting security requirements based on cyber security ontology. In *International Conference on Model and Data Engineering*, pages 219–232. Springer, 2018.

[4] I. E. da Silva. Conformidade dos processos de negócio: aplicação à modelação e operação de um processo de desenvolvimento de software. Master's thesis, Instituto Superior Técnico, 2019.

[5] M. Dumas, M. La Rosa, J. Mendling, and H. A. Reijers. *Fundamentals of business process management*, volume 1. Springer, 2017.

[6] A. Elgammal, S. Sebahi, O. Turetken, M.-S. Hacid, M. Papazoglou, and W. van den Heuvel. Business process compliance management : an integrated proactive approach. In K. Soliman, editor, *Proceedings of the 24th International Business Information Management Association Conference, 6-7 November 2014, Milan, Italy*, pages 764–781. International Business Information Management Association (IBIMA), 2014. conference; 24th International Business Information Manage-

ment Association Conference; 2014-11-06; 2014-11-07 ; Conference date: 06-11-2014 Through 07-11-2014.

[7] S. Guerreiro. Enterprise dynamic systems control enforcement of run-time business transactions using demo: principles of design and implementation. *Instituto Superior Técnico-Universidade Técnica de Lisboa, Lisboa*, 2012.

[8] S. Guerreiro. Conceptualizing on dynamically stable business processes operation: a literature review on existing concepts. *Business Process Management Journal*, 2020.

[9] S. L. Guerreiro. On ontology of integration between access control and business process deep structure. In *Novel Approaches to Information Systems Design*, pages 226–246. IGI Global, 2020.

[10] P. Harmon. *Business process change: a business process management guide for managers and process professionals*. Morgan Kaufmann, 2019.

[11] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, et al. Guide to attribute based access control (abac) definition and considerations (draft). *NIST special publication*, 800(162), 2013.

[12] K. C. Laudon and J. P. Laudon. *Management information systems*. Prentice Hall PTR, 1999.

[13] OMG. *Business Process Model and Notation (BPMN), Version 2.0.2*. Object Management Group, Dec. 2013.

[14] C. Wolter and C. Meinel. An approach to capture authorisation requirements in business processes. *Requirements engineering*, 15(4):359–373, 2010.

[15] C. Wolter and A. Schaad. Modeling of task-based authorization constraints in bpmn. In *International Conference on Business Process Management*, pages 64–79. Springer, 2007.