Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

Vol. 9, No 2

2010

doi:10.5329/RESI.2010.0902

Sumário

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente. Ela voltou a ser diagramada em uma única coluna para facilitar a leitura na tela do computador. Mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

(mapa de palavras com os termos mais frequentes nos artigos desta edição)

EVALUATING TOOLS FOR EXECUTION AND MANAGEMENT OF AUTHORIZATION BUSINESS RULES[1]

(paper submitted in October, 2010)

Leonardo Guerreiro Azevedo
Núcleo de Pesq. e Prática em Tecnologia
Departamento de Informática Aplicada
Univ. Federal do Estado do Rio de Janeiro
azevedo@uniriotec.br

Diego Alexandre Aranha Duarte
Núcleo de Pesq. e Prática em Tecnologia
Departamento de Informática Aplicada
Univ. Federal do Estado do Rio de Janeiro
diego.duarte@uniriotec.br

Fernanda Baião
Núcleo de Pesq. e Prática em Tecnologia
Departamento de Informática Aplicada
Univ. Federal do Estado do Rio de Janeiro
fernanda.baiao@uniriotec.br

Claudia Cappelli
Núcleo de Pesq. e Prática em Tecnologia
Departamento de Informática Aplicada
Univ. Federal do Estado do Rio de Janeiro
claudia.cappelli@uniriotec.br

ABSTRACT

Information security is an essential subject for commercial and government organizations, and its deployment should be supported by software tools, both at design time (when authorization business rules are planned and designed) and at run time (when authorization business rules are applied and monitored). An authorization business rule (or authorization rules, for short) is a rule that states which operations may be executed on each data item by each user. Therefore, *information security supporting tools should include features for editing, managing, and assuring the application and monitoring of authorization rules. These features may be structured in a framework composed by rule management and rule execution components. In real scenarios, evaluating and selecting tools to support organization business processes is typically handled by prospecting activities that are conducted in an ad-hoc way, and therefore are very time-consuming and hard to track. However, the rapid evolution of business scenarios, the increasing demand for traceability in business-IT alignment and the great number of IT solutions available for being evaluated require prospecting activities to be more systematic, traceable and quickly adapted to different scenarios. This work proposes a set of criteria and a systematic method for evaluating tools for management and execution of authorization rules. We have applied our approach in a real scenario. The results demonstrated that BRMS (Business Rule Management Systems) tools can be used for authorization rule management, and Oracle DBMS is the most suitable tool for authorization rules storage and execution.*

Key-words: business rules; authorization rules; business rule management systems; IT enterprise architecture; tool evaluation.

RESUMO

Segurança da informação é um tópico essencial para organizações privadas e governamentais e sua disponibilização deve ser apoiada por ferramentas de software, tanto em tempo de projeto (quando regras de negócio de autorização são planejadas e projetadas) como em tempo de execução (quando regras de negócio de autorização são aplicadas e monitoradas). Uma regra de negócio de autorização (ou regra de autorização, de forma resumida) é uma regra que afirma quais operações podem ser executadas em cada item de dado por cada usuário. Portanto, ferramentas para apoiar a segurança da informação devem incluir características como edição, gestão, e garantir a aplicação e monitoramento de regras de autorização. Estas características podem ser estruturadas em um framework composto por componentes de gestão e execução de regras. Em cenários reais, avaliar e selecionar ferramentas para apoiar processos de negócio da organização é em geral tratado por atividades de prospecção que são conduzidas de uma forma ad-hoc, e portanto consomem muito tempo e são difíceis de serem rastreadas. Entretanto, a evolução rápida de cenários do negócio, a demanda crescente de rastreabilidade para alinhamento do negócio e TI e o grande número de soluções de TI disponíveis para serem avaliadas requerem atividades de prospecção mais sistemáticas, rastreabilidade e rápida adaptação a diferentes cenários. Este trabalho propõe um conjunto de critérios e um método sistemático para avaliação de ferramentas para gestão e execução de regras de autorização. Nós aplicamos nossa abordagem em um cenário real. Os resultados demonstraram que ferramentas BRMS (Business Rule Management Systems) podem ser usadas para gestão de regras de autorização, e que o SGBD Oracle, dentre as ferramentas analisadas, é a ferramenta mais adequada para armazenamento e execução de regras de autorização.

Palavras-chave: regras de negócio; regras de autorização; sistemas de gestão de regras de negócio; arquitetura de TI da empresa; avaliação de ferramentas.

[1] The authors thank TIC/TIC-E&P/GDIEP (PETROBRAS) for supporting this work.

1 INTRODUCTION

Information security has been receiving increasing attention from academic researchers, industry and government institutions, since the unauthorized access to confidential information may lead to serious financial or legal problems and impact on business goals achievement in organizations.

Information security is defined as the preservation of three foundational qualities: confidentiality, integrity and availability of information (ISO, 2005). Data confidentiality is handled by data access control mechanisms (SANDHU *et al.*, 1996; YANG, 2009; CALI & MARTINENGHI, 2008; MURTHY & SEDLAR, 2007), which assure that a special type of business rules, named action assertion authorization, are applied.

A business rule is a statement that defines or constrains some aspect of the business, and it is intended to assert business structure or to control or influence the behavior of the business (BRG, 2009). In particular, one of the categories of business rules is the authorization action assertion (hereafter named authorization rule). An authorization rule specifies who is allowed to perform a certain action in an organization (including data manipulation actions). The definition and control of who may have access to each piece of information is vital to prevent frauds and to conduct controlling initiatives.

Deitert and McCoy (2007) point to the adoption of supporting tools for business rules management and execution, due to the increasing belief that business rules should not be embedded into applications and documents but, rather, explicitly presented as reusable artifacts. Traditionally named Business Rule Engines (BRE), those tools comprised an environment for rule development and an execution engine. More recently, with the increasing adoption of business rule management by organizations and their demand for handling more complex business rules, new features were added and the so-called BRE evolved to Business Rule Management Systems (BRMS). According to Deitert and McCoy (2007), the architecture of a BRMS is composed by the following components: execution engine; repository; integrated development engine (IDE); simulation model; rule analysis and monitoring; rule management and administration; rule *templates*. The works of Sinur (2005) and Rymer and Gualtieri (2008) present evaluation results of several BRMS available.

Prospection and evaluation of software tools in organizations are typically conducted as part of IT Enterprise Architecture initiatives (BOTTO, 2004). Those activities are required when organizations need to select new software tools to support business processes. Ideally, the evaluation and selection of software tools should be based on pre-defined technical criteria, and each criterion should have a fixed score interval and weight, reflecting its importance to the final evaluation. BRMS evaluations conducted by Sinur (2005) and Rymer and Gualtieri (2008) contribute to the initial step of tool searching. However, to effectively select a tool

doi:10.5329/RESI.2010.0902009

which meets organizational specific requirements, a set of more detailed and specific criteria is required.

The present work focuses on the evaluation of BRMS tools for authorization rules management and execution. We defined a set of criteria and applied authorization rules to control access to databases. We report the results of a broad and detailed evaluation of several BRMS tools available, showing that most of the existing BRMS tools address structural business rules (terms and facts), derivations and action assertions (BRG, 2009); however, they do not handle action assertions authorization rules appropriately. On the other hand, we concluded that authorization rules execution is the focus of typical DBMS (Database Management Systems) products (Oracle, Sybase, SQL Server) (YANG, 2009), which do not present an adequate interface for authorization rules management.

The remainder of this work is structured as follows. Section 2 characterizes mechanisms for the execution of authorization rules. Section 3 presents our proposal of criteria for BRMS tool evaluation. Section 4 presents the detailed questions used in the evaluation and the results of the evaluation of several BRMS tools according to the proposed criteria. Finally, Section 5 concludes the work and points to future directions.

2 MECHANISM FOR ACCESS CONTROL

The mechanisms for access control can be classified into: DAC (Discricionary Access Control), MAC (Mandatory Access Control), both proposed by DoD (1983), and more recently RBAC (Role-Based Access Control) (FERRAIOLO; KHUN, 1992).

The DAC mechanism restricts the access to objects based on identity of users and/or groups to which they belong. Yang (2009) presents that DAC policies do not enforce any control on the flow of information, thus making it possible for processes to leak information to users not allowed to read it. MAC policies, also known as label security, are based on mandated regulations determined by a central authority (YANG, 2009). The most common form of MAC is the multilevel security policy using classification of subjects (users and groups) and objects (data) of the systems. MAC policy controls the flow of information; however, it does not address actions that subjects are allowed to execute over data (FERRAIOLO; KHUN, 1992). Besides, since a label is attached to each data instance, management and maintenance costs may be high, and not so flexible, if many policies are applied. For RBAC, the access control considers functions and information. In this case, the main interest is to protect the information integrity: *who* is allowed to perform which *actions* over which *information* (FERRAIOLO; KHUN, 1992). Ferraiolo *et al.* (2001) propose a pattern for RBAC in order to consolidate different RBAC reference models, commercial products and research prototypes.

The access control mechanisms are implemented in different Database Management Systems (DBMS), as Oracle, Sybase and Microsoft SQL-Server

(YANG, 2009). After analyzing these tools, we observed that the implementations are more focused to handle the execution of authorization rules than the management of the rules. The definition of these rules requires a deep knowledge of database concepts (SQL and storage procedures), thus the authoring, edition and maintenance by the business user is not the focus of these tools, and hence the database administrator should be in charge of these tasks. On these tools the authoring, composition, query and visualization of rules and their dependencies, versioning, validation, simulation of rule execution, and others features are not simple to be executed or are simply not supported. Therefore the execution of these functionalities by the business users is unfeasible, even being the users the ones most suited to perform it, considering their deep knowledge about the business and about the restrictions of information access.

On the other hand, BRMS are developed to make the authoring, management and maintenance of the business rules possible to be executed by the business users, and also to allow the execution of business rules. Sinur (2005) analyzes the BRMS tools and characterizes the vendors as: leaders, visionaries, challengers or niche players. Rymer and Gualtieri (2008) present an analysis of the tools using some criteria and interviews with the vendors and customers of each platform. To help the selection between the platforms, they present five views of the business rules market: general-purpose platforms, specialized platforms, platforms for Java application developers, platforms for .NET application developers, and platforms for business analysts who develop and maintain applications. The tools were evaluated by the support of all business rule types defined by BRG (2009). However, they do not deal with the specificity of authorization rules appropriately, for example, the control of the rules at storaged data access time.

There is a set of tools focused on the authorization rules execution, while there is another set of tools that handle the management and execution of general business rules, but which does not deal with the specificity of authorization rules. So, for the first set of tools a module is necessary (or another tool) that makes authoring, edition, modification, versioning and deployment of authorization rules easier. On the other hand, the second set of tools must be carefully analyzed with the purpose of evaluating the potential of use for authorization rules.

For the tool evaluation, a framework that considers the two sets of tools must be applied. This paper applies a framework proposed by Azevedo *et al.* (2010) which divides the authorization rules in two modules: (i) authorization rule management (ARM) and (ii) authorization rule execution (ARE). The module ARM (Figure 1) is responsible for the authoring, modification, visualization, composition, tests and simulation of authorization rules. ARM allows the definition of access rules to the terms/concepts of the organization including the operations that could be executed for each existent profile. An example of rule is “The *local*

manager can *select* only the *orders* with *amount less than $ 1,000.00*". Every rule created in this module is stored in an authorization rule database.

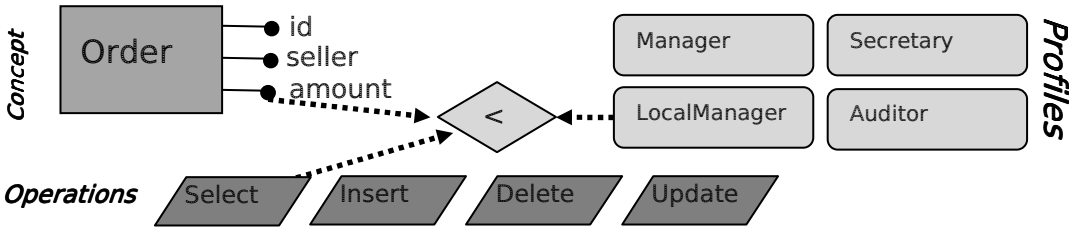

Figure 1 – Definition of authorization rule in a rule management tool
Source: Azevedo *et al.*, 2010

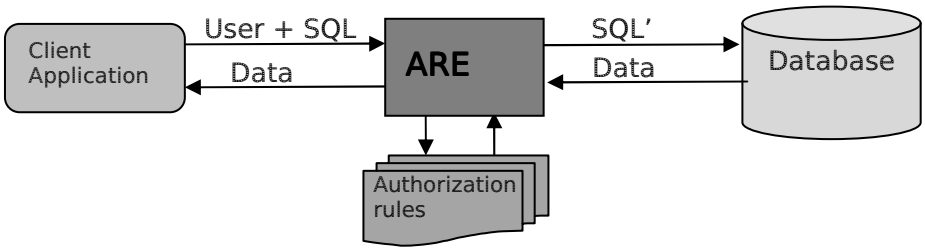

Figure 2 - Authorization rule execution tool
Source: Azevedo *et al.*, 2010

ARE module presented in Figure 2 is responsible to ensure that the defined authorization rules, stored in the rules database, are enforced. All operations (select, insert, delete and update) invoked by the business application over the corporative data are controlled at execution time.

3 CRITERIA FOR BRMS TOOL EVALUATION

As existent BRMS market tools have several components for managing and executing business rules, in this paper, we propose a set of criteria to evaluate specifically these tools for managing and executing authorization rules according to the framework proposed by Azevedo *et al*. (2010), presented in section 2.

The criteria were defined from questionnaires, as proposed by Tariq and Akhter (2005). These questionnaires identify the most important features in a tool according to the priorities of the organization. The criteria were developed based on different tools assessments (AZEVEDO *et al.*, 2008b), tools features listed from different works in academic community in this area (BRG 2009; BRCommunity 2000), and BRMS tools assessments (SINUR, 2005; RYMER & GUALTIERI, 2008). The criteria were evaluated and reviewed by experts and researchers. For each evaluation criterion, a scale score of 0 to 1 was defined, following the approach of Kitchenham (1996). The 0 (zero) means total absence or inadequacy of the criterion in the tool and 1 (one) means that the tool fully meets the criterion (tables 1 to 21). In order to define how a criterion should be

scored, we detailed an interval of values for each criterion. It is important to emphasize that, the way of scoring can vary from organization to organization, and, in this work, we followed the requirements of the organization where we conducted the BRMS evaluation. Also according to Kitchenham (1996), and according to organizations reality today, weights were defined for each group of criteria using a scale of 1 to 5, reflecting the importance of the final evaluation (Table 22). Weight 1 indicates an insignificant feature, weight 2 indicates a little importance feature, weight 3 indicates a useful feature, weight 4 indicates a desirable feature but not an essential feature, and weight 5 indicates an indispensable feature. This score can vary from organization to organization.

In this proposal, we extended Kitchenham's (1996) approach, and beyond the scale score and weights assigned to criteria, different weights were defined to evaluate the tool documentation (weight 1) and to evaluate the assessment criteria in the laboratory test (weight 2). Thus, for example, if the documentation assessment, according to a criterion, resulted in a score of 0.8 and the same criterion in the laboratory test resulted in a score of 0.6, then the final result would be equal to $(1 \times 0.8 + 1 \times 2 \times 0.6) / (1 + 2) = 0.67$.

From the existing features in market tools and from needs to better support authorization rules management and execution activities, the criteria were defined, evaluated and reviewed with experts and researchers.

The criteria were organized according to taxonomy of macro-criteria and were classified into generic and specific. Macro-generic criteria represent a set of criteria that can be used to assess any kind of tool, regardless of its application area. They can therefore be used for both: authorization rule management tool or authorization rule execution tool. Macro-specific criteria are applied specifically to the tools of the authorization area and were divided into specific criteria for management and specific criteria for execution tools.

Analyzing each macro-criterion, if we sum all scores of criteria, we will end up with a macro-criterion with many criteria having a higher weight than a macro-criterion with few criteria. So, doing the simple sum, we could result in a non-important criterion having a higher score than an important one. For example, the macro-criterion "Security" has six criteria, which could produces a maximum score of 6, while the macro-criteria "Rules Composition" has two criteria and could reach a maximum score of 2. However, according to BRMS experts' analysis, we observed that "Security" is not four times more important than "Rules Simulation". To avoid these problems, weights for each macro-criterion were defined. That was based on a deep analysis among researchers and experts, resulting in the content presented in Table 22. Thus, the calculation of the scoring is weighted under the weight assigned to each macro-criterion.

Table 1. Distribution

Generic Criteria - Distribution	
Criteria	**Score interval**
How new versions of the tool are distributed to customers?	0: Vendor's team executes the installation at the customer's site, and it takes more than one week 0.5: Vendor's team executes the installation at the customer's site, and it takes less than one week 0,5: CD, DVD 1: Internet
Is the vendor in an acquisition process by another company?	1: no 0: yes
Was the company acquired by another one recently?	0: t ≤ 2 years (company is less than 2 years old) 0,50: 2 years < t ≤ 5 years 1: t > 5 years or the company was not acquired by another company.
How many customers for the tool does the vendor have?	0: less than 20 customers 0.25: between 20 and 50 customers 0.5: between 50 and 100 customers 1: more than 100 customers
How old is the company?	0: less than 1 year 0.25: between 1 and 5 years 0.5: between 5 and 10 years 1: more than 10 years
When was released the first version of the BRMS tool?	0: less than 1 year ago 0.5: between 1 and 5 years ago 1: more than 5 years ago
Is the BRMS tool supplied as a single product?	0: no 1: yes
Do new versions of the tool support features of old versions?	

Table 2. Scalability

Generic Criteria - Scalability	
Criteria	**Score interval**
Maximum number of rules that can be created / executed.	0: < 1.000 0.5: >= 1.000 and < 10.000 1: >= 10.000
Maximum time for rule execution.	0: t > 0,25 s 0.5: 0,01 s ≤ t ≤ 0,25 s 1: t < 0,01 s

Table 3. Flexibility

Generic Criteria - Flexibility	
Criteria	**Score interval**
Is the tool flexible to include new features?	0: no 1: yes
What are the main requirements to implement new functionalities (program language and software requirements)	0: it is not possible to implement new functionalities to comply with customers' requirements 0.25: new requirements can be implemented, but customer must pay the development made by supplier's team 0.5: it is possible for the customer's development team to implement new functionalities. If it is needed, the supplier can support this work according to a contract between the customer and the supplier. 1: it is possible for the customer's development team to implement new functionalities, and the supplier supports this work without fees.
Is it possible to custom the tool according to customer requirements?	0: no 1: yes

Table 4. Integration with other systems

Generic Criteria - Integration with other systems	
Criteria	**Score interval**
Does the BRMS tool allow making an explicit relationship between rules and database elements, for example, tables, columns etc.?	0: no 1: yes
Does the BRMS tool have integration with business process modeling tool?	0: no 1: yes
Does the BRMS tool have integration with DBMS?	0: no 1: yes

Table 5. Operational Systems

Generic Criteria - Operational System	
Criteria	**Score interval**
Is it possible to install the tool in Linux?	0: no 1: yes
Is it possible to install the tool in Windows?	0: no 1: yes

Table 6. Quality of Documentation

Generic Criteria - Quality of Documentation	
Criteria	**Score interval**
Is the documentation clear about tool's goals and architecture?	0: no 1: yes
Is the documentation clear about tool's setup and configuration?	0: no 1: yes
Is the documentation clear about tool functionalities?	0: no 1: yes
Are there tutorials explaining tool functionalities?	0: no 1: yes
Does the documentation present scalabilities and performance test results?	0: no 1: yes
Is there a forum to discuss topics about the tool? Is the forum used very often?	0: there is no forum or it exists but has a volume of less than 10 messages per week. 1: the forum is frequently used.

Table 7. Support

Generic Criteria - Support	
Criteria	**Score interval**
Is there support available for new versions of the tool?	0: no 1: yes
Is the documentation clear about tool's setup and configuration?	0: no 1: yes
Is there support available by email?	0: no 1: yes
Is there support available by telephone?	0: no 1: yes
Is there support available *in loco*?	0: no 1: yes

Table 8. Rule Edition

Management Specific Criteria - Rule edition	
Criteria	**Score interval**
Can multiple users edit rules simultaneously?	0: concurrent users < 10 0.5: 10 ≤ concurrent users ≤ 20 1: concurrent users > 20
Does the tool have an IDE (Integrated Development Environment) to create, edit and view rules, for versioning control etc.?	0: no 1: yes
Does the tool allow including, changing and deleting elements of the rule?	0: no 1: yes
Does the tool detect conflicts between rules during rule edition?	0: no 1: yes
Is it possible to build a vocabulary or data dictionary	0: no 1: yes

in order to describe business entities, terms, attributes, relationships between concepts?	
Does the tool use a business rule language to create rules? Which one?	0: the tool does not have a language for rules. 0.5: the tool has a proprietary business rule language 1.0: the tool allows writing rules in a non-proprietary language.
Is it possible to create/import users from an existing database and relate them to rules?	0: the tool allows rule management, but does not allow user management and management of their relationship with rules. 0.25: the tool allows to create users and groups/roles and relate them to rules. 0.75: the tool allows to import user information from corporative user database, to create groups/roles and to relate them to rules. 1: the tool allows to relate users from corporative user database and rules without the need to import the information.
Rule elements can be created using a graphical interface?	0: no 1: yes
What types of business rules does the tool support according to Business Rule Group?	0: the tool does not support any type of rule defined by (BRG, 2000) 1: the tool supports at least the following rule types: rule terms definition, relationship definition and authorization (BRG, 2000)
Are there templates for rule creation?	0: no, there are no templates and it is not possible to develop templates 0.25: there are templates, but it is not possible to customize them. 0,5: it is possible to develop templates. 1: it is possible to develop templates and there are templates installed with the tool as well.
Are there wizards for rule creation?	0: no, there are no wizards and it is not possible to develop wizards. 0.25: there are wizards for rules which define business entities. 0.5: there are wizards for rules which define business entities and relationships. 0.75: there are wizards for rules which define business entities, relationships and restrictions. 1: there are wizards for the four business rule types defined by BRG.
Is it possible to develop new wizards?	0: no 1: yes
Is it possible to change rules using an API?	0: no 1: yes or the business rule management and business rule execution correspond to a single tool and an integration API is not required.

Table 9. Query rules

Management Specific Criteria - Query rules	
Criteria	**Score interval**
Is it possible to query rules using rule query languages?	0: no, it is not possible to query rules using rule query language. 0,5: yes, but only using a proprietary language. 1: yes, using non-proprietary language as well as the proprietary language.
Is it possible to execute domain-specific queries?	0: no, it is not possible to execute a query in a specific domain. 0.25: yes, but only in a specific project. 0.5: yes, it is possible to execute a query in a specific rule project and considering entities (for example, rules which includes one or more terms). 1: yes, it is possible to execute a query in a specific rule project or considering entities (for example, rules which includes one or more terms) or in a specific domain.
Does tool have an inference mechanism?	0: no 1: yes
Is it possible to use the inference mechanism in queries?	0: no 1: yes
Is it possible to create explanations, in natural language, to explain the inference generated in rule execution?	0: no 1: yes
Is it possible to generate reports including results of queries?	0: no 0.5: yes, but it is only possible to execute prebuilt reports. 1: yes, it is possible to generate a report from query results.
Is it possible to query rules through an API?	0: no 1: yes or the business rule management and business rule execution correspond to a single tool and an integration API is not required.
Is it possible to generate reports from data dictionary (or vocabulary) used in rules?	0: no 0.5: yes, but it is only possible to execute prebuilt reports. 1: yes, it is possible to generate a report from query results over the data dictionary.

Table 10. Rule viewing

Management Specific Criteria - Rule viewing	
Criteria	**Score interval**
Does the tool have a graphical interface for rules viewing and browsing?	0: no, there is no graphical interface for rule viewing 0.5: it is only possible to view the text of the rules. 1: it is possible to view the text of the rules as well as view the rules in graphical interface. Besides, dependencies between rules are presented in a graph of dependencies.

Is it possible to access rule properties when viewing the rule in the graphical interface?	0: no 1: yes
Is it possible to print rule view?	0: no 1: yes
Is it possible to generate a report considering rule view?	0: no 1: yes
Is there support available for new versions of the tool?	0: no 1: yes or the business rule management and business rule execution correspond to a single tool and an integration API is not required.

Table 11. Import/Export

Management Specific Criteria - Import/Export	
Criteria	**Score interval**
Does the tool allow converting rules from one format to another one?	0: no 1: yes
Is it possible to import and export rules in different rule representation formats?	0: no 1: yes
Does the tool allow discovering rules automatically?	0: no 1: yes

Table 12. Rule repository and versioning

Management Specific Criteria - Rule repository and versioning	
Criteria	**Score interval**
Is it possible to store rule versions?	0: no 1: yes
Is it possible to compare and merge different version of rules?	0: no, it is not possible to compare and merge rules. 0.5: yes, but it is only possible to compare versions of rules, not to merge rules. 1: yes, it is possible to compare and merge different versions of rules.
Is it possible to detect collisions and/or inconsistencies between rule versions?	0: no 1: yes
Is the version control on rule level (not file-based)?	0: no 1: yes
Is it possible to have a distributed rule repository?	0: no 1: yes
Is it possible to extend the repository metamodel?	0: no, it is not possible to extend the repository metamodel. 0.25: yes, but it is only possible to extend attributes of metamodel. 0.75: yes, it is possible to extend attributes and relationships. 1: yes, it is possible to extend attributes, relationships and attributes of rule view.
Is the rule repository independent from rule execution component? For example, rule be stored in an external database.	0: no 1: yes
Is it possible to store history of rule changes?	0: no 1: yes

Table 13. Rule composition

Management Specific Criteria - Rule composition	
Criteria	**Score interval**
Is it possible to compose rules?	0: no 0.25: yes, but it is only possible to create a group of rules that must be valid for a group of actions to take place. 1: yes, it is possible to combine rules using some operators.
Is it possible to define exception rules?	0: no 1: yes

Table 14. Rule validation

Management Specific Criteria - Rule validation	
Criteria	**Score interval**
Are there tools for testing and debugging?	0: no 1: yes
Is it possible to generate reports for rule validation?	0: no 1: yes
Is it possible to evaluate rule consistency? For example, to verify if rules are complete.	0: no 1: yes

Table 15. Rule simulation

Management Specific Criteria - Rule simulation	
Criteria	**Score interval**
Is there a model for rule simulation?	0: no 1: yes
Is there a graphical tool to view the sequence of rule execution and dependencies?	0: no 1: yes
Is it possible to simulate rule execution using new data as well as old datasets?	0: no 1: yes

Table 16. Security

Management Specific Criteria - Security	
Criteria	**Score interval**
Is it possible to create user accounts?	0: no 1: yes
Does the tool provide concurrency control?	0: no 1: yes
Is it possible to create roles for rule management access?	0: no 1: yes
Is it possible to associate roles to users stored at a corporative database?	0: no 1: yes
Is it possible to define rule permissions accordingly with rule types?	0: no 1: yes
Does the tool control user access to rule's elements?	0: no 1: yes

Table 17. Quality of rules

Management Specific Criteria - Quality of rules	
Criteria	**Score interval**
Is it possible to define organization patterns to describe rules? For example, pattern for rule names.	0: no 0.5: yes, extending rule elements. 1: yes, it is possible to define patterns to handle rule elements.
Is it possible to verify if rules comply with organization patterns?	0: no 1: yes

Table 18. Management

Management Specific Criteria - Management	
Criteria	**Score interval**
Does the tool have functionalities to deploy rules in different environments (for example, development, test and production environments)?	0: no 1: yes
Does the tool allow promoting rules to environments (development, test, staging and production)?	0: no 1: yes

Table 19. Rule execution

Execution Specific Criteria - Rule execution	
Criteria	**Score interval**
What is the transparency level for client applications in order to use the rule execution tool?	0: changes in the application source code are required. 0.5: changes in the application database connection properties (ODBC or JDB connection) are required. 0.75: changes in the application code are required only to modify the costumer user that is logged on the application. 1: no change is required.
Are there code generation functionalities (to other programming languages)?	0: no 1: yes
Is it possible to invoke rules using web services technology?	0: no 1: yes
Can the rule be executed for a specific user/role?	0: rules are executed independently from the user or role that is executing the rule. 0.25: the user is considered during rule execution. 1: the roles to which the user is associated with are considered during rule execution.
Does the tool allow executing different modes of execution (dynamic/static)?	0: no 1: yes

Table 20. Management of execution environment

Execution Specific Criteria - Management of execution environment	
Criteria	**Score interval**
Is it possible to monitor and trace rule execution in the rule engine? (For example, how long did it take to execute a rule?; what was the data handled by the tool and what was the result?; logging?; etc.)	0: no 1: yes
Is it possible to monitor server performance? (For example, if the server is overloaded; used memory etc.)	0: no 1: yes

Table 21. Audit

Execution Specific Criteria - Audit	
Criteria	**Score interval**
Is it possible to query the execution log?	0: no 1: yes
Is it possible to view the log in a graphic interface?	0: no 1: yes
Are there wizards to create reports for rule impact analysis?	0: no 1: yes
Is it possible to verify the relationship between user roles and rules which are in the production environment?	0: no 1: yes
Does the tool store history of rule x role association, and does it allow querying this information?	0: no 1: yes

Table 22. Weights for each kind of criterion

M.	Criteria	Weight
Generic	Scalability	3
	Flexibility	3
	Integration with other systems	3
	Quality of documentation	3
	Support	3
	Operational System	2
	Distribution	1
Execution	Management of execution environment	5
	Rule execution	2
	Audit	2

M.	Criteria	Weight
Management	Rule edition	5
	Query rules	4
	Security	3
	Rule viewing	2
	Rule repository and versioning	2
	Rule composition	2
	Rule validation	2
	Rule simulation	2
	Import/export	2
	Quality of rules	1
	Management	1

4 AUTHORIZATION RULE TOOLS EVALUATION

In this section, BRMS tool evaluation is presented. The evaluation was conducted for the Information and Data Management department of E&P (Exploration and Production) (DGIEP) of Petrobras (TIC/TIC-E&P/GDIEP). The goal of the work was to choose the best tool to support management and execution of authorization rules. Petrobras is the largest Oil Company of Brazil. It is responsible for the majority of Oil and Gas derivatives exploration and production in the country. The Information and Data Management department of E&P (GDIEP) is responsible for information and data management in the oil and gas domain.

The process for tool evaluation used in this study was proposed by Azevedo *et al.* (2008a) (Figure 3). It corresponds to an adaptation of the process proposed by SEI (Software Engineering Institute) (COMELLA-DORA, 2004).

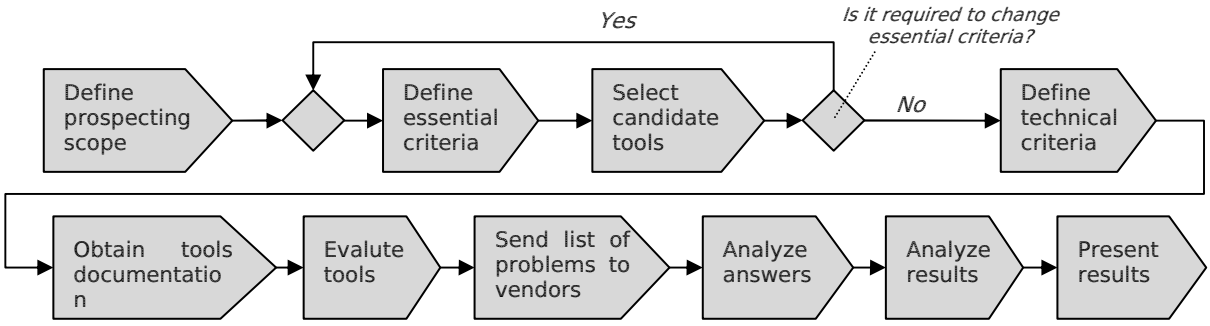

Figure 3 – Process for tool evaluation
Source: Azevedo *et al.*, 2008a

1. **Define prospecting scope:** the goal of tool prospecting was to identify a tool that supported GDIEP to perform management of authorization rules as well as execution of authorization rules.
2. **Define essential criteria:** criteria were defined according to type of tool. Criteria for tools for rule management are: (i) existence of user graphical interface for rule management; (ii) possibility of integration with rule execution tool; (iii) existence of support for the tool. Criteria for tools for rule execution are: (i) execution of authorization rules on data stored in Oracle DBMS with fewer changes on the existing architectures for data access; (ii) existence of support for the tool.
3. **Select candidate tools**: Candidate tools were identified from other BRMS evaluation works (SINUR, 2005; RYMER & GUALTIERI, 2008), BRMS tools listed by business rules communities (BRG, 2000; BRCommunity, 2000), and search on the Internet.

The following tools were selected for evaluation: Corticon Business Rules Management System[2]; ESI Logist[3]; FICO Blaze Advisor[4]; ILOG BRMS[5]; JBoss Enterprise BRMS[6]; RuleXpress[7]; SAP NetWeaver BRM[8]; Sapiens eMerge[9]; Ness Usoft[10]; Visual Rules[11]; G2 Plataform[12]; Versata BRMS[13]; PegaRules[14]; InRule[15]; Oracle Business Rules[16], ARIS Business Rule Designer[17].

Documentation available from tool vendors was analyzed in order to answer essential criteria (presented in step 2).

Almost all tools passed on essential criteria evaluation considering authorization rule management, while some of them passed on essential criteria evaluation related to authorization rule execution.

Since there were many tools to evaluate, in the next steps, and there was not enough time to do that in detail, essential criteria were changed in order to reduce the list of tools. In Figure 3, change in essential criteria corresponds to the decision point “Is it required to change essential criteria?”.

A new essential criterion was created: only tools that have good score in evaluations performed by Gartner and Forrester institutes was considered. These evaluations were presented by Sinur (2005) and Rymer e Gualtieri (2008).

After this change, the essential criteria evaluation was performed again and the following tools passed this test: WebSphere Ilog BRMS; InRule; Corticon; FICO Blaze Advisor; Usoft; ESI Logist.

Besides, the tools Oracle Business Rules and ARIS Business Rule Designer were also considered for the next evaluation steps even though they did not have a good score in Gartner and Forrester institutes evaluations. It was a choice of GDIEP to evaluate these tools. The reasons for that were: (i) the DBMS used by this department is Oracle DBMS, and GDIEP would like to evaluate if it was simple to

[2] http://www.corticon.com/Products/Business-Rules-Management-System.php
[3] http://www.esi-knowledge.com/products_logist.aspx
[4] http://www.fico.com/en/Products/DMTools/Pages/FICO-Blaze-Advisor-System.aspx
[5] http://www.ilog.com/products/businessrules/index.cfm
[6] http://www.jboss.com/products/platforms/brms/
[7] http://www.rulearts.com/RuleXpress
[8] http://www.sap.com/platform/netweaver/components/brm/index.epx
[9] http://www.sapiens.com/Dev2Go.Web?id=207028
[10] http://www.usoft.com
[11] http://www.visual-rules.com/business-rules-management-enterprise-decision-management.html
[12] http://www.gensym.com/index.php?option=com_content&view=article&id=47&Itemid=54
[13] http://www.versata.com/index2.php?option=com_content&task=view&id=124
[14] http://www.pega.com/Products/RulesTechnology.asp
[15] http://www.inrule.com/products/InRule.aspx
[16] http://www.oracle.com/technology/products/ias/business_rules/index.html
[17] http://www.ids-scheer.com/en/ARIS/ARIS_Platform/ARIS_Business_Rules_Designer/3747.html

integrate a management tool and an execution tool from the same vendor; and, (ii) ARIS Platform is used to model business processes, where there a lot of rules are modeled; therefore, GDIEP would like to evaluate if it was simple to migrate rules from business models to BRMS tool.

4. **Define technical criteria:** technical criteria used in the evaluation were presented in section 3.2. There were 29 general criteria, 60 criteria to evaluate tools related to rule management and 14 criteria for tools related to rule execution.
5. **Obtain tools documentation:** the evaluation team contacted the vendors and got manuals, tutorials, videos, data sheets, white paper and other documents to execute the evaluation.
6. **Evaluate tools:** tools were evaluated according to criteria defined in step 4, and presented in section 3.4 (Tables 1 to 21). The evaluation was executed by system analysts (called assessors). They were trained to execute the tool evaluation process and to use the defined criteria. All results produced by the assessors were reviewed by an expert in tool evaluation and in assessing the criteria. He was called Master Assessor. All comments resulting from the Master Assessor's revision were handled by Assessors.

   Macro-criteria (presented in Table 22) were prioritized by professionals of GDIEP.

   Three evaluations were conducted for each tool: evaluation using general criteria; evaluation using specific criteria for rule management; and evaluation using specific criteria for rule execution. Each of these evaluations was executed two times: (i) tool documentation: in this case, each criterion was assessed using only the documentation available from the vendor; and, (ii) laboratory (hands on evaluation): in this case, each criterion was assessed executing the tool.

   Since laboratory evaluation is more important than the documentation evaluation, results from the laboratory evaluation were assigned weight 2 and results from the documentation evaluation were assigned weight 1.

   Each evaluation was stored in a spreadsheet including the points for each criterion. Criteria that did not receive maximum value were justified, presenting the reasons, individually.
7. **Send list of problems to vendors:** any criteria that could not be answered using the documentation and laboratory evaluations was converted into a question and sent to vendors in order to get help.
8. **Analyze answers:** the answers to the problems identified during the evaluation returned from vendors were analyzed, and the results of evaluations were adjusted accordingly.
9. **Analyze results**: the complete analysis of evaluation results is presented below in Table 23. The table presents a percentage

doi:10.5329/RESI.2010.0902009

corresponding to the criteria values and the weight for each macro-criterion.

In some cases, there is a value "-" for the result. This value was assigned after a deep analysis of the tool which confirmed that the tool did not have an architecture that was suitable for that kind of tool. This analysis, in some cases, was executed using conference calls, meetings and emails including assessors and vendors technical team. This was the case of Ilog and Corticon, which do not comply with rule execution needs.

It is important to emphasize that some criteria did not receive a value because the vendor did not returned an answer for them. In those cases, a zero was assigned as the value for the criterion. Table 23 also presents the value that the tool would get if it received the maximum score for cases like that. These cases are highlighted using "()". For instance, Corticon comply with 68% of rule management criteria, but if the issues that did not get a response received maximum score, the evaluation result would be changed to 90%.

Table 23 – Final result

		ILOG	Corticon	FICO Blaze Advisor	InRule	USoft	ESI Logist	Oracle BR
General		80%	77%	66% (94%*)	32% (57%*)	47% (90%*)	48% (86%*)	47%
Management	Documentation	61%	68% (90%)	58% (88%*)	47% (51%*)	53% (83%*)	39% (70%*)	21%
	Laboratory	60%	-	47%	47%	-	37%	-
Total		**67%**	-					-
Execution	Documentation	-	23% (37%*)	46% (82%)	59% (62%*)	23% (95%)	43% (75%*)	-
	Laboratory	-	-	-	33%	-	-	-
Total		-	-					-

90% ≤ R < 100% | 80% ≤ R < 90% | 70% ≤ R < 80% | 60% ≤ R <70% | 50% ≤ R <60% | R ≤50%

10. **Presenting results:** the results were presented to GDIEP professionals that were part of the evaluation group. They were responsible to take the final decision. Two analyses where conducted about the presented results: qualitative and quantitative analysis.

    In the quantitative analysis, no tool complied with the requirements for authorization rule execution, and ILog complied in moderate level with requirements for authorization rule management.

    On the other hand, the qualitative analysis had the goal to make explicit weaknesses and strength of tools. In this case, no tool complied with specific criteria for management and execution at the same time. Related to management criteria, it is important to

emphasize that the main weaknesses were that storage format is proprietary and tools do not have features to relate enterprise users to rules. Considering management criteria, no tool complied with the requirements.

5 CONCLUSIONS

Information security is a very relevant research topic, which is gaining increasing attention both in commercial and in governmental organizations. In this context, preventing unauthorized access to confidential information is determinant. Authorization rules are a category of business rules that specifies who is allowed to perform a certain action in an organization.

BRMS are tools to support business rules management and execution. Sinur (2005) and Rymer and Gualtieri (2008) present evaluations of existing BRMS focusing on some business rule types (structural assertions – terms and facts, derivations and action assertions). Those evaluations do not address, however, authorization rules and their specificities, such as the support for dynamic control at run time, and the performance overhead on applications accessing corporative data sources.

This work proposed an evaluation approach for BRMS tools with regard to their support for authorization rules. The evaluation approach comprised taxonomy of evaluation criteria, a method for combining each criteria score to calculate the overall score, as well as an evaluation process involving a sequence of systematic steps. The evaluation approach was validated by specialists on the domain of information security and on tool evaluation.

The evaluated BRMS tools were selected from previous evaluations, literature research, and access to the most relevant players of the market. The evaluation results showed that most BRMS provide features for authorization rule management (editing, querying, visualization, versioning, concurrency control, and rule description at a high level of abstraction), but does not support authorization rules execution properly. Moreover, those tools focus on business rules categories other than authorization rules. Therefore, they should be considered for supporting business rule management, while rule storage and execution could be handled by DBMS.

Future works could include applying our evaluation approach to other scenarios.

REFERENCES

AZEVEDO, L. G.; LOPES, M.; SOUZA, J.; SIQUEIRA, S.; CAPPELLI, C.; BAIAO, F. A. Uma metodologia de avaliação de ferramentas para gestão de ontologias [A methodology for the evaluation of ontology management tools]. In: Seminário de Pesquisa em Ontologia no Brasil. Niterói. *Proceedings...*, Niterói, 2008a.

AZEVEDO, L. G.; LOPES, M.; SOUZA, J.; SIQUEIRA, S.; CAPPELLI, C.; BAIAO, F. A. *Inspeção de ferramentas de ontologias* [Inspection of ontology tools]. Relatório técnico 0003/2008, Departamento de Informática Aplicada da UNIRIO, Rio de Janeiro, 2008b.

AZEVEDO, L. G.; PUNTAR, S.; THIAGO, R.; BAIÃO, F.; CAPPELLI, C. A flexible framework for applying data access authorization business rules. In: International Conference on Enterprise Information Systems (ICEIS). 12., Funchal. *Proceedings...* ICEIS, 2010.

BRCOMMUNITY. *Business Rules Community*, 2000. Available at: http://www.brcommunity.com. Accessed: 28/10/2010.

BRG. *The Business Rules Group*. 2009. Available at: http://www.business rulesgroup.org. Accessed: 28/10/2010.

BRG. Defining business rules: what are they really?, 2000. Available at: http://www.businessrulesgroup.org/first_paper/BRG-whatisBR_3ed.pdf. Accessed: 28/10/2010.

CALÌ, A.; MARTINENGHI, D. Querying data under access limitations. In: International Conference on Data Engineering (ICDE). Cancun. *Proceedings...* ICDE, 2008.

CHEN, L.; CRAMPTOM, J. Set covering problems in role-based access control. In: European Symposium on Research in Computer Security. 14., Saint-Malo, France. *Proceedings...*, 2009.

COMELLA-DORA, S.; DEAN, J.; LEWIS, G.; MORRIS, E.; OBERNDORF, P.; HARPER, E. *A process for COTS software*. Technical report CMU/SEI-2003-TR-017. Carnegie Mellon Software Engineering Institute, 2004.

DEITERT, E.; MCCOY, D. *The anatomy of a business rule management system*. Gartner Research, 2007.

DoD. *Trusted computer security evaluation criteria*. Department of Defense, DoD 5200.28-STD, 1983.

FERRAIOLO, D. F.; KHUN, D. R. Role-based access control. In: National Computer Security Conference, 15. Baltimore, MD. *Proceedings...*, 1992, p. 554-563.

FERRAIOLO, D. F.; SANDHU, R.; GAVRILA, S.; KUHN, D. R.; CHANDRAMOULI, R. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, v. 4, n. 3, p. 224-274, 2001. doi:10.1145/501978.501980

ISO 27001. *Information security management*: specification with guidance for use, 2005.

KITCHENHAM, B. DESMET: a method for evaluating software engineering methods and tools, 1996. Available at: http://www.osel.co.uk/desmet.pdf. Accessed: 28/10/2010.

MURTHY, R.; SEDLAR, E. Flexible and efficient access control in Oracle. In: *ACM SIGMOD 2007*, Beijing. *Proceedings...*, 2007, p. 973-980. doi:10.1145/1247480.1247596

RYMER, J., GUALTIERI, M. *The Forrester wave*: business rules plataform, Q2, 2008. Forrester Research, Available at: http://www.forrester.com/go?docid=39088. Accessed: 28/10/2010.

SANDHU, R. S.; COYNE, E. J.; FEINSTEIN, H. L.; YOUMAN, C. E. Role-based access control models. *IEEE Computer*, v. 29, n. 2, p. 38-47, 1996.

SINUR, J. Magic quadrant for business rule engines. Gartner Research, 2005.

TARIQ, N. A.; AKHTER, N. Comparison of model driven architecture (MDA) based tools. In: Nordic Baltic Conference (NBC), 13. *Proceedings...* NBC, 2005.

YANG, L. Teaching database security and auditing. *ACM SIGCSE'09*, v. 1, n. 1, p. 241-245, 2009.