ReMoLa: Responsibility Model Language to Align Access Rights with Business Process Requirements

Feltus, Christophe; Petit, Michaël; Dubois, Eric

Published in:
Proceeding of the Fifth IEEE International Conference on Research Challenges in Information Science (IEEE RCIS 2011), Gosier, Guadeloupe, French West Indies

DOI:
10.1109/RCIS.2011.6006828

Publication date:
2011

Document Version
Early version, also known as pre-print

ReMoLa: Responsibility Model Language to Align Access Rights with Business Process Requirements

Christophe Feltus[1,2], Michaël Petit[1], Eric Dubois[2]
1. PReCISE Research Centre, Faculty of Computer Science, University of Namur, Belgium
2. Public Research Center Henri Tudor, Luxembourg-Kirchberg, Luxembourg
christophe.feltus@tudor.lu, mpe@info.fundp.ac.be, eric.dubois@tudor.lu

***Abstract*—Access controls is an important IT security issue and has accordingly been a huge research topic for the last decade. Many models and role engineering methods have been provided since then, and RBAC has appeared to be one of the most significant contributions. In parallel to those developments, new requirements have appeared in the field of IT governance and they provide new constraints for the elicitation of access control policies. One of those requirements is to have access rights strictly aligned with the business process and to have the responsibility of the employees involved in those processes strictly defined and suitably assigned to the employee. RBAC doesn't permit to integrate these new requirements. In this paper we propose a responsibility modeling language to align access rights with business processes requirements. To achieve that, our approach uses the concept of employees' responsibility as a means to bridge the gap through frameworks from the business layer down to frameworks from the technical layer.**

Keywords: Alignment; COBIT; Responsibility; Traceability; RBAC; Access right; Requirements engineering; Business process.

I. INTRODUCTION

In all company layers, standards and norms define business activities. Those activities are called strategic activities at the higher layer, such as the activity to report the company's results to the board of directors. They are called management activities at the intermediary layer, like activities to manage the budget of a company unit, and operational activities at the lower layer, such as the activity to encode customers' data. For all of those activities, implementation rules (e.g. access right policies) must accordingly be defined. Meanwhile governance standards and norms [1][2][3] request a strict alignment between the different business layers of activities and the corresponding rights. This strict alignment affords e.g. to respect the principle of least privilege and, by consequence, to provide to the employees with strict rights, which are indispensable to achieve their goals. Some sectors, like the financial sector, are particularly sensitive to this requirement and additionally request to show evidence of this alignment of permission and rights according to business needs. In practice, this alignment between the business view and the technical view, as well as the traceability of the right assigned to the employee according to the business specifications, are problematic [1], as further explained below.

[1] ISO/IEC 38500, International Standard for Corporate Governance of IT.

[2] P. S. Sarbanes, and M. Oxley (2002) Sarbanes-Oxley Act of 2002.

[3] Basel Committee on Banking Supervision, International convergence of capital measurement and capital standards; BIS; Basel, June 2004.

In most companies, the management of employees' permissions and rights is done by using the central concept of role which permits on the one hand to manage a large amount of users and on the other hand the permissions assigned to the role. Role engineering is a process to define roles, which ought to be affected to a set of users, who have the same function in the company. The Role Based Access Control (RBAC [2]) has emerged as a reference model in this discipline.

Using the concept of role presents weaknesses due to the difficulty to align the role defined at the business layer (business role) with the roles used at the IT layer to operate IT transactions (application role). This weakness discloses two kinds of situations. In the first case, the company restricts its number of application roles to the amount of business roles. In order to avoid defining too many roles, the company may define a limited number of roles and employees receive the permissions and rights associate to that role. In that case, they receive more rights and permissions than they need. In the second case, the company defines as many application roles as potential IT transactions. In that case, the company operates with many roles, which renders the access right management difficult and decreases the advantages of exploiting RBAC. This problem mainly emerges due to the misalignment between the business role and the application role. Business roles gather employees with the same function, who can perform different tasks, although application roles gather employees who perform the same tasks, but who could be assigned to different business role. This misalignment pleads for having distinct models at the business and at the IT level.

At the business level, based on the review of the literature, we have observed that the concept of responsibility is central to the business models and that it can be modeled with concepts from the business view like the employee's obligations and accountabilities, and concepts from the technical view like the employee's rights, access rights and permissions needed to perform business obligations. In previous work [3,4,5], we have elaborated a responsibility meta-model (Figure 2) built around three sets of concepts: (i) the accountability of an employee regarding an obligation derived from a responsibility; (ii) the rights and capabilities required to fulfill the obligation; and (iii) the commitment pledged by the employee to fulfill the obligation. Whereas the first two sets are common in the field of IT, the last one derives from social aspects, which underline the importance of dealing with the employee engagement in the responsibility assignment process.

In the first part of that paper, we present a responsibility centered meta-model named *ReMoLa*, which is an integrated

meta-model covering both, the business view and the technical view and that may be used as a pivot to assure the alignment between the two of them (Figure 1). To enhance that alignment considering governance requirements, we complete *ReMoLa* with the four types of predefined obligations from the COBIT framework [6] RACI chart. We consider that the semantic of those four obligations cover all the existing obligations in a company and that, in practice they can be aligned with the majority of semantic of the obligations encountered in the professional standards and norms. The use of those four types of obligation permits to refine the responsibilities of the employee and by the way, to assign those rights closer to the real needs of the employees. In the second part, we introduce a proof-of-concept to illustrate how the meta-model may be used in practice.

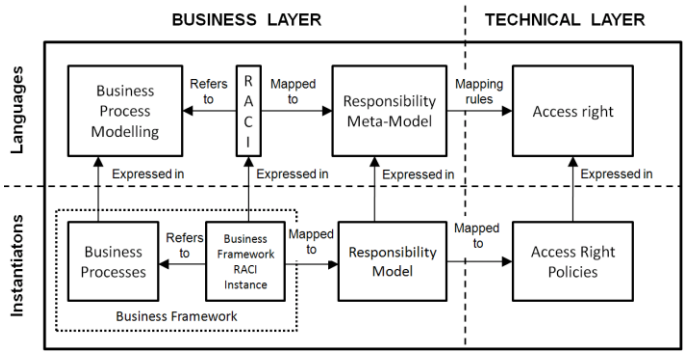

Figure 1. Responsibility meta-model in the layers view.

In the next section, we present the responsibility meta-model and its concepts together with their definitions. Afterwards, we map it with the four type of obligation from COBIT RACI chart. In section III we present the mapping of *ReMoLa* with the business layer and with the technical view. In section IV we present a proof-of-concept that highlights our *ReMoLa* can be used in the context of an audit of the traceability of the rights assignment to employees. Finally, we conclude the paper in section V.

II. RESPONSIBITY MODELING LANGUAGE (*REMOLA*)

In that section, we introduce the responsibility meta-model and we integrate the RACI chart obligations to it.

A. Responsibility meta-model

The elaboration of the responsibility meta-model (Figure 2) has been performed based on literature overview. As explained in previous papers [3,4,5], we have in the first place analyzed how the responsibility is included in information technology professional frameworks, in the field of requirements engineering and role engineering, and in the field of access right with the review of access control models. That literature overview in the field of IT has afterward been completed by a literature review in the field of Human Sciences. To ease the understanding of the UML diagrams, we introduce the following color code for Figure 2: **Red** boxes correspond to concepts from the business view, **Green** boxes correspond to concepts from the technical view, and **White** boxes correspond to concepts existing in both views (business and technical). **Blue** boxes correspond to concepts that represent employee intrinsic characteristics or specificities.

- The **responsibility** is a state assigned to an employee to signify him its obligation concerning a behavior, the accountability regarding that obligation and the right necessary to perform it.
- The **obligation** is the most frequent concept to appear as well in literature as in industrial and professional frameworks. Obligation is a duty which links a responsibility with a task that must be performed. We define a task as an action to use or transform an object.
- The **accountability** is a duty to justify the performance of a task to someone else under threat of sanction. Accountability is a type of obligation to report the achievement, maintenance or avoidance of some given state to an authority and, as consequence, is associated to an obligation. Accountability contribute to generate trust or to remove trust depending of the accountability outcomes.
- The **capability** describes the requisite qualities, skills or resources necessary to perform a task. Capability may be declined through knowledge or know-how, possessed by the agent such as ability to make decision, its processing time, its faculty to analyze a problem, and its position on the network.
- The **right** is common component but is not systematically embedded in all frameworks. Right encompasses facilities required by an agent to fulfill his obligations e.g. the access right that the agent gets once he is assigned responsible.
- The **assignment** is the action of linking an agent to a responsibility. Delegation process is the transfer of an agent's responsibility assignment to another agent.
- The **commitment** pledged by the agent related to this assignment or delegation process represents his engagement to fulfill the task and the assurance that he does it in respect of good practices.
- The **motivation** is the willingness of the employee to perform a task without being forced to do it.

B. Integration of the RACI chart obligation in ReMoLa

Most of the business frameworks often address the responsibility very globally and without specifying assignment constraints such as the employee involvement or interest, his capabilities, his accountability, etc. COBIT is a framework that goes deeper in the definition of the responsibility by providing a RACI chart. That chart defines four types of specific obligations that cover most of the obligations existing in a company. It defines semantic of those obligations and permits to link them to the different tasks that are necessary to achieve an activity. To improve the specification of the employees' responsibility, we integrate that four RACI chart obligations in *ReMoLa*. The expected output of this integration consists in four responsibility models that correspond to the semantic of the four types of obligations from COBIT. The mapping of COBIT with the responsibility meta-model permits as consequence to instantiate the responsibility meta-model with these specific obligations and with four types of task that correspond to these obligations. Additionally, those models specify all the characteristics that the employee who is responsible for that task inherits or must possess (capabilities, rights, commitment, obligations, etc.)

In practice, the models generated by the mapping must be refined according to the specifications of the business framework but, due to the lack of information about the

concept of responsibility in these business frameworks, the models of responsibility do not evolve much from the COBIT specifications. Assuming that an employee can be responsible, accountable, consulted or informed, we depict in the next sub-sections the characteristics of the responsibilities corresponding to each of the four COBIT obligation types:

Responsible: An employee who performs a task has the obligation to be *responsible* for that task. The employee assigned to that responsibility must by consequence be strongly committed to achieve the task; he requires strong personal capabilities before the assignment and access rights specific to the task to be done after the assignment. The responsible has obligations and accountabilities towards the achievement of the task. He refers to this achievement towards the employee who is accountable for it. The rights which are necessary to achieve the task are mostly not enforced by law requirement, rather from practical constraints.

Accountable: An employee who directs and makes authorization of a task has the obligation to be *accountable* for that task. The employee assigned to this responsibility must by consequence be committed to that responsibility. He requires personal capabilities to decide and to direct the task before being assigned responsible and he requires access rights specifically for the task to be direct after the assignment. The responsible has obligations and accountabilities towards the management of the task. He refers to this achievement towards the board of directors or toward a governmental authority.

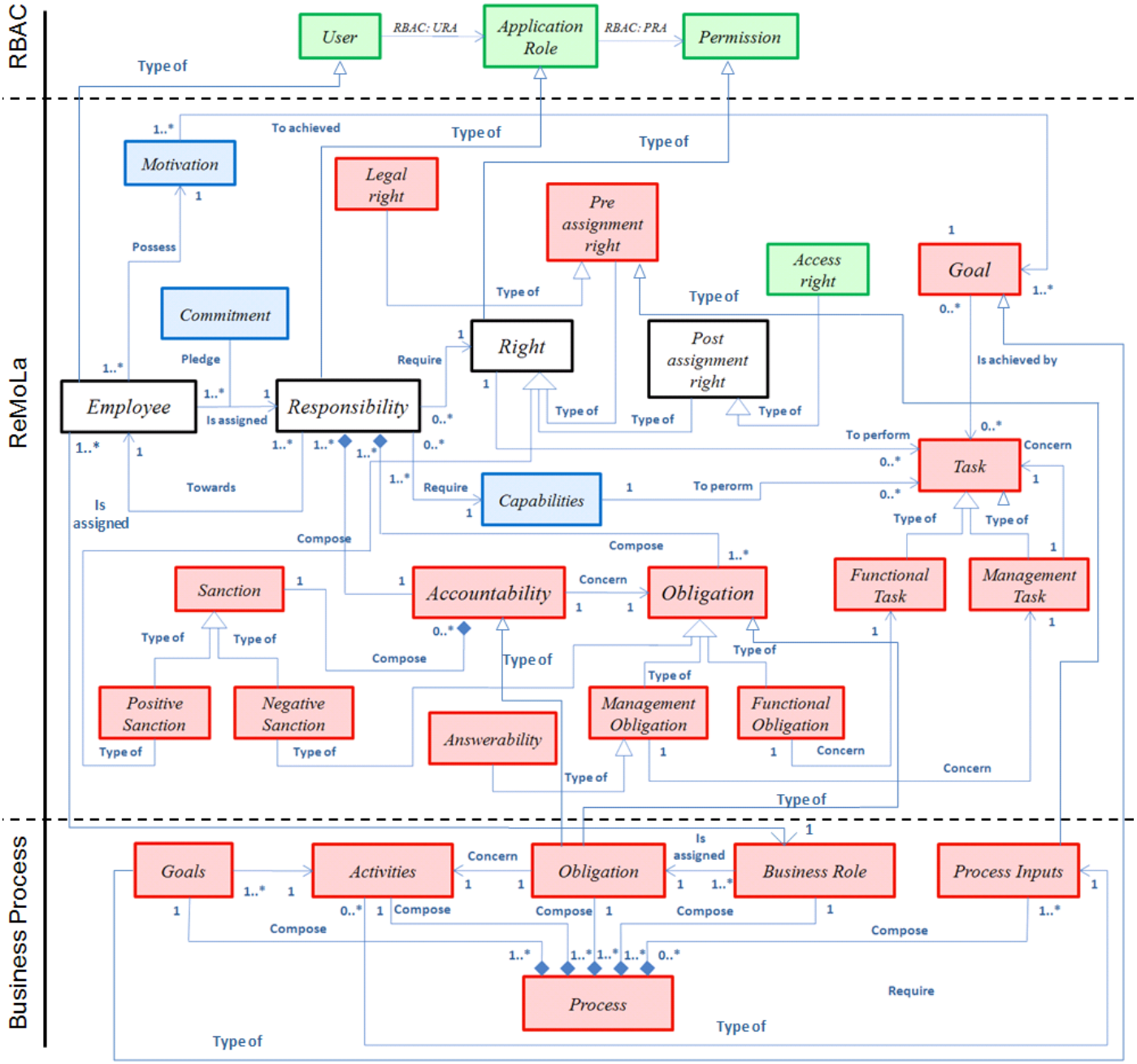

Figure 2. Responsibility meta-model UML diagram.

Consulted: An employee who provides consultancy to permit a task to be done is *consulted* for that task. The employee assigned to that responsibility must by consequence be committed to provide the accurate information. He requires personal capabilities before being assigned responsible and given access rights specific for the task to be done after the assignment. The responsible has obligations but most of the time, its accountability are limited. The level of commitment expected at least to be neutral. He doesn't have to be resistant to divulge or disclose information.

Informed: Employee that needs to be informed about the achievement of the task is *informed*. The employee assigned to that responsibility does not need to be committed to the responsibility neither to require personal capabilities. However, the informed employee requires access rights which are specific for the task he is informed of. The responsible has neither obligations nor accountability. Most of the time, the rights are formalized in a professional framework, in a corporate policy or in a law like SOX [2]. Using *ReMoLa* for aligning Business process with technical Rules

III. ALIGNMENT OF *REMOLA* WITH THE BUSINESS PROCESS AND WITH THE TECHNICAL RULE

In that section, we explain the mapping between *ReMoLa* with the business process in the first hand, and between *ReMoLa* and the technical layer in the second hand.

A. Alignment of ReMoLa with the business process

To align *ReMoLa* with the business process, we extract some main components of a business process and map them with *ReMoLa*. The concepts that present an interest for the elaboration of the responsibility and that have an impact on the definition of the technical rules are represented in business process UML diagram (Figure 2). Those concepts are: the goals of the process and the tasks necessary to achieve the goals, the obligations that concern those tasks and the business roles that are assigned those obligations. We also consider the concept of process inputs that stands for all the inputs that are identified useful at the business layer to perform the process.

The mapping between the concepts of the business process with the concepts of *ReMoLa* is the following:

- the business process includes the concepts of goal and the concept of task. Both of them correspond to the concepts of goal and task of *ReMoLa*,
- the concept of obligation at the business process level is mapped to the obligation or to the accountability in *ReMoLa*,
- the process input is the concept that represents the inputs that are necessary to achieve a business process. Those inputs are, as consequence, mapped to the pre-assignment rights needed to perform a task in *ReMoLa*,
- the business framework doesn't consider the concept of employee but the concept of business role that is assigned to employees. As consequence, the concept of employee in *ReMoLa* is assigned to the concept of business role.

B. Alignment of ReMoLa with technical rule

That second alignment is illustrated in the field of access right and considers the RBAC model. RBAC is a high level model with the objective to simplify the management of granting permissions to users. This is especially necessary in multinational companies where the amount of employees is often counted in thousands. It provides access decisions based on two associations – the association of users to roles based on the function that users assume, and based on their responsibilities, and the association of permission to roles describing that a role has the permission to perform specific operations on objects. This means that it is easy to change the assignment of people to roles without changing permissions.

To capitalize on the advantages of RBAC for managing access rights which the employees need to perform a task, we propose to map (Figure 2):

- the responsibility concept of *ReMoLa* with the RBAC concept of role (application role) and consider those responsibility as types of application role,
- the concept of employee corresponds to the RBAC concept of a user,
- the concept of right assigned to the responsibility corresponds to the RBAC concept of permission.

From that mapping of RBAC with *ReMoLa*, we model the assignment of permissions to employee by the intermediary concept of responsibility and consider both: (i) the task performed by the employee that justifies the rights assigned to that employee and (ii) its commitment to achieve that task.

The simplest way for a manager to assign permissions to an employee is to *simply* assign this employee to a responsibility, which encompasses specific tasks to be performed and is associated with the permissions which are needed to perform those tasks. By doing so, the manager implicitly obliges the employee to accept the responsibility to perform the tasks, but he does not actually know whether the employee has agreed to this. Not taking the employee's commitment into account is an authoritarian way of managing the staff and may result in company goals not being achieved due to unwillingness of employees to perform assigned tasks. Although this may seem unavoidable, especially in large companies, the assignment could easily be improved by incorporating acceptance of responsibility by an employee within the responsibility assignment process. When being assigned to a responsibility, the employee needs to explicitly commit to the obligation to achieve the task(s) related to the responsibility. This concept of commitment does not exist in RBAC as it considers the assignment of an employee to a role as a task performed solely by the employee's manager

IV. PROOF-OF-CONCEPT

To illustrate the alignment of rights with business process requirements, we introduce a proof-of-concept related to an audit activity that aims to verify the assignment of rights to employees. The business process that we analyze is the *System acceptance*[4] issued from ISO/IEC 27002/2005[5]. The audit of that business process highlights that 5 employees (Carla, Alice,

[4] The main outcomes of this process are *acceptance criteria for new information systems, upgrades, and new versions that should be established and suitable tests of the system(s) carried out during development and prior to acceptance.*

[5] ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management.

Emma, Denis and Bob) are involved in it. By depicting the access right database, we observe that those employees have the rights inventoried in Table I and the business roles itemized in Table II.

TABLE I. RIGHTS OF THE EMPLOYEES.

Employees	Rights
Carla	Access to all
Alice	Access to the list of requirements
	Access to migration priorities
	Allow participating in migration meetings
	Access to the migration risks
	Access to operational efficiencies requirements list
Emma	Access to migration priorities
	Allow to participate migration meetings
	Access migration risk analysis
Denis	Access to preparation template
	Access to testing template
	Access to the training support
	Time to participate to training
	Access to the system manual
	Access to the set of security controls in place
	Access to the list of errors
Bob	Access to the tests results

TABLE II. BUSINESS ROLES OF THE EMPLOYEES.

Employees	Business roles
Carla	Chief information officer
Alice	Employee assigned to the *System Acceptance* process
Emma	*System Acceptance* process manager
Denis	Project leader
Bob	System architect

Based on these values, the auditor has to check that the rights correspond to what is strictly necessary for the employee to perform the task and challenge the company to justify and explain why the rights are assigned to those employees. Using *ReMoLa* makes possible to check and justify that assignment. To do so, the following steps are necessary:

- **responsibility to task association**: enumeration of the tasks that compose the business process, association of obligation to those tasks and determination of the responsibility specifications,
- **rights to task association**: analysis of the rights that are necessary to perform the tasks,
- **responsibility to employee assignment**: assignment of the responsibility to the employee that has the profile corresponding to the responsibility specifications.

A. Responsibility to task association

The first action consists to identify all the tasks that compose the business process. The first column of Table III lists the 8 tasks that compose the process. Afterwards, the semantic of those tasks is analyzed and they are associated to one of the four RACI obligations. For the tasks necessary to perform the best practice *System acceptance,* the second column of Table III provides these types of obligation. For instance, the task *provide acceptance for the migration of new system* corresponds to an accountability because the semantic of that task means to make a decision, the task *preparation and testing of routine operating procedures to defined standards* corresponds to the obligation to be responsible because the semantic of that task corresponds to an action to perform, etc. Once we have identified to which obligations corresponds to the tasks, we can consider the responsibility model specifications for that obligation, which provides the specific requirements that the employee assigned to that responsibility needs.

TABLE III. RACI OBLIGATIONS TO TASKS ASSOCIATION.

Tasks	Obligation
Ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested	R
Provide acceptance for the migration of new information systems, upgrades, and new versions	A
Ensure the operational efficiency of the proposed system design	C
Preparation and testing of routine operating procedures to defined standards	R
Training in the operation or use of new systems	I
Agreed set of security controls in place	A
Appropriate tests should be carried out to confirm that all acceptance criteria have been fully satisfied	R
Consider error recovery and restart procedures, and contingency plans	R

B. Rights to task association

For the business process *System acceptance*, the rights and permissions are not explicitly described in the business framework. By consequence, the required rights are extracted from a fine grain analysis of the tasks. Table IV provides an example of those rights associated to the tasks.

TABLE IV. RIGHTS TO TASKS ASSOCIATION.

Tasks	Rights
Ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested	Access to the list of requirements
	Access to the agreement documentation
	Access to the test results
Provide acceptance for the migration of new information systems, upgrades, and new versions	Access to migration priorities
	Access to migration meetings
	Access migration risk analysis
Ensure the operational efficiency of the proposed system design	Access to operational efficiencies requirements list
Preparation and testing of routine operating procedures to defined standards	Access to preparation template
	Access to testing template
Training in the operation or use of new systems	Access to the training support
	Time to participate to training
	Access to the system manual
Agreed set of security controls in place	Access to the set of security controls in place
Appropriate tests should be carried out to confirm that all acceptance criteria have been fully satisfied	No access required
Consider error recovery and restart procedures, and contingency plans	Access to the list of errors

C. Responsibility to employee assignment

Most often, business framework does not provide specifications for the assignment of employees to responsibility. The assignment of rights to the employees that perform the task are obviously also not specified. As consequence, in practice, the assignment of rights to the employee is not achieved in function of the task to be performed but based on the business role. In that third step, we have to verify that the responsibility and rights necessary to perform the tasks are assigned to the employee that has the good profile.

The transfer of an obligation related to a task to an employee is possible if the employee‘s manager accepts the assignment of the responsibility to the employee and if this employee explicitly commits to fulfill the task. The first condition corresponds to a double control: the employee's availability and the employee's pre-assignment rights. The second condition corresponds to the commitment pledged by the employee according to his perception of the environment, guarantees received, interest in the task, etc. Once the process manager receives the agreement from the employee's manager and the commitment from the employee, the process manager requests the RBAC administrator to provide the permissions needed to achieve the task. As soon as the permissions are granted, the employee is assigned to the responsibility.

In that proof-of-concept, we have for example to audit that the responsibility of the *Provide acceptance for the migration of new information systems, upgrades, and new versions* is assigned to an employee with the good profile, we firstly have to identify to which responsibility this task corresponds. According to Table III, we see that it corresponds to the semantic of the obligation of being accountable. That means that the employee that is assigned to it requests i.e. personal capabilities to decide and to direct the task. Additionally, according to Table VI, that responsibility requests the following rights: *Access to migration priorities, Allow participating in migration meetings and Access migration risk analysis.*

Suppose that Alice is an employee assigned to the *System Acceptance* process. Before the assignment, the employee manager had to check e.g. that Alice had enough capabilities to achieve the work and that she had sufficient availability. Additionally, that responsibility was proposed to Alice who had to commit herself to it.

In the frame of the audit, we observe that the business role of Alice is *Employee assigned to the System Acceptance process.* In the company, that business role automatically receives the rights: *access to the list of requirements, access to migration priorities, allow participating in migration meetings, access to migration risks and access to operation efficiencies requirements list.* Alice that is only assigned to the task *Provide acceptance for the migration of new information systems, upgrades, and new versions* needs only the following rights: *access to migration priorities, allow participating in migration meetings, access to migration risks.* As consequence the audit highlights that Alice has too much rights in that she does not need *access to the list of requirements and access to operation efficiencies requirements list.*

V. CONCLUSIONS

The alignment of processes from the business layer with rules at the technical layer is challenging because business role cannot directly be mapped to application roles. We propose to use the concept of responsibility to make the link between these two layers and their respective types of role. Our perception of responsibility is that it does not attempt to replace the role or to be a subset of it, but rather, that it has for finality to refine the existing links between an employee, its business obligations, and its IT rights and permissions.

In this paper, we define an organizational responsibility meta-model (*ReMoLa*) elaborated based on the review of the literature in different fields. *ReMoLa* is an integrated meta-model covering both, the business view and the technical view and it is exploited as an hyphen to guarantee the alignment between those two views. To improve that alignment considering governance requirements, the four types of obligation from the COBIT RACI chart (Responsible, Accountable, Consulted and Informed*)* have been integrated in *ReMoLa*. We consider that the semantic of those four obligations covers the semantic of all the existing obligations related to a task and that, in practice, they can be aligned with all of the obligations encountered in a business framework. The use of those four types of obligation permits to refine the responsibilities of the employee and by the way, to assign those rights closer to their real needs.

Afterwards, we introduce a proof-of-concept to illustrate how the meta-model may be used in practice. In that proof-of-concept, we explain how *ReMoLa* is instantiated to define the responsibilities associated to the task that compose the business processes. After that, we list the rights that are necessary to perform the task. Finally, based on the specificities of the responsibilities, we justify their assignment considering the employees profile and map them to RBAC to assign the right to the employees.

ACKNOWLEDGMENT

This research was funded by the National Research Fund of Luxemburg in the context of TITAN project ref. CO/08/IS/21.

REFERENCES

[1] Fischer-Hubner, S., Otto, A. (2008) From a Formal Privacy Model to its Implementation. 21st NISSC. Arlington, VA, 5–8 October 5-8, 1998.

[2] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, R. Chandramouli. 2001. Proposed NIST standard for role-based access control. ACM Trans. Inf. Syst. Secur. 4, 3, 224-274, doi:10.1145/501978.501980

[3] C. Feltus, M. Petit, and M. Sloman, Enhancement of Business IT Alignment by Including Responsibility Components in RBAC, 5th International Workshop on Business/IT Alignment and Interoperability (BUSITAL 2010), Hammamet, Tunisia.

[4] C. Feltus, M. Petit, and E. Dubois, Strengthening employee's responsibility to enhance governance of IT: COBIT RACI chart case study. 1st ACM Workshop on Information Security Governance. ACM, New York, NY, 23-3, doi:10.1145/1655168.1655174

[5] C. Feltus, E. Dubois, M. Petit, Conceptualizing a Responsibility based Approach for Elaborating and Verifying RBAC Policies Conforming with COBIT Framework Requirements, RELAW10, in conjunction with the 18th IEEE RE2010, 27/9-1/10/2010, Sydney, Australia., doi: 10.1109/RELAW.2010.5625355

[6] COBIT 4.1, Control Objectives for Information and Related Technology, Information Systems Audit and Control Association.