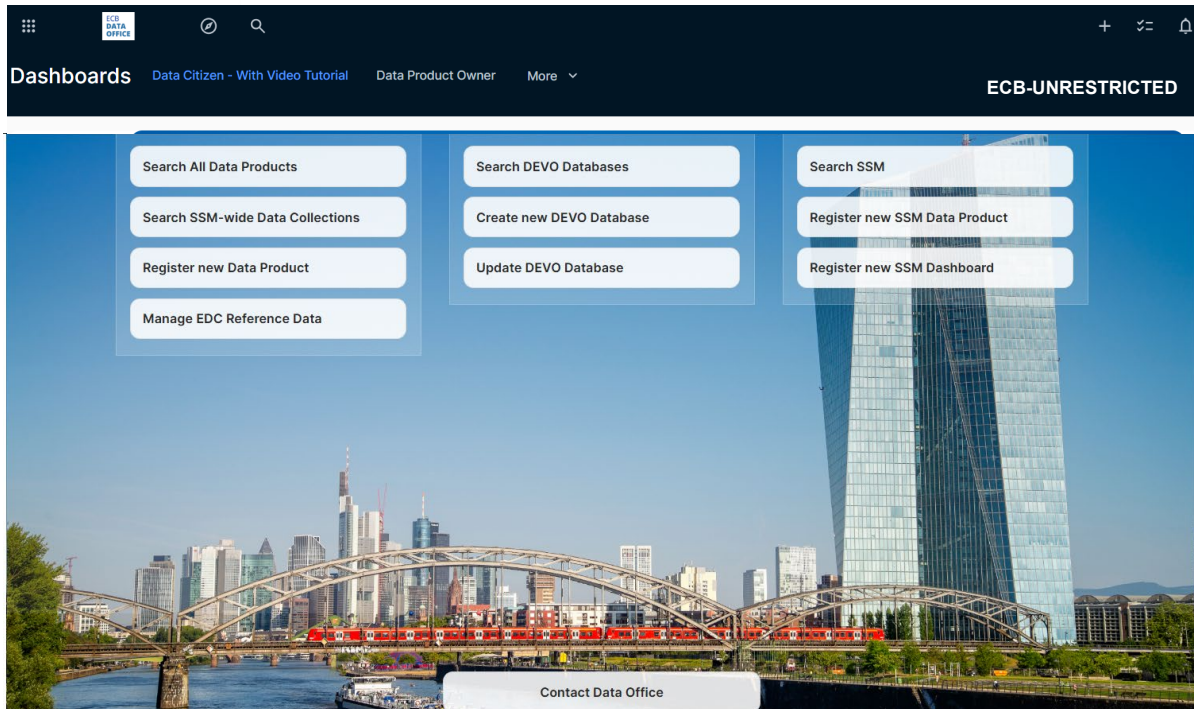


# From Coarse-Grained (RBAC) to Fine-Grained (ABAC) Access Control with the Data Catalogue implementation

IFC Lisbon – Workshop on  
Data Security and Privacy  
14/09/2026



**Bernadette Lauro**  
**Bernadette.Lauro@ecb.europa.eu**  
**DG Statistics/Data Office**

# The Challenges at the ECB

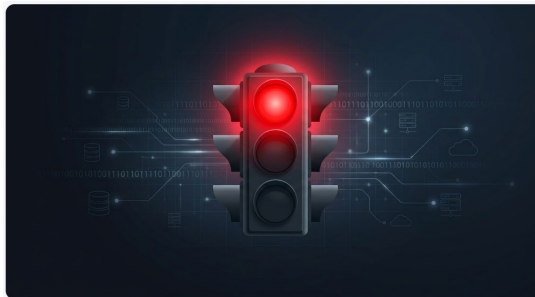
1. Compliance to Legally Binding Requirements (LBRs)
2. Complex IT and growing granular data environment
3. Transition: Manual versus Automated control



# Compliance: Access Control Management approaches

## **DAC - Discretionary**

Based on individual owner's decisions.  
Easy to apply.  
Maximum user's freedom.



## **MAC - Mandatory**

Strict control over access decided by authority's decision. High security level requirements. Rigid Setting.

## **RBAC - Role-Based**

Assigns permissions to roles and roles to users (according to functions).  
**Coarse-grained Access Control.**

## **ABAC/PBAC - Attribute-Based**

Dependent on decisions based on attributes' values (Who, What, When, How, to access data, as defined by owner) and Policy's rules. Fit to zero-trust based architectures.  
**Fine-grained Access Control.**

# Compliance: Role versus Attribute based access control

## RBAC

- Roles managed in Identification Access Management System



The Catalogue makes roles needed to access data **more transparent**

*Migration to  
attribute/policy-based  
access control*



Example of attribute and rule definitions:

- The **X report**
- saved in the Knowledge Management Repository (DARWIN)
- can only be accessed **with business justification Y**
- by H-band** or above in DG Statistics or SSM
- until the **embargo period** expires.

(what)  
(where)  
(why)  
(who)  
(when)



# Compliance: Policy evaluation

Example of policy applied to the TABLEAU Dashboard

**Security Level:** Restricted

**Permissions:**

**Staff members** with **Security level** Medium and above: Read

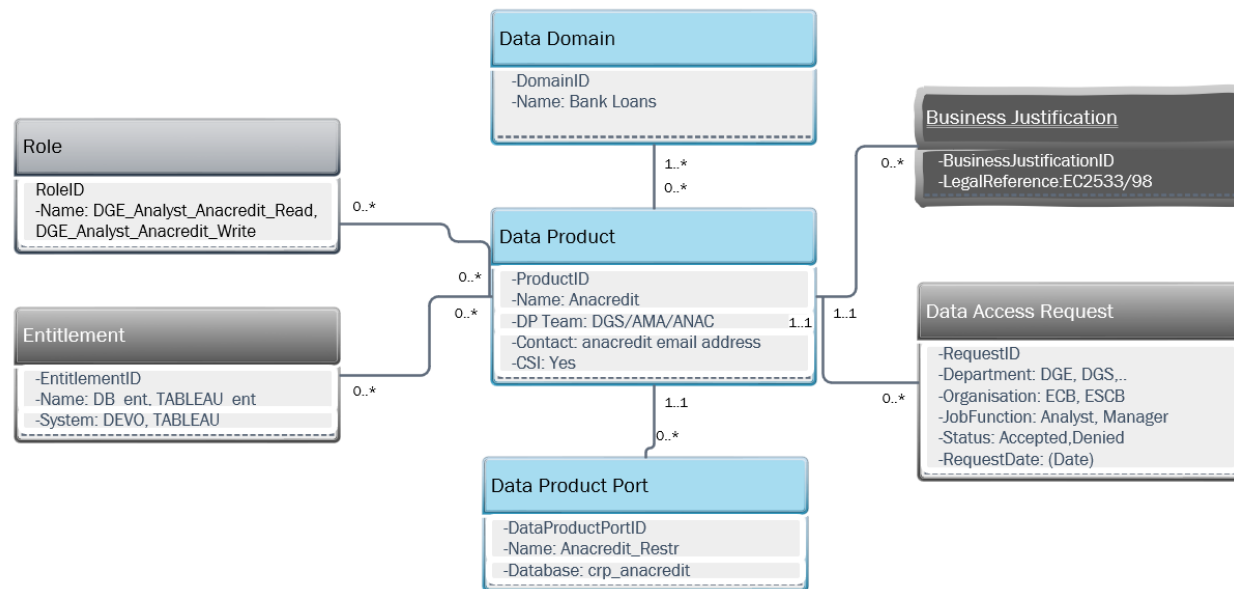
**Staff members** with **Security level** High: Read/Write

**Allowed devices:** company issued

**Embargo until:** 5PM

| Attributes                                                                                                                                                             | Evaluation           | Evaluation      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>Who:</b><br><b>Role:</b><br><b>Security Level:</b><br><b>Department:</b><br><b>Location:</b><br><b>Device:</b><br><b>Access Time:</b><br><b>Permission Request:</b> | = James Wrigh<br>= Consultant<br>= High<br>= DGMF<br>= On site<br>= Company Laptop<br>= 2 PM<br>= Write | = Tim Vod<br>= Manager<br>= Medium<br>= DG HR<br>= Offsite<br>= Mobile phone<br>= 10 PM<br>= Write |

# Complex IT - Growing Data environments: Catalogue's Asset Model



- Centralized, **metadata-driven system** for managing **data products** access.
- Can support RBAC and ABAC **hybrid approach** for smoother transition.
- It includes entities with metadata fields for **Roles** and **Permissions** required to access data products.

# Complex IT - Growing Data environments:

## Types of Data Products - Special Cases



### Embargoed

**Data:** access for authorised users during the restricted period, while others must wait until the embargo is lifted.



### Restricted

**repositories:** data that can be accessed only through roles specific for accessing the repository in which they reside.



### Confidential Statistical Information (CSI)\*:

imposes users to provide a valid business justification to access them, for example a Need to Know.



### Other Legally Binding Requirements

**(LBR):** Some datasets have contractual access restrictions, such as limiting access to specific business units or job roles.

\*See [COUNCIL REGULATION \(EC\) No 2533/98 of 23 November 1998](#)

# Transition - Manual versus Automated control:

## Challenges of transitioning from RBAC to ABAC



**Transition from RBAC to ABAC: maintaining a coexistent access models.** While RBAC assigns access based on pre-defined roles, ABAC uses attributes like data product identifiers, confidentiality levels, and user-specific criteria.



**Standard naming convention for entitlements** is crucial. It ensures that access policies are consistently applied, allowing for easy reconciliation of “who accesses what and when.”

*E.g.*

**Legacy RBAC :** *DGE\_Analyst\_Anacredit\_Read*

**New attributes:**

**Department=** *DGE*

**JobTitle =** *Analyst*

**DataProduct=** *Anacredit*

**PermissionLevel =** *Read*

# Transition - Manual versus Automated control

## Successful ABAC implementation depends (also) on..



- **Compatibility of risk level of integrated repositories**
  - E.g., **ability** to **exchange** resource attributes with authorization services
- **Clear business and technical requirements**
  - Especially in the **planning** phase
- **Clear roadmap**
  - **Sequence** repositories, capabilities, policies, user groups, in a controlled way
  - **Focus** on a limited set of high-values/medium complexity repositories
  - **Enhance** governance and compliance
  - **Plan** hybrid RBAC/ABAC model
- **Strong stakeholder management**
  - **Without alignment**, the catalogue may fail even if the technology works

# Conclusion

The Data Catalogue is a vital tool for managing **modern data environments**, it **accommodates data-centric access management** with benefits in terms of security, user experience, flexibility, complexity management and accountability, improving **transparency and compliance** but also preparing organizations for the **growing complexity** and **volume of data assets**.

It **supports the transition to ABAC** to address inefficiencies and risks of traditional access management systems **through automation of access control**.

The challenges in terms of complexity and investment require **enabling a hybrid RBAC-ABAC** model, with:

- **priority** given to the access to high-priority/medium complexity systems
- clear **roadmap** for requirements collection and implementation
- strong **stakeholder** management