TalentRadar

access management

scope

On the client instances of TalentRadar (hosted on Domo), both client and randstad users will have access to dashboards and related data, according to the role based access policy defined and agreed between the **client stakeholder** and the **randstad account leader**.

This process is owned and managed by the data access control manager, part of the data governance function at randstad enterprise.

principles

- **Role Based Access Control** (RBAC) refers to the concept of assigning permissions to users based on their role within an organization. It offers a simple, manageable approach to access management that is less prone to error than assigning permissions to users individually.
- **Principle of Least Privilege** (PoLP) is an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task.

accountability

- The **randstad account leader** for the client program, is responsible for the role based access policy (both client and randstad) and will make sure this is in alignment with the client stakeholder.
- The **client stakeholder provides** the needs for access control to the account leader, who will request the role based access policy setup and updates on behalf of the client.
- The **data access control manager**, wil set up and manage the implementation of the role based access policy for the client's instance of TalentRadar.

request history

All requests are saved in the randstad ticketing system and can be consulted by the data governance and information security functions.

activity logs

All activity on the TalentRadar solution is registered (100% logging) and these logs are available for the data governance and information security functions as read-only.

concept

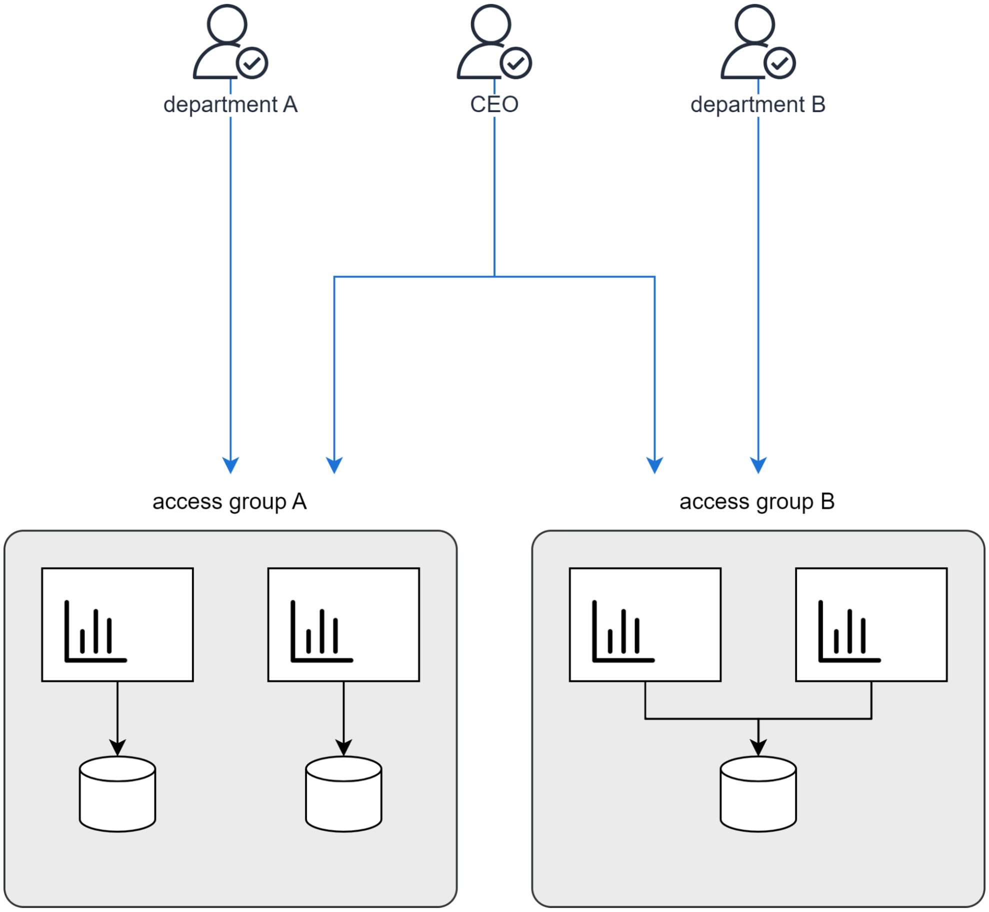
Authenticated users get access to dashboards and related data via a role based access policy. The attributes on the **users profile**, will assign them to **access groups** which unlock certain dashboard and datasets.

In the example below you see 3 users:

- *user who is a member of department A*
- *user who is the CEO*
- *user who is a member of department B*

The RBA policy dictates in this example:

- *users with the department A will get to see the dashboards and data on the left*
- *users with the department B will get to see the dashboards and data on the right*
- *users with the role CEO will see all dashboards and data*



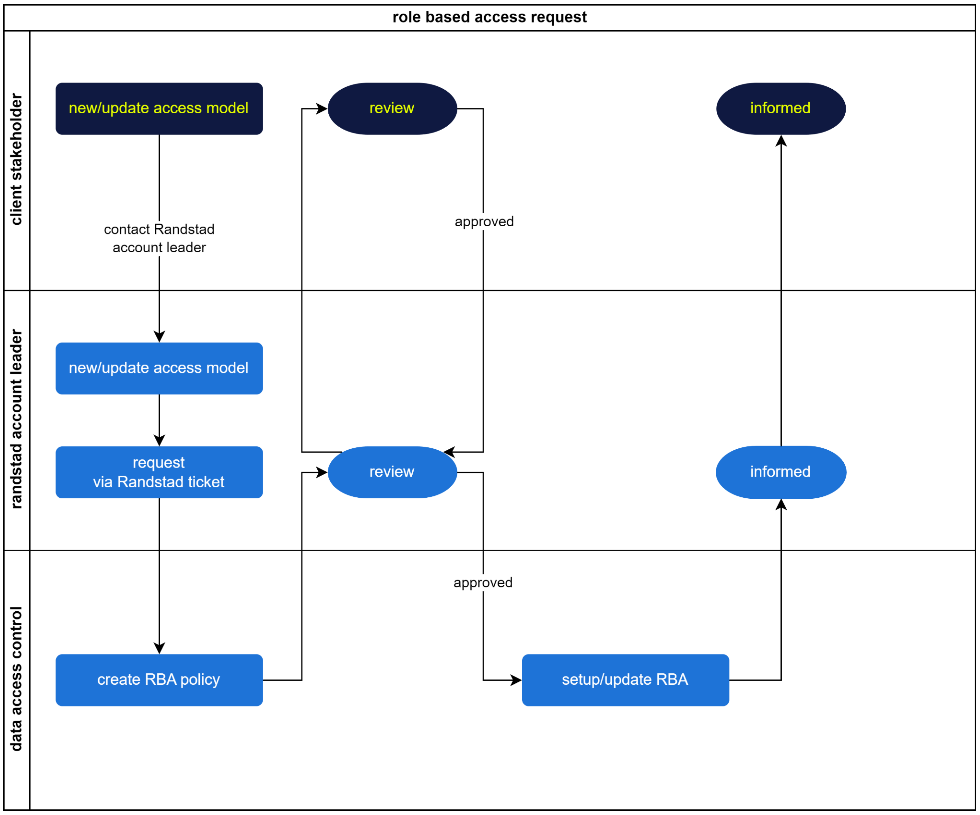
request: RBA policy create/update

A new user is requested by the randstad account leader for the client program, via the randstad ticketing system, and the request is reviewed by the randstad data access control manager.

The related role based access policy will be created or updated and sent for approval to the randstad account leader.

Once approved the role based access policy will be implemented and changes are the privilege of the randstad account owner, representing the client stakeholder.

talentradar.


role based access request
client stakeholder
randstad account leader
data access control
new/update access model
review
informed
contact Randstad
account leader
approved
new/update access model
request
via Randstad ticket
review
informed
approved
create RBA policy
setup/update RBA