Security and Access Control Lists

General information

- Permissions are assigned to user roles
- Each user has one or more roles
- Users are grouped in business units
- Business units have hierarchy
- Business units relate to organization

https://github.com/oroinc/platform/blob/3.1/src/Oro/Bundle/SecurityBundle/Resources/doc/examples.md

Ownership

- Entity may have an owner
- Owner is represented by one of the entities:
  - User
  - Business Unit
  - Organization (EE only)
- Owner is used to check permissions
- Specified at the entity configuration

https://github.com/oroinc/crm/blob/3.1/src/Oro/Bundle/ContactBundle/Entity/Contact.php#L51-L57

Security

- Two types of ACLs:
  - Entity based
  - Action based (capabilities)

Demonstration >>>

Entity permissions

- Permissions
  - VIEW, CREATE, EDIT, DELETE, ASSIGN, ...
  - permissions.yml
- Access levels without ownership
  - None, Global
- Access levels with ownership
  - None, User, Business Unit, Division, Organization, Global

[Documentation]

Entity permissions

- ACL can be enabled using entity configuration
- Make sure to run
    - bin/console oro:entity-config:update

https://github.com/oroinc/crm/blob/3.1/src/Oro/Bundle/ContactBundle/Entity/Contact.php#L58-L62

Ownership Access Levels

- Global
- Organization
- Division
- Business Unit
- User
- None

How to define entity permissions

- Controller annotations
- Resources/config/oro/acls.yml

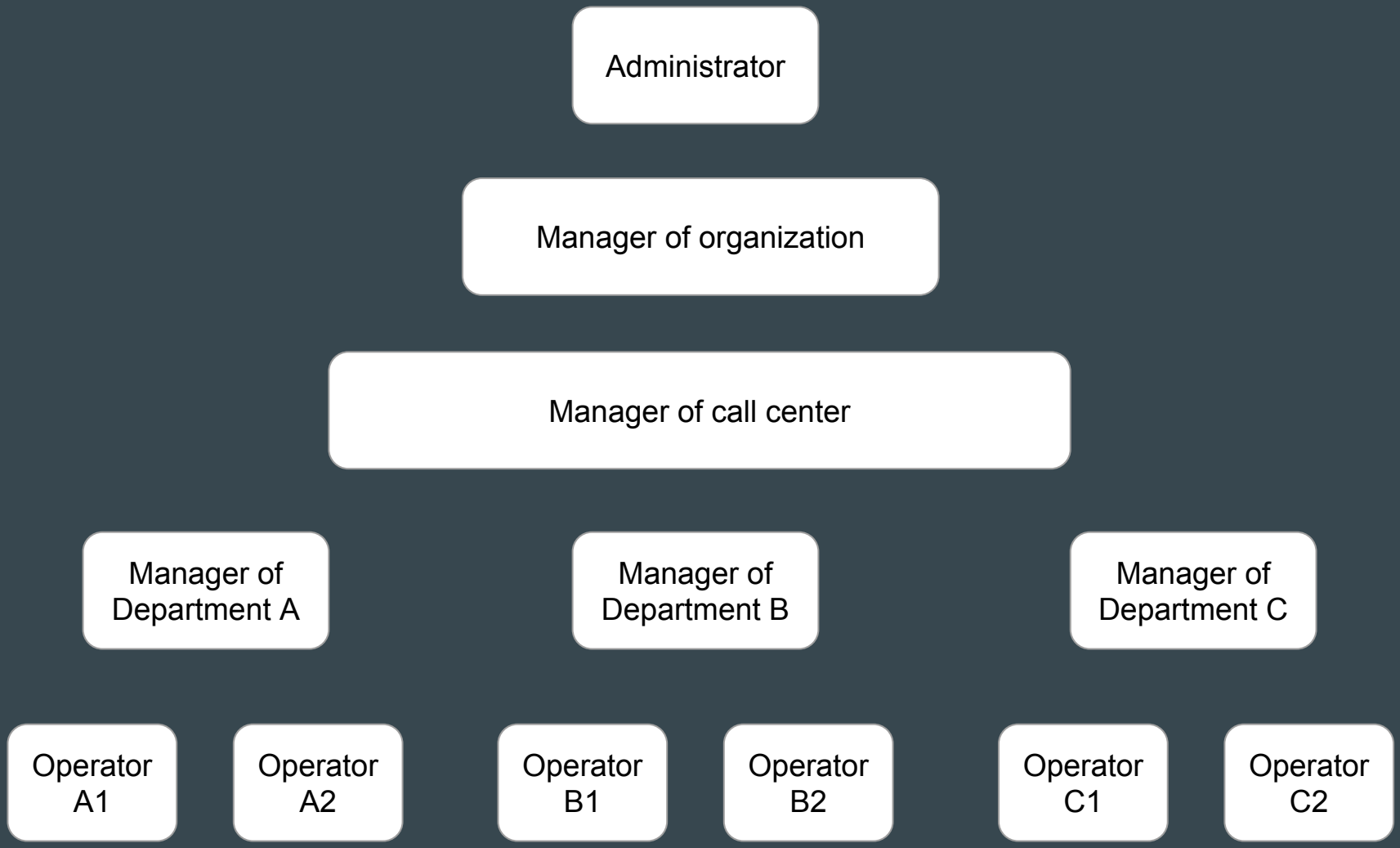
https://github.com/oroinc/platform/blob/3.1/src/Oro/Bundle/UserBundle/Controller/UserController.php#L32-L37

https://github.com/oroinc/platform/blob/3.1/src/Oro/Bundle/CommentBundle/Resources/config/oro/acls.yml

How to check entity permissions

```
// PHP code

$checker = $this->container->get('security.authorization_checker');

if ($checker->isGranted('VIEW', $entity)) {

}

.yml
acl_resource: acl_name


{# Twig template #}

{% if is_granted('VIEW', entity) %}

{% endif %}
```

Example: Call center



Example: Operator

- Requirement: Operator must be able to see only contacts assigned directly to him
- Contact owner: User (Operator)
- ACL:
  - Permission=VIEW
  - Level=User

Example: Manager of department

- Requirement: Manager of department must be able to see contacts assigned to operators in his departments
- ACL:
  - Permission=VIEW
  - Level=Business Unit
- Manager of department and all operators has to be in the same business unit

Example: Manager of call center

- Requirement: Manager of call center must be able to see all contacts processed by call center
- ACL:
  - Permission=VIEW
  - Level=Division
- Business unit of manager of call center must include all department business units

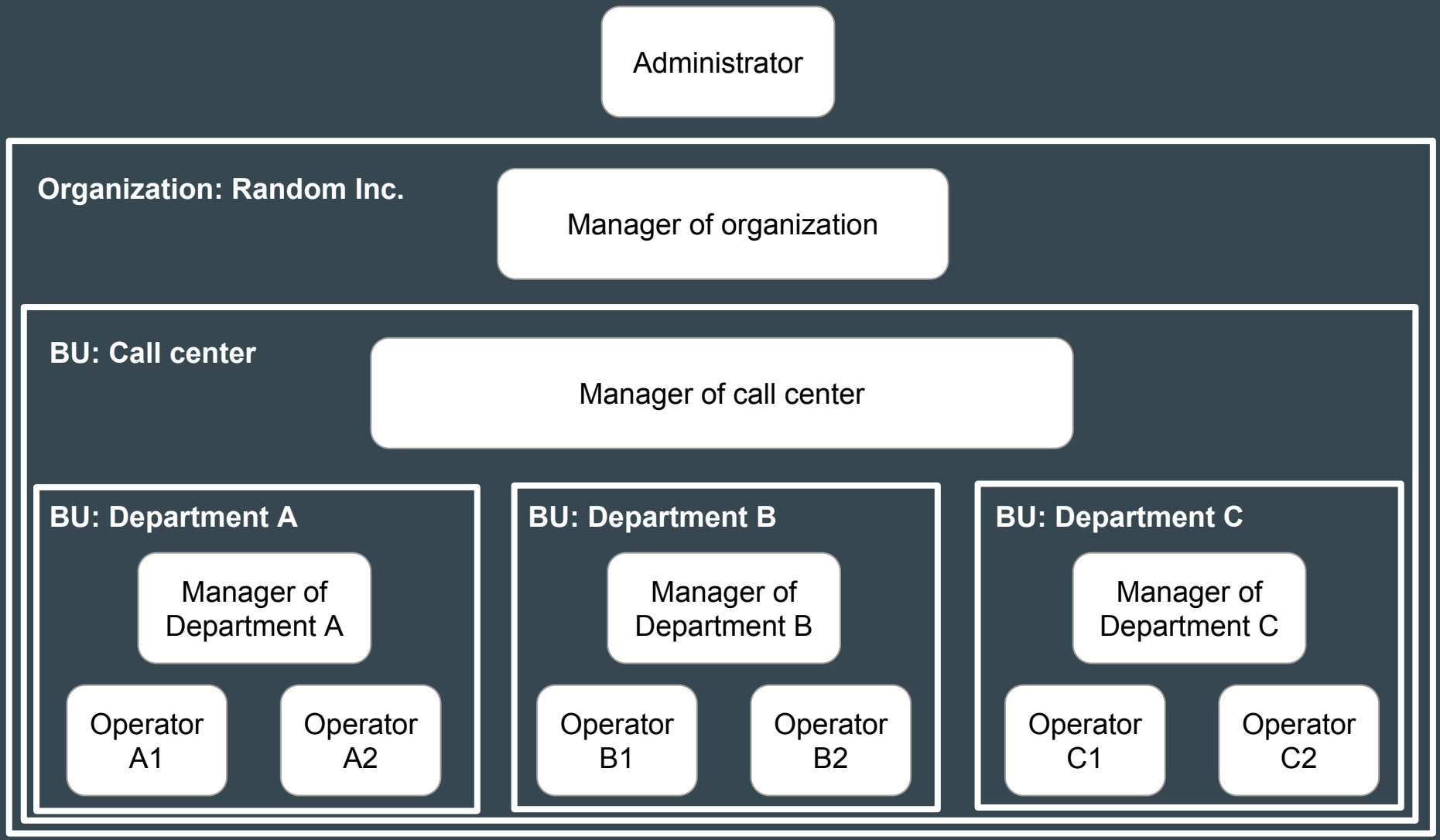
Example: Manager of organization

- Requirement: Manager of call organization must see all contacts in his organization
- ACL:
  - Permission=VIEW
  - Level=Organization
- Manager and department business units must be in the same organization

Example: Administrator

- Requirement: Administrator must see all contacts
- ACL:
  - Permission=VIEW
  - Level=Global

Example: Call center with hierarchy



Action permissions (capabilities)

- Binary values - On/Off
- No action access levels (User, ..., Global)
- No permissions (VIEW, EDIT, ...)

Demonstration UI >>>

How to define action permissions

- Controller annotations - example
- Resources/config/oro/acls.yml - example

How to check action permissions

```
// PHP code

$checker = $this->container->get('security.authorization_checker');

if ($checker->isGranted('capability_name')) {

}

.yml
acl_resource: capability_name


{# Twig template #}

{% if is_granted('capability_name') %}

{% endif %}
```

More

- Workflow permissions
- Field based ACL

https://github.com/oroinc/crm/blob/3.1/src/Oro/Bridge/TaskCRM/Migrations/Data/ORM/CrmRoles/workflows.yml

https://github.com/oroinc/platform/blob/3.1/src/Oro/Bundle/SecurityBundle/Resources/doc/field-acl.md

Docs

https://oroinc.com/orocrm/doc/2.0/admin-guide/security/access-management-access-levels

https://oroinc.com/orocrm/doc/2.0/admin-guide/security/access-management-ownership-type