Third International Workshop on Requirements Engineering and Law
(RELAW 10) - September 28th 2010

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

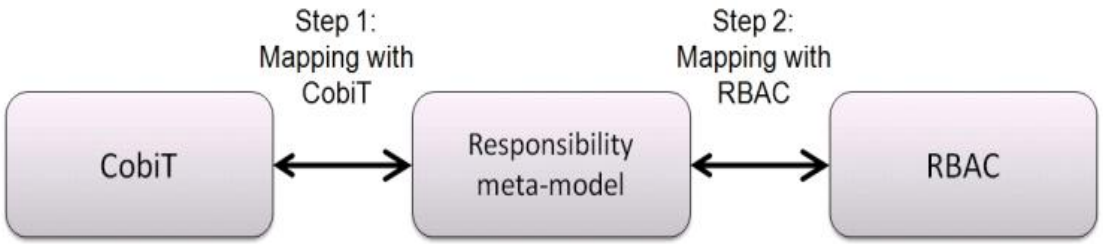
Christophe Feltus, Eric Dubois, Michaël Petit

Motivation

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

Motivation

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

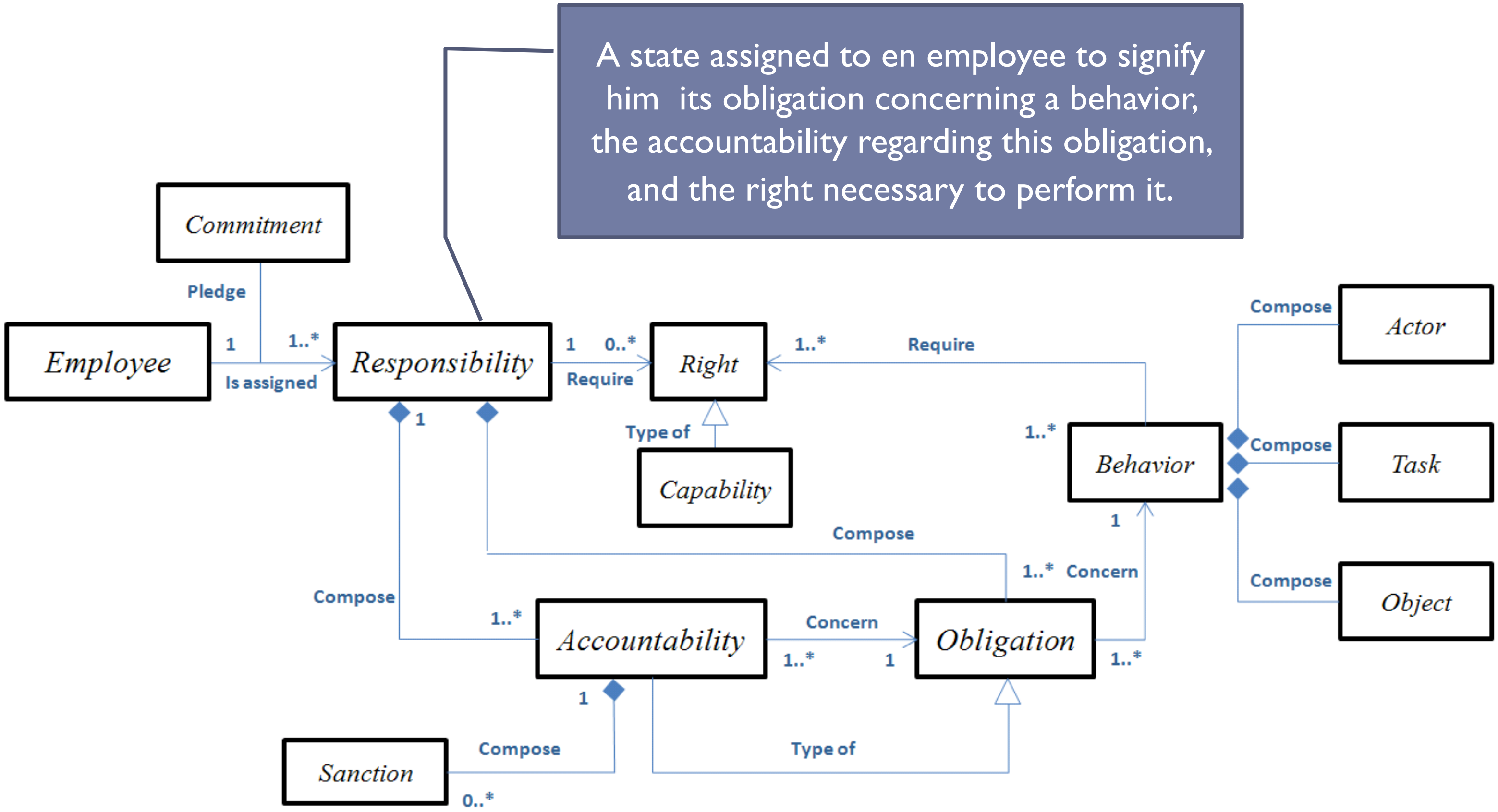


Outlines

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

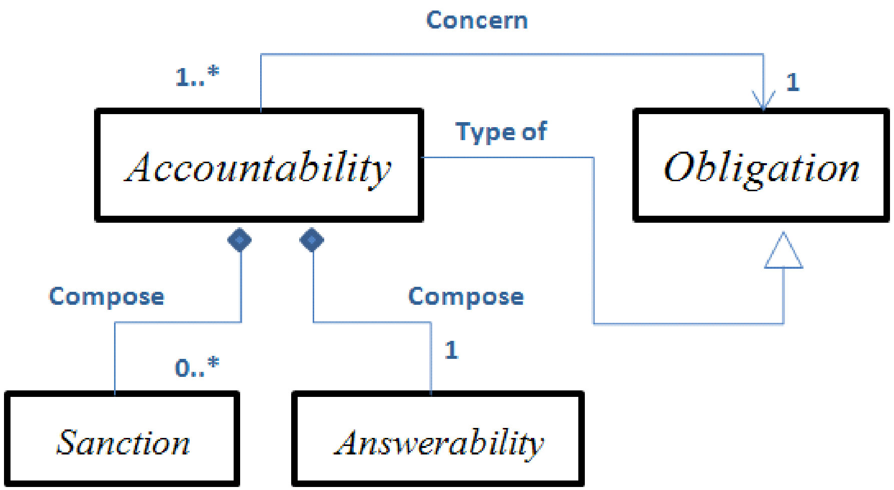
Presentation of the Responsibility meta-model

- Elaboration of the meta-model



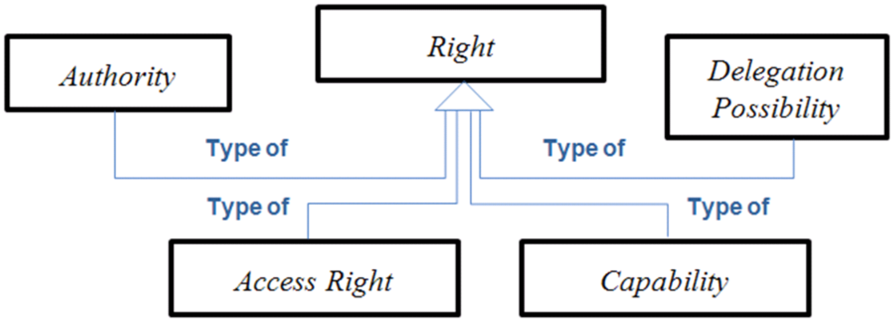
A state assigned to en employee to signify him its obligation concerning a behavior, the accountability regarding this obligation, and the right necessary to perform it.

Concept of obligation/accountability



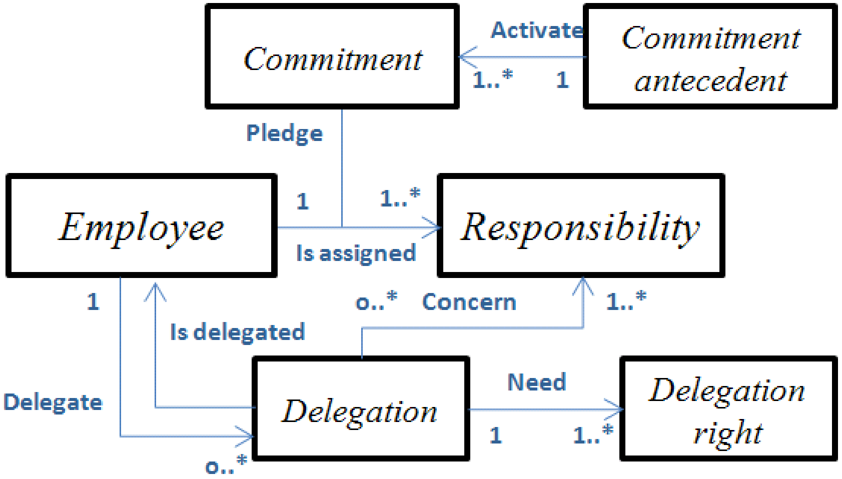
Answerability	*a state assigned to an employee which could justify the performance of a behavior to someone else*
Sanction	*a task or an object gained by the employee resulting of the performance of an accountability*
Accountability	*a type of obligation to justify the performance of a behavior to someone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

Concept of right



Right	*a facility required to perform a behavior*
Delegation Possibility	*the right to delegate all or some part of the responsibility to another employee*
Authority	*the power or right to give orders or make decisions (from CIMOSA)*
Access Right	*the right to access an object*
Capability	*employee qualities, skills or resources*

Assignment/delegation process



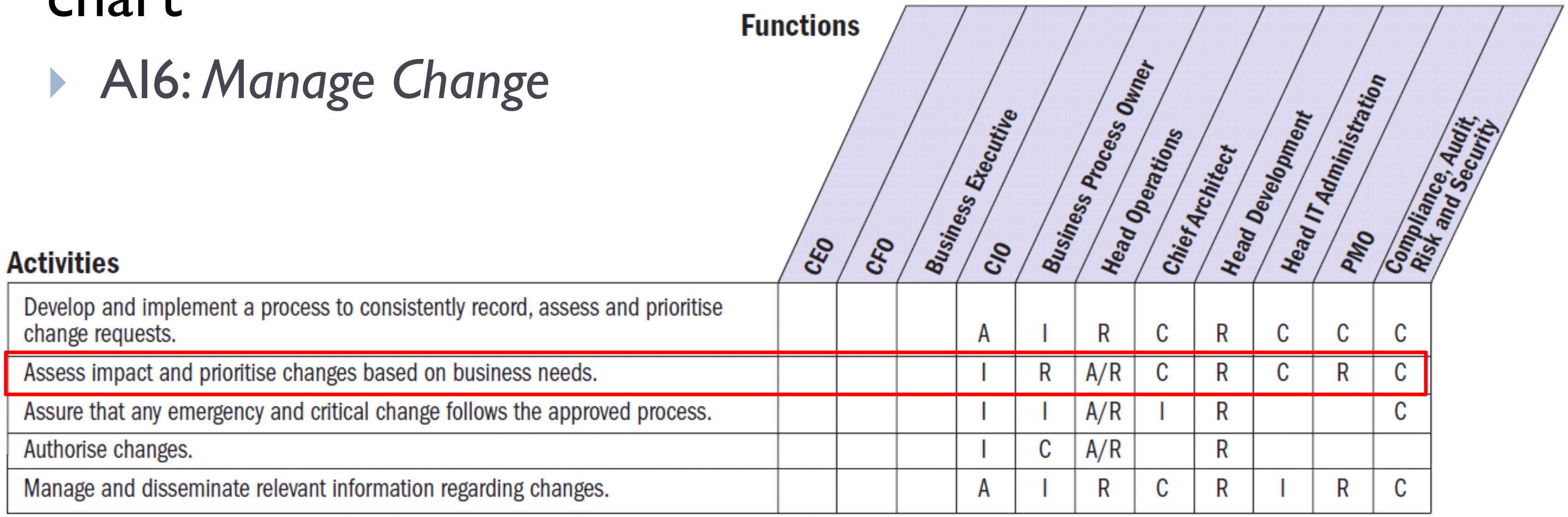
Commitment	*a state of being of an employee who pledges a personal engagement to perform a behavior*
Commitment Antecedant	*a state or behavior that brings about commitment*
Commitment Outcomes	*a state or behavior that results in employee commitment*

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
  - AI6: *Manage Change*

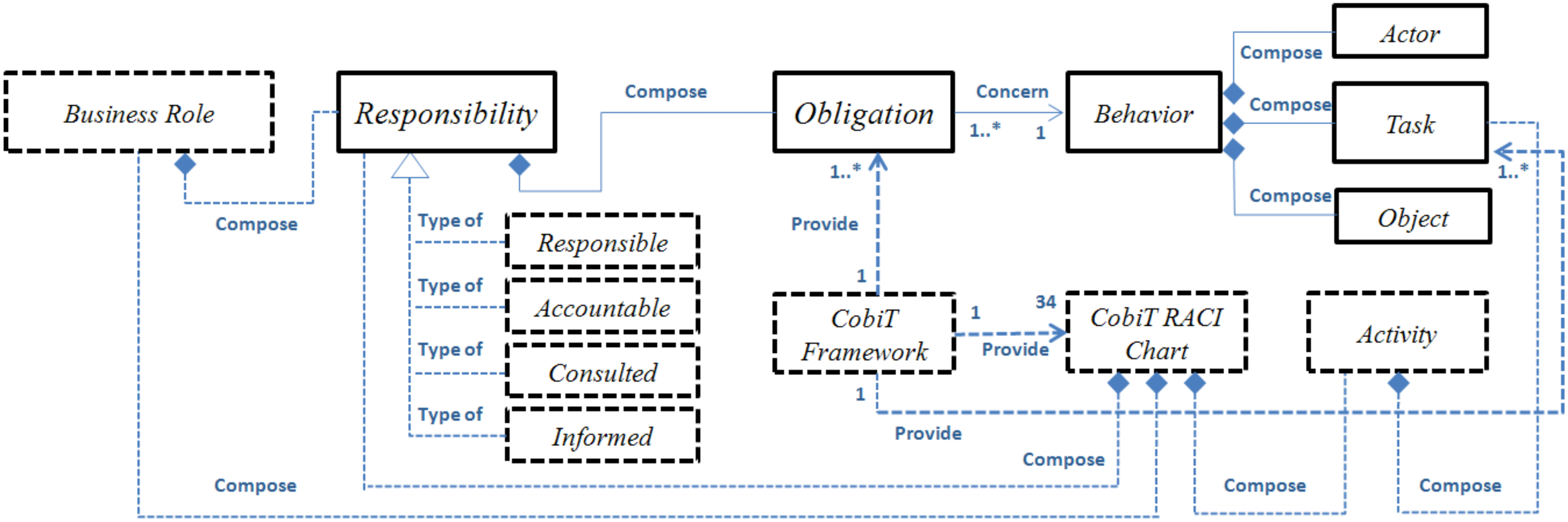


Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop and implement a process to consistently record, assess and prioritise change requests.				A	I	R	C	R	C	C	C
Assess impact and prioritise changes based on business needs.				I	R	A/R	C	R	C	R	C
Assure that any emergency and critical change follows the approved process.				I	I	A/R	I	R			C
Authorise changes.				I	C	A/R		R			
Manage and disseminate relevant information regarding changes.				A	I	R	C	R	I	R	C

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

Collect of tasks

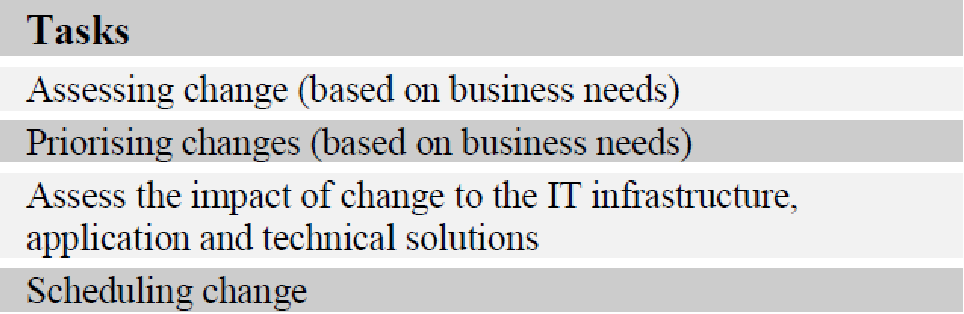
- Responsibilities from CobiT



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

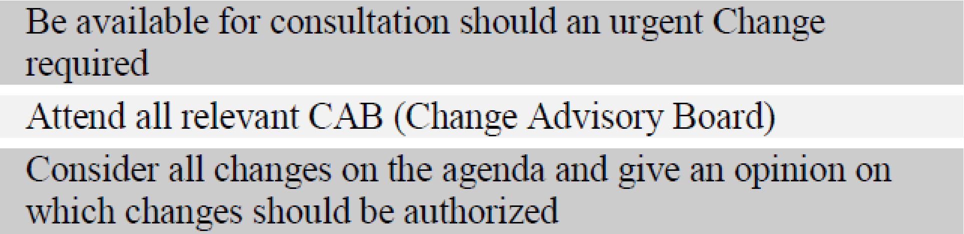
Responsibilities to tasks association

- From CobiT:



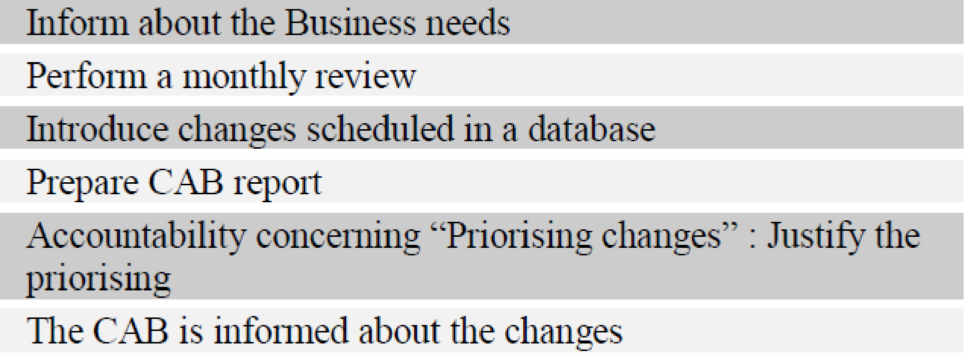
Tasks
Assessing change (based on business needs)
Priorising changes (based on business needs)
Assess the impact of change to the IT infrastructure, application and technical solutions
Scheduling change

- 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 priorising
The CAB is informed about the changes

Responsibilities to tasks association

- From CobiT:

is the employee who gets the action done

Tasks	Resp.
ess needs)	R
	R
e IT infrastructure, application and technical solutions	R
Scheduling change	R

- From IT

is the employee, who provides direction and authorizes an action

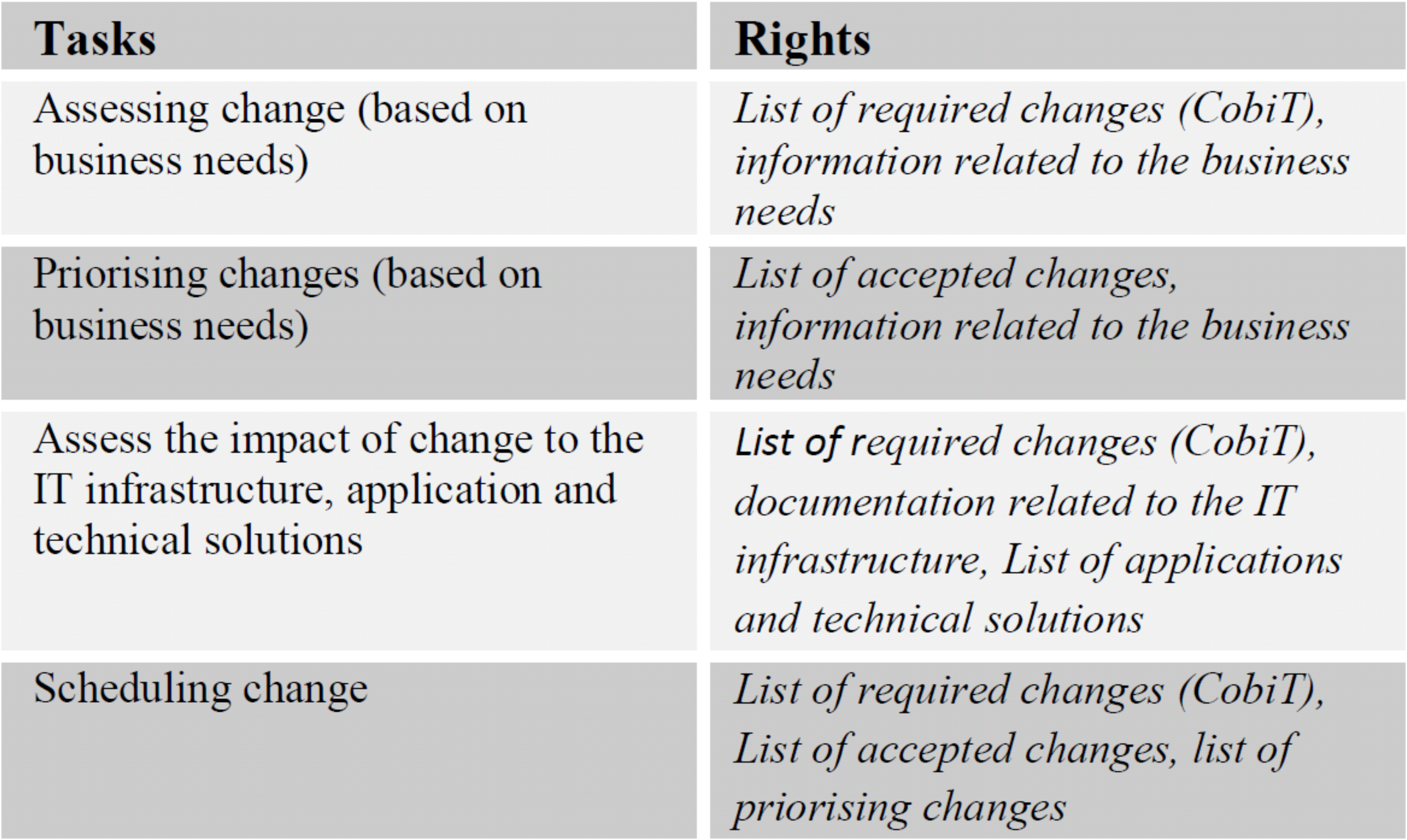
d an urgent Change	C
	A
and give an opinion on which changes should be authorized	A

- From the company:

Inform about the Business needs	C
Perform a monthly review	A
Introduce changes scheduled in a database	R
Prepare CAB report	A
Accountability concerning “Priorising changes” : Justify the priorising	A
The CAB is informed about the changes	I

Rights to tasks association

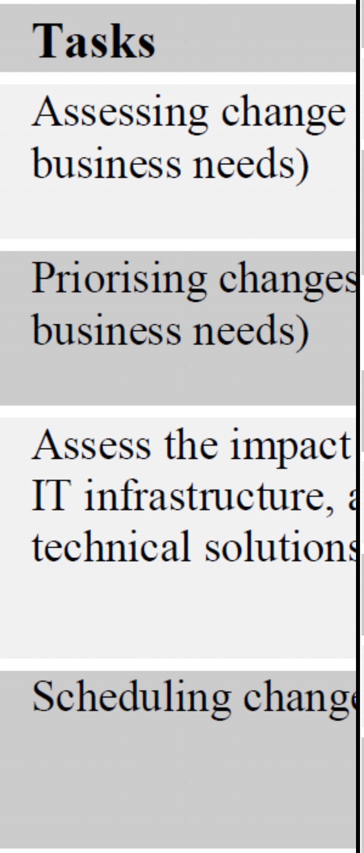
- From CobiT:



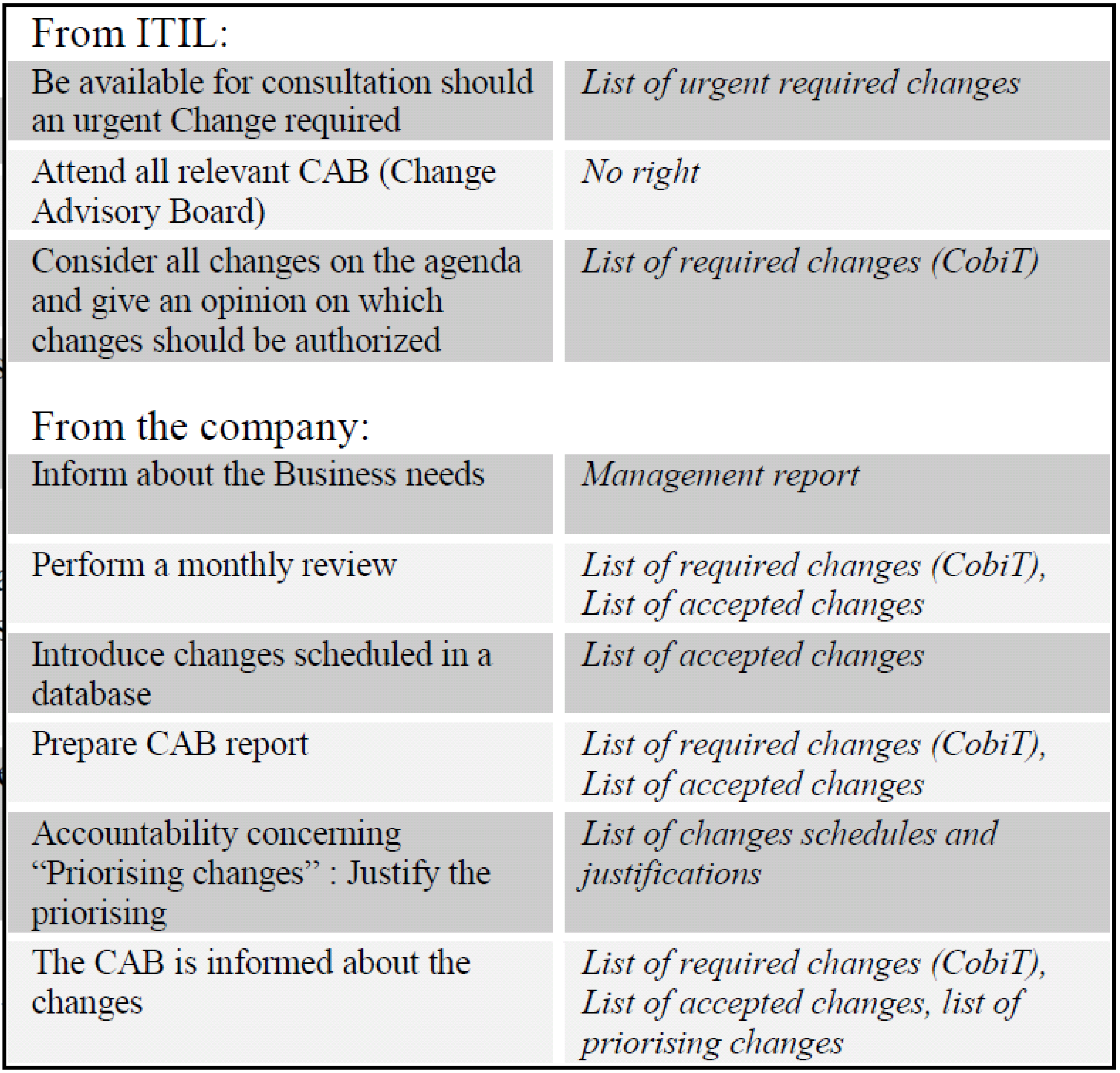
Tasks	Rights
Assessing change (based on business needs)	*List of required changes (CobiT), information related to the business needs*
Priorising changes (based on business needs)	*List of accepted changes, information related to the business needs*
Assess the impact of change to the IT infrastructure, application and technical solutions	*List of required changes (CobiT), documentation related to the IT infrastructure, List of applications and technical solutions*
Scheduling change	*List of required changes (CobiT), List of accepted changes, list of priorising changes*

Rights to tasks association

- From CobiT:



Tasks
Assessing change business needs)
Priorising changes business needs)
Assess the impact IT infrastructure, a technical solutions
Scheduling change



From ITIL:

Be available for consultation should an urgent Change required	*List of urgent required changes*
Attend all relevant CAB (Change Advisory Board)	*No right*
Consider all changes on the agenda and give an opinion on which changes should be authorized	*List of required changes (CobiT)*

From the company:

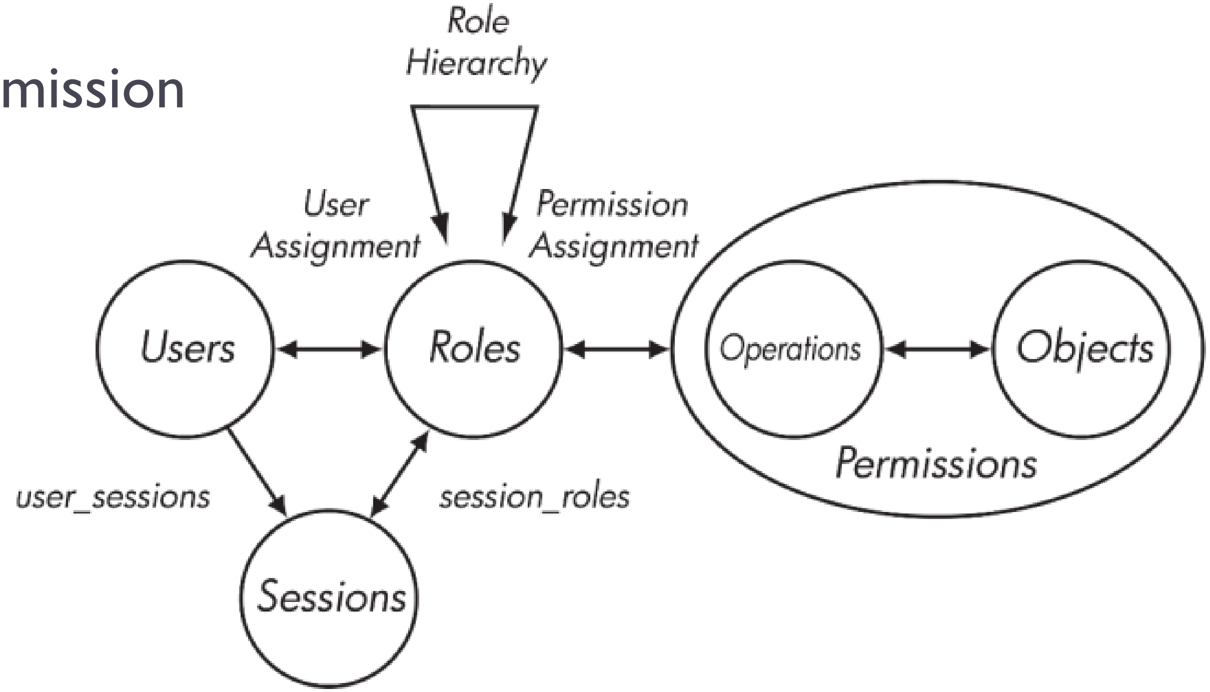
Inform about the Business needs	*Management report*
Perform a monthly review	*List of required changes (CobiT), List of accepted changes*
Introduce changes scheduled in a database	*List of accepted changes*
Prepare CAB report	*List of required changes (CobiT), List of accepted changes*
Accountability concerning “Priorising changes” : Justify the priorising	*List of changes schedules and justifications*
The CAB is informed about the changes	*List of required changes (CobiT), List of accepted changes, list of priorising changes*

Outlines

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

RBAC :

- 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)



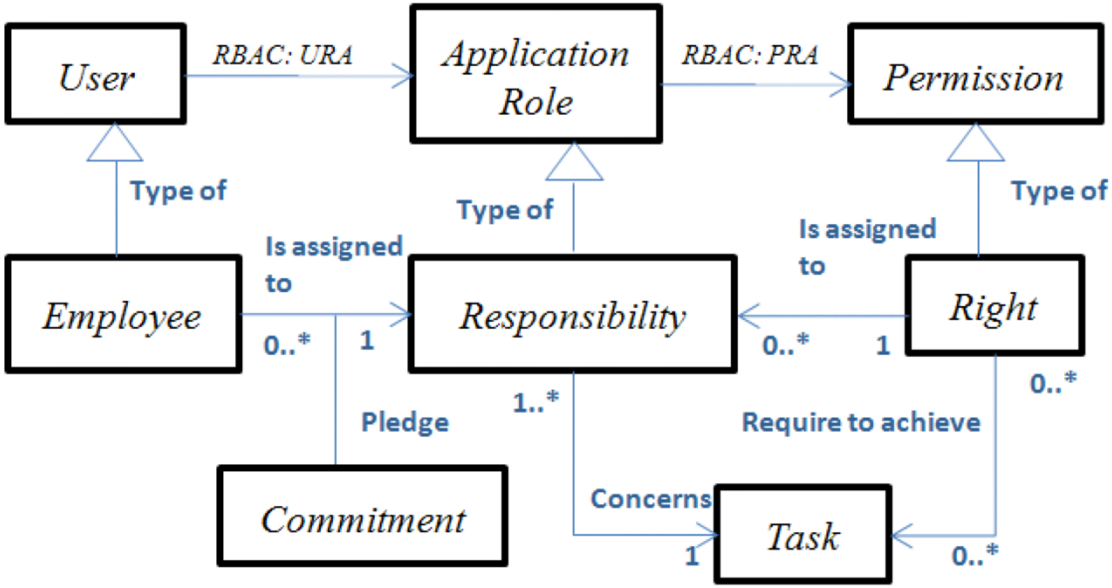
Mapping responsibility to RBAC role

- 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.

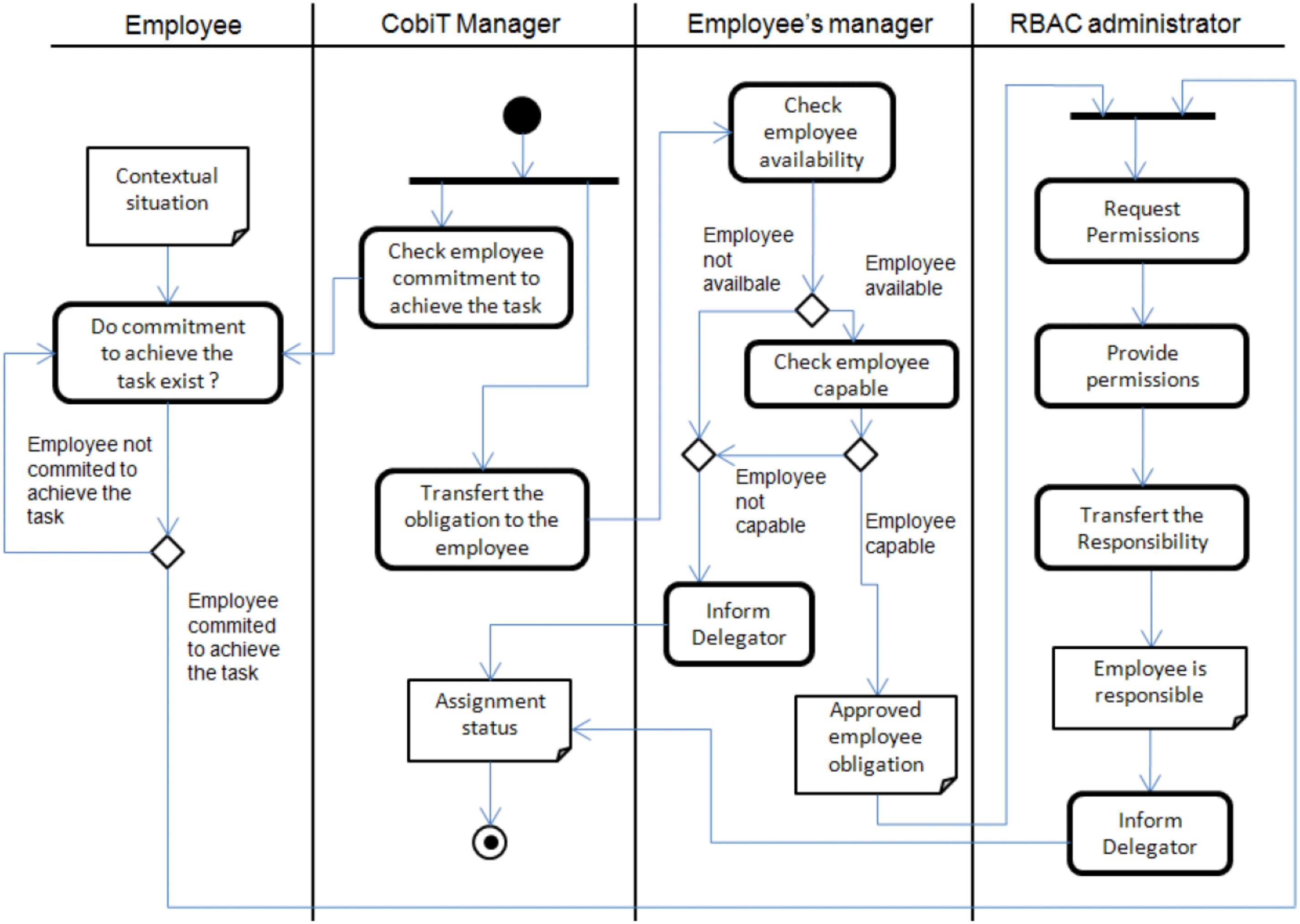
→ If Business role = applictaion role, some employees receives to much permissions.

Mapping responsibility to RBAC role



→ Employee is consulted during assignment process

Mapping responsibility to RBAC role



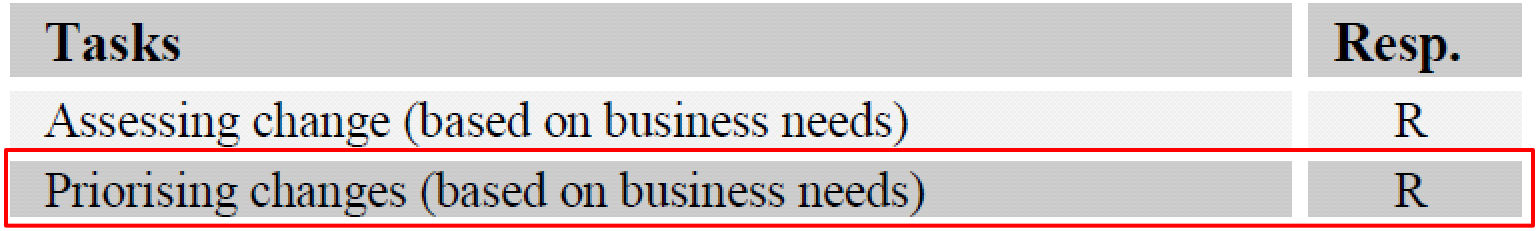
Employee
CobiT Manager
Employee's manager
RBAC administrator
Contextual situation
Do commitment to achieve the task exist ?
Employee not commited to achieve the task
Employee commited to achieve the task
Check employee commitment to achieve the task
Transfert the obligation to the employee
Assignment status
Check employee availability
Employee not availbale
Employee available
Check employee capable
Employee not capable
Employee capable
Inform Delegator
Approved employee obligation
Request Permissions
Provide permissions
Transfert 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

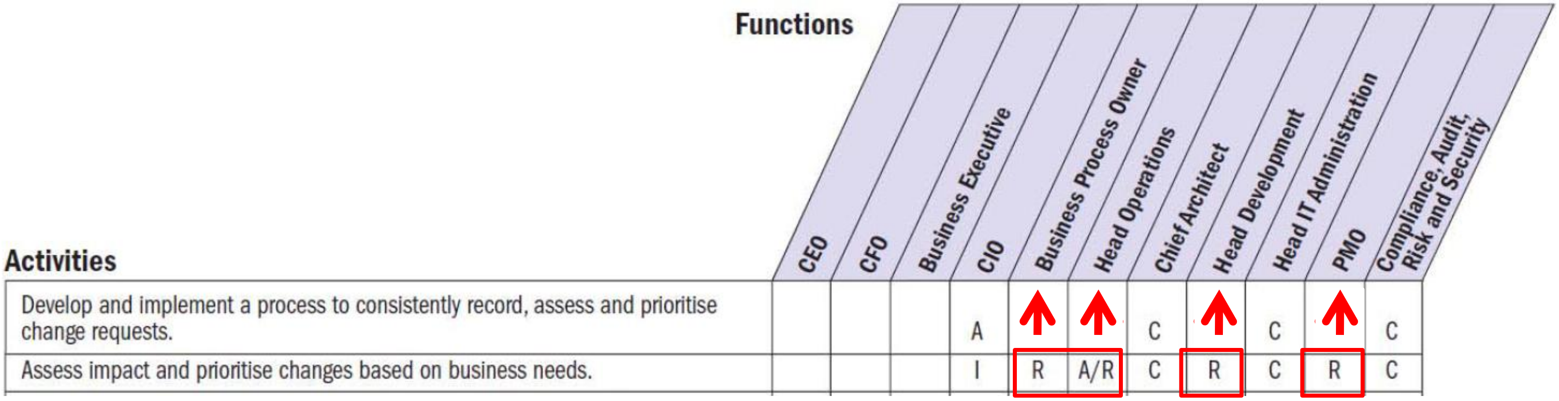
Example of assignment process

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



Tasks	Resp.
Assessing change (based on business needs)	R
Priorising changes (based on business needs)	R

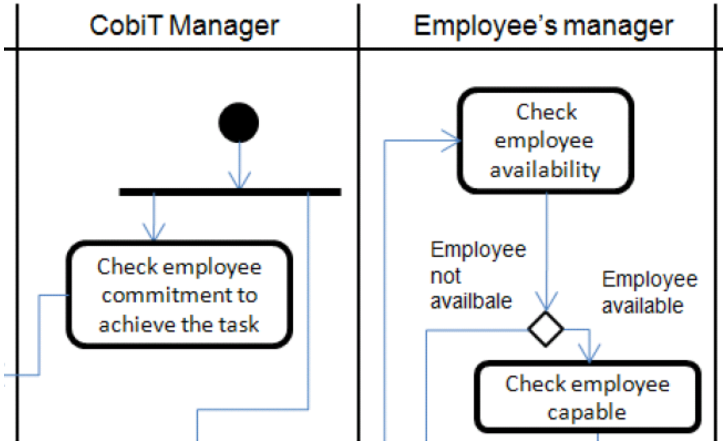
- Following RACI chart : that activity is assigned to the business roles : *BPO, PMO, Head operation, Head development*



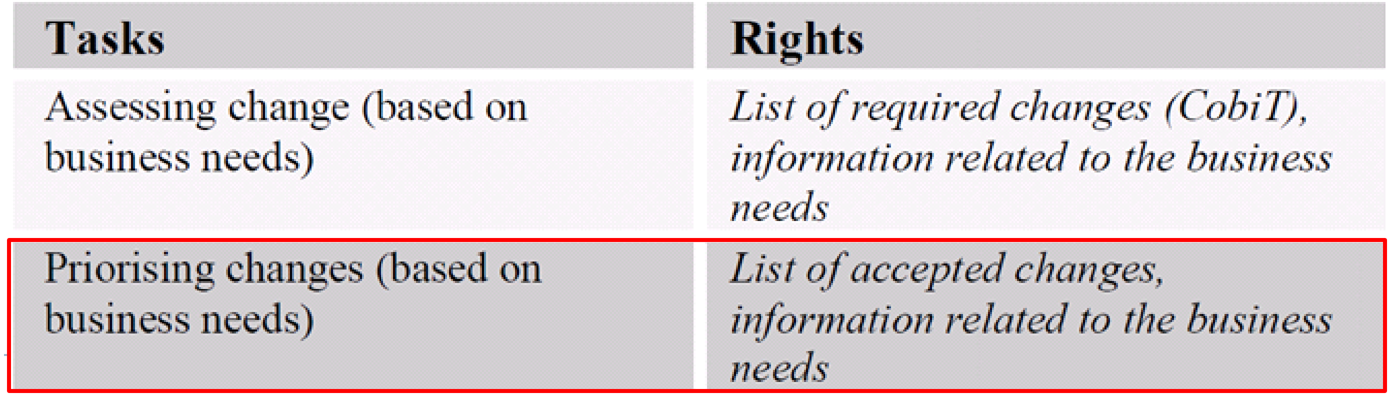
Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop and implement a process to consistently record, assess and prioritise change requests.				A	↑	↑	C	↑	C	↑	C
Assess impact and prioritise changes based on business needs.				I	R	A/R	C	R	C	R	C

Example of assignment process

- Suppose Bob one BPO identified by the CobiT manager



- RBAC adminsitrator may assigned for that task:



Tasks	Rights
Assessing change (based on business needs)	*List of required changes (CobiT), information related to the business needs*
Priorising changes (based on business needs)	*List of accepted changes, information related to the business needs*

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 alignement of the employees' responsibility from the management frameworks down to the technical rules
- Our approach is to use the responibility as a pivite between high layer requirements down to techical 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 ?