

Advanced data security in Power BI



A step further than just rls

Hylke Peek

Hylke Peek



Data Consultant



@hylkepeek

 [Linkedin.com/hylkepeek](https://www.linkedin.com/hylkepeek)

I'm working on a lot of different stuff. Focus on **Azure** and **Power BI**.

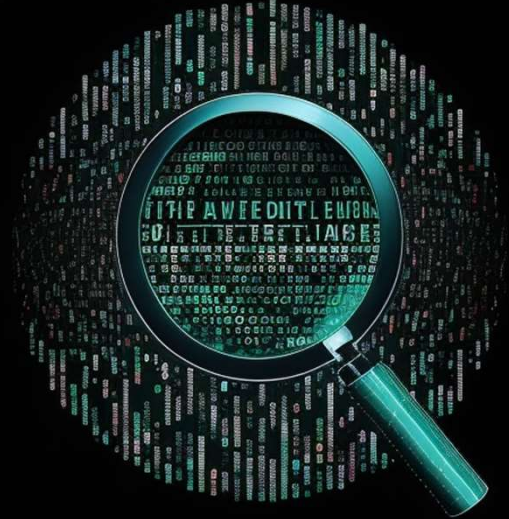
- Data Platform
- Datawarehousing
- Analytics
- Azure data solutions
- Power BI

Topics

The complexity of data security

The implementation

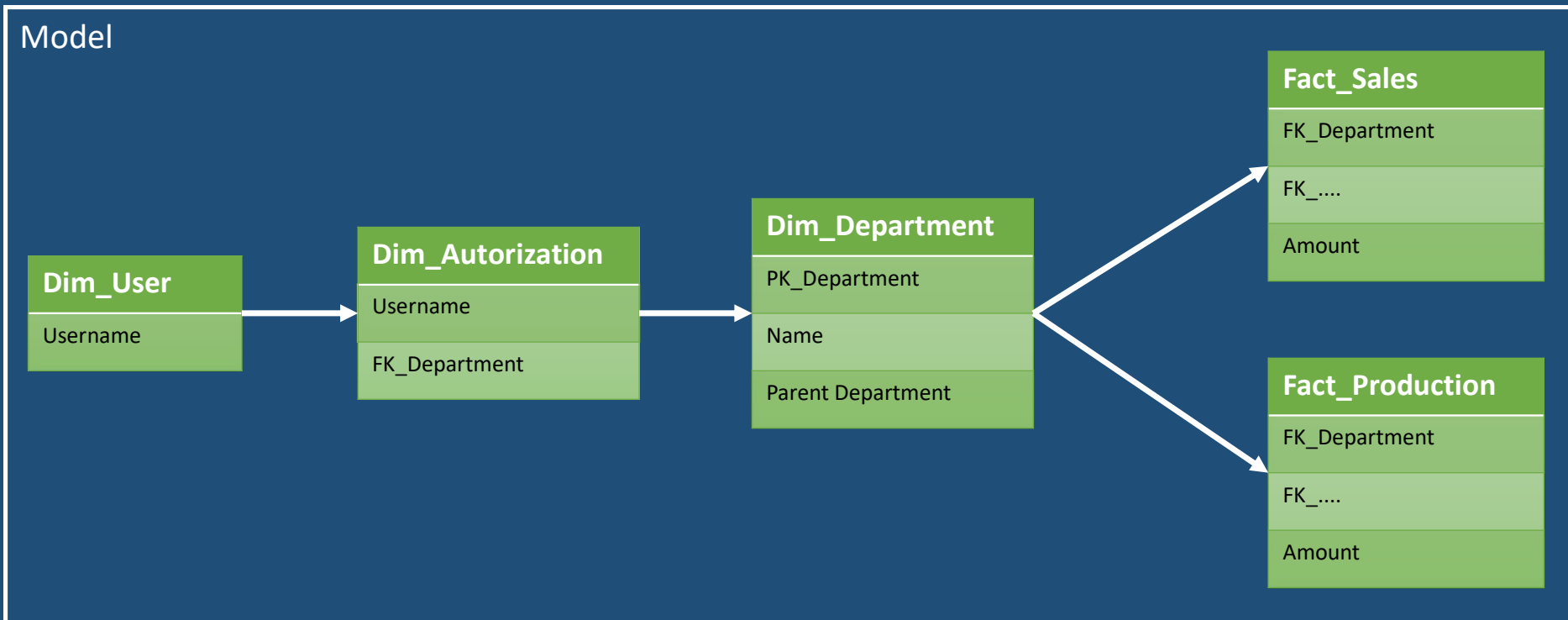
Takeaways





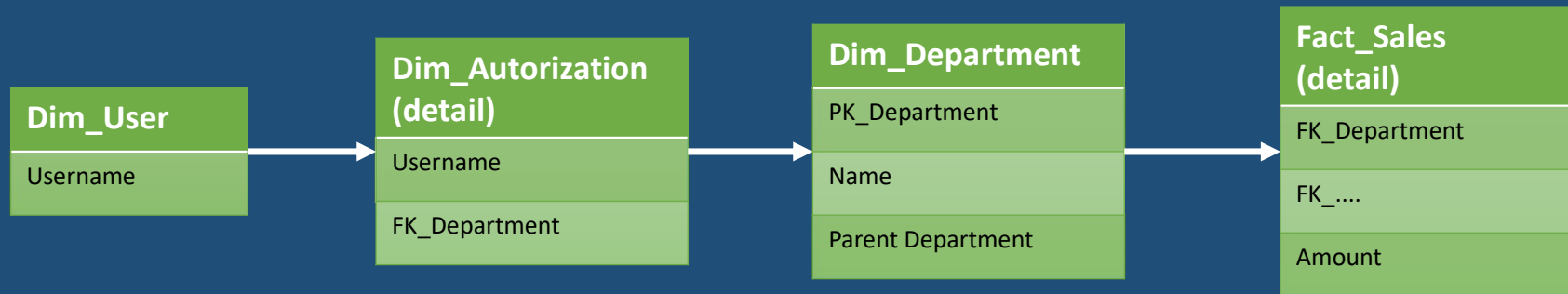
The complexity of data security

Scenario 1: Based on organization hierarchy

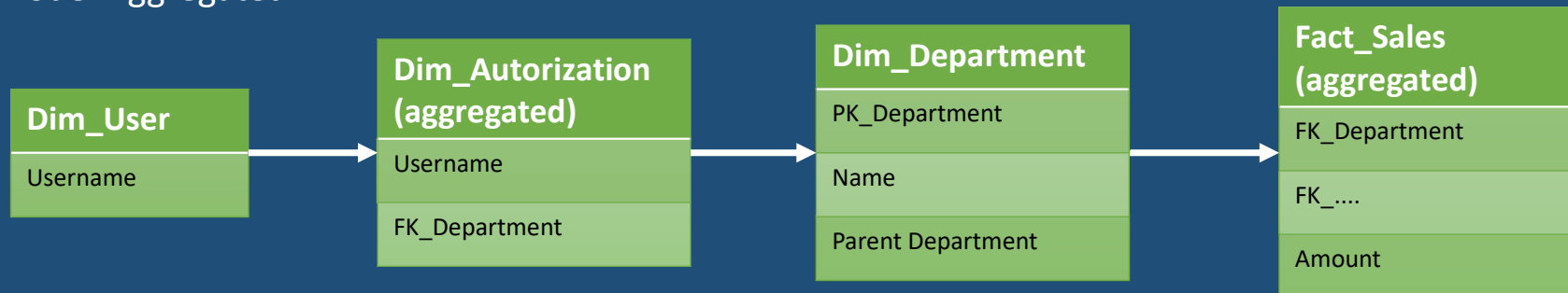


Scenario 2: Detail vs. Aggregation

Model Detail



Model Aggregated



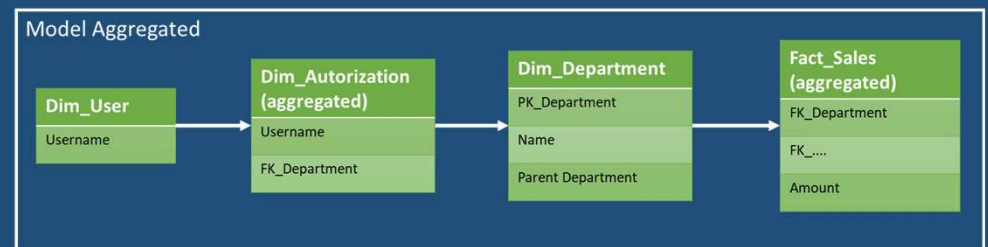
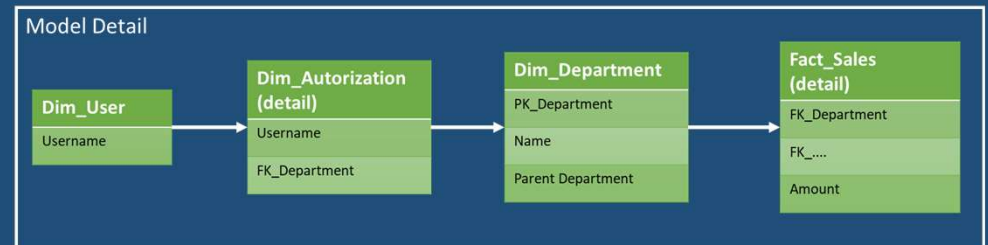
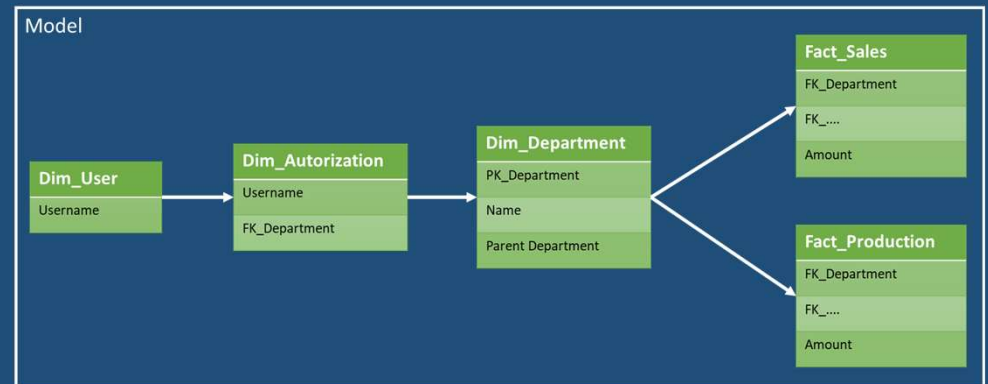
But what about...

Differences between domains?

Differences between roles?

Object Level Security

Without getting lost....



Example use case

Managers are allowed to see all data from **THEIR** departments.

e.g absenteeism per employee

Managers are allowed to see aggregated data from **OTHER** departments.

e.g absenteeism on department level

Managers are allowed to see date of birth from employees within **THEIR** departments **ONLY**.

e.g John is born on 03-05-1947

Managers are allowed to see aggregated client related data from **ALL** departments.

e.g Health care costs for your department are 4m.

Managers are **NOT** allowed to see detailed client data within **ANY** department.

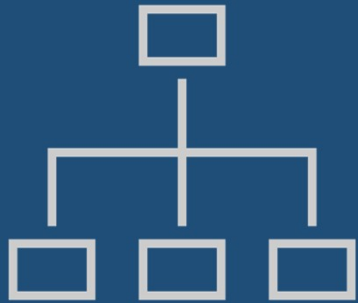
e.g Health care costs for Will are 500,-

Same for finance.

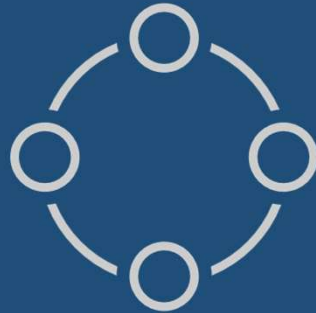
Care personnel are not allowed to see employee data but are allowed to client data in detail.

Aspects to data security

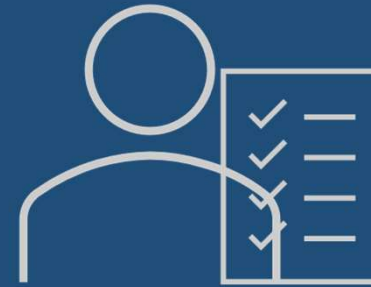
Organizational hierarchy



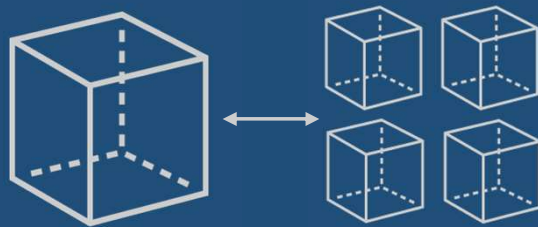
Domain



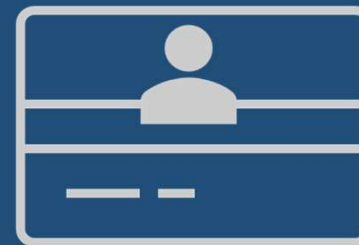
Roles



Granularity



PII data





The implementation

Setting up data security

Business – Clear understanding of this ‘business logic’

Source(s) – Organizational hierarchy and responsibilities

Microsoft Entra (AAD) – Security groups and group assignments

Data platform – Translate business logic to authorization definition

Data platform – Integrate authorization into your data model

Power BI – Configure data security, setup relationships and add/adjust measures

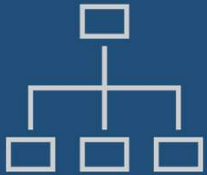


The background of the slide is a solid dark blue. A large, stylized arrow shape is formed by a horizontal bar extending from the left edge and a triangular point on the right. The word "Takeaways" is written in white, sans-serif font, centered within the horizontal bar of the arrow.

Takeaways

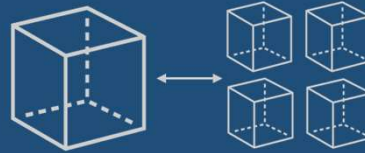
What makes it more complex?

Organizational hierarchy



Basic data security using RLS.

Granularity



1 authorization table is not enough because of different permissions on different granularity. Need changes to the data model.

Domain



Permission differs between domains so, we need separate authorization tables for each domain. Need changes to the data model.

Roles



The business logic behind the costcenters you're allowed to see differs between roles. Configure Entra and add logic for defining authorization.

PII data



OLS can be used with RLS but with limitations. You can't use 'conditional OLS'. Configure Power BI.

Takeaways

It's a team effort. Involve the business asap to have a clear understanding of their needs.

Define your scenario. Which aspects (Organizational hierarchy, granularity, domains, roles, PII data) are relevant and which are not?

When and how to configure each component (Entra, database, RLS, OLS, audiences) according to your scenario.

Create a dynamic solution where you can add new groups

Using RLS and OLS? → For each set of OLS-permissions, create a separate role. Works as expected in basic scenario's.

Conditional PII for more complex scenario's, limit build permissions or add PII data to fact tables.



Extra takeaways

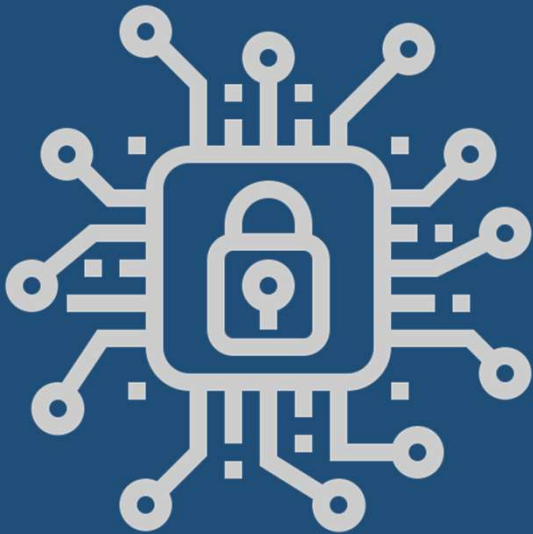
Automate group assignment based on functioncode from a source.

Be critical about who need to build reports.

With AAS is more or less the same. But no many-to-many relationships and build permission like Power BI.



Advanced data security in Power BI



THANK YOU

Hylke Peek