Conceptualizing a Responsibility based Approach for Elaborating and Verifying RBAC Policies Conforming with CobiT Framework Requirements

Christophe Feltus, Eric Dubois, Michaël Petit
Motivation

- The concept of role
  - Business role
  - Application role
- Governance requirements
Motivation

- Our approach
- The method that we target is a 2 steps approach
Outlines

- Presentation of the Responsibility meta-model
- Mapping with CobiT
- Mapping with RBAC
- Example of assignment process
- Conclusions and future works
Elaboration of the meta-model

A state assigned to an employee to signify him its obligation concerning a behavior, the accountability regarding this obligation, and the right necessary to perform it.
Concept of obligation/accountability

| **Answerability** | a state assigned to an employee which could justify the performance of a behavior to someone else |
| **Sanction**       | a task or an object gained by the employee resulting of the performance of an accountability |
| **Accountability** | a type of obligation to justify the performance of a behavior to someone else under threat of sanction |
| **Obligation**     | a type of behavior that links a responsibility with a behavior that must be performed |
Concept of right

<table>
<thead>
<tr>
<th>Right</th>
<th>a facility required to perform a behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delegation Possibility</td>
<td>the right to delegate all or some part of the responsibility to another employee</td>
</tr>
<tr>
<td>Authority</td>
<td>the power or right to give orders or make decisions (from CIMOSA)</td>
</tr>
<tr>
<td>Access Right</td>
<td>the right to access an object</td>
</tr>
<tr>
<td>Capability</td>
<td>employee qualities, skills or resources</td>
</tr>
</tbody>
</table>
Assignment/delegation process

<table>
<thead>
<tr>
<th>Commitment</th>
<th>a state of being of an employee who pledges a personal engagement to perform a behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commitment Antecedent</td>
<td>a state or behavior that brings about commitment</td>
</tr>
<tr>
<td>Commitment Outcomes</td>
<td>a state or behavior that results in employee commitment</td>
</tr>
</tbody>
</table>
Outlines

- Presentation of the Responsibility meta-model
- Mapping with CobiT
- Mapping with RBAC
- Example of assignment process
- Conclusions and future works
Building the responsibilities

- Responsibility in CobiT are represented using a RACI chart
  - A16: Manage Change

- Assess impact and prioritise changes based on business needs
- Same rights and obligations to all employees?
- Need more precisions
Collect of tasks

- Responsibilities from CobiT

  - Business Role
  - Responsibility
  - Obligation
  - Behavior

- Instantiation with CobiT informations:
  - 4 responsibilities, business role (from RACI) and tasks (partially)
Responsibilities to tasks association

- From CobiT:
  - Tasks
    - Assessing change (based on business needs)
    - Priorising changes (based on business needs)
    - Assess the impact of change to the IT infrastructure, application and technical solutions
    - Scheduling change

- From ITIL:
  - Be available for consultation should an urgent Change required
  - Attend all relevant CAB (Change Advisory Board)
  - Consider all changes on the agenda and give an opinion on which changes should be authorized

- From the company:
  - Inform about the Business needs
  - Perform a monthly review
  - Introduce changes scheduled in a database
  - Prepare CAB report
  - Accountability concerning “Priorising changes” : Justify the prioritising
  - The CAB is informed about the changes
# Responsibilities to tasks association

## From CobiT:
- **Tasks**: Business needs, The IT infrastructure, Application and technical solutions, Scheduling change
- **Resp.**: R (responsible, performs the action)

## From ITIL:
- **Tasks**: Co-ordinate and lead an urgent Change
- **Resp.**: C (co-ordinator, leads the action), A (authorises the action)

## From the company:
- **Tasks**: Inform about the Business needs, Perform a monthly review, Introduce changes scheduled in a database, Prepare CAB report, Accountability concerning “Priorising changes” : Justify the prioritising, The CAB is informed about the changes
- **Resp.**: C (communicates the need), A (authorises the action), I (informs about the changes)
Rights to tasks association

From CobiT:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing change (based on business needs)</td>
<td>List of required changes (CobiT), information related to the business needs</td>
</tr>
<tr>
<td>Priorising changes (based on business needs)</td>
<td>List of accepted changes, information related to the business needs</td>
</tr>
<tr>
<td>Assess the impact of change to the IT infrastructure, application and technical solutions</td>
<td>List of required changes (CobiT), documentation related to the IT infrastructure, List of applications and technical solutions</td>
</tr>
<tr>
<td>Scheduling change</td>
<td>List of required changes (CobiT), List of accepted changes, list of priorising changes</td>
</tr>
</tbody>
</table>
## Rights to tasks association

### From CobiT:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>From ITIL</th>
<th>From the company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing change needs and aligning IT with business needs</td>
<td>Be available for consultation should an urgent Change required</td>
<td>List of urgent required changes</td>
</tr>
<tr>
<td></td>
<td>Attend all relevant CAB (Change Advisory Board)</td>
<td>No right</td>
</tr>
<tr>
<td></td>
<td>Consider all changes on the agenda and give an opinion on which changes should be authorized</td>
<td>List of required changes (CobiT)</td>
</tr>
</tbody>
</table>

### From the company:

<table>
<thead>
<tr>
<th>Inform about the Business needs</th>
<th>Management report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform a monthly review</td>
<td>List of required changes (CobiT), List of accepted changes</td>
</tr>
<tr>
<td>Introduce changes scheduled in a database</td>
<td>List of accepted changes</td>
</tr>
<tr>
<td>Prepare CAB report</td>
<td>List of required changes (CobiT), List of accepted changes</td>
</tr>
<tr>
<td>Accountability concerning “Prioritising changes”: Justify the prioritising</td>
<td>List of changes schedules and justifications</td>
</tr>
<tr>
<td>The CAB is informed about the changes</td>
<td>List of required changes (CobiT), List of accepted changes, list of prioritising changes</td>
</tr>
</tbody>
</table>
Outlines

- Presentation of the Responsibility meta-model
- Mapping with CobiT
- Mapping with RBAC
- Example of assignment process
- Conclusions and future works
Role Based Access Control

To simplify the management of granting permissions to users

3 main elements:
- User, Role and Permission

2 main functions:
- User-role assignment (URA)
- Permission-role assignment (PRA)
Mapping responsibility to RBAC role

- Business role from Cobit = RBAC concept of role?
- No, because:

  Cobit Role (or Business role): an employee assigned to that role is not obligatory assigned responsible for all the tasks of the activities.

  → If Business role = application role, some employees receives too much permissions.
Mapping responsibility to RBAC role

→ Employee is consulted during assignment process
Mapping responsibility to RBAC role

- **Employee**
  - Contextual situation
  - Do commitment to achieve the task exist?
    - Employee not committed to achieve the task
  - Employee committed to achieve the task
    - Transfer the obligation to the employee
      - Assignment status

- **CobiT Manager**
  - Check employee availability
    - Employee not available
    - Employee available
      - Check employee capable
        - Employee not capable
        - Employee capable
          - Inform Delegator

- **Employee's manager**
  - Check employee availability
  - Employee not available
  - Employee available
    - Check employee capable
      - Employee not capable
      - Employee capable
        - Inform Delegator
        - Approved employee obligation

- **RBAC administrator**
  - Request Permissions
  - Provide permissions
  - Transfer the Responsibility
  - Employee is responsible
    - Inform Delegator
Outlines

- Presentation of the Responsibility meta-model
- Mapping with CobiT
- Mapping with RBAC
- Example of assignment process
- Conclusions and future works
Example of assignment process

- **Task**: *Prioritizing changes*

- That task corresponds to one responsibility of being responsible of activity *Assess impact and prioritizing changes*.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing change (based on business needs)</td>
<td>R</td>
</tr>
<tr>
<td>Priorising changes (based on business needs)</td>
<td>R</td>
</tr>
</tbody>
</table>

- Following RACI chart: that activity is assigned to the business roles: **BPO, PMO, Head operation, Head development**.
Example of assignment process

- Suppose Bob one BPO identified by the CobiT manager

- RBAC administrator may assigned for that task:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing change (based on business needs)</td>
<td>List of required changes (CobiT), information related to the business needs</td>
</tr>
<tr>
<td>Priorising changes (based on business needs)</td>
<td>List of accepted changes, information related to the business needs</td>
</tr>
</tbody>
</table>
Outlines

- Presentation of the Responsibility meta-model
- Mapping with CobiT
- Mapping with RBAC
- Example of assignment process
- Conclusions and future works
Conclusions and future works

- Business needs for a better alignment of the employees’ responsibility from the management frameworks down to the technical rules.

- Our approach is to use the responsibility as a pivot between high layer requirements down to technical rules.

  - **Step 1: Responsibility building:**
    - Business Role, Activities, Tasks, and Rights → Responsibilities

  - **Step 2: Responsibility assignment:**
    - Responsibilities, Employees, Commitment
      → Application roles assigned to users
Conclusions and future works

- The meta-model of responsibility is considered more or less stable

- The method is theoretical and is exploited based on the Cobit framework
  - Apply it on other frameworks
  - Generalized the approach
  - Case study
Thank you! Questions?