Role-Based Access Control (RBAC) vs. Attribute-Based Access Control (ABAC)

IAM Conference
February 2025

pwc

Welcome

PwC

Henrik Kaaber
T: 2887 9798
E: henrik.kaaber@pwc.com

Learn more about PwC's transformative consulting capabilites on our website:
pwc.dk/consulting

PwC

Tim Olsen
T: 2159 0276
E: tim.olsen@pwc.com

Learn more about PwC's transformative consulting capabilites on our website:
pwc.dk/consulting

Agenda
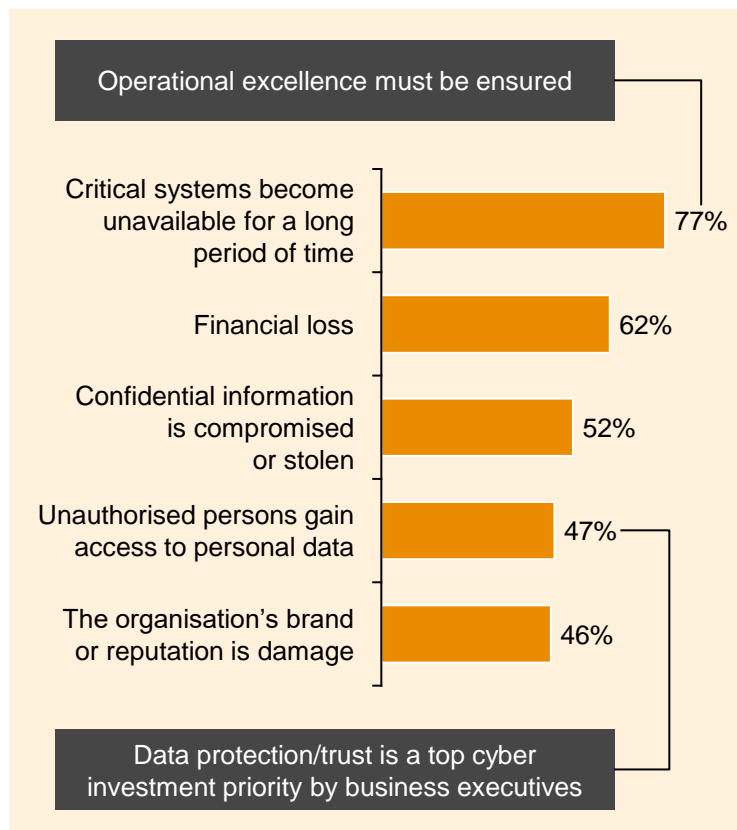
01. Threats, concerns and investment outlook

02. Evolution of access control models

03. The differences between RBAC and ABAC

04. **Ex:** Implementing ABAC to support strategic requirements

05. Our approach to implementing ABAC

We are at an inflection point where identity-related cyber threats and concerns are evolving, and budgets are increasing

Concerns, prioritisation and investment outlook, PwC Cybercrime Survey; Global Digital Trust Insights

Operational excellence must be ensured

Concern	%
Critical systems become unavailable for a long period of time	77%
Financial loss	62%
Confidential information is compromised or stolen	52%
Unauthorised persons gain access to personal data	47%
The organisation's brand or reputation is damage	46%

Data protection/trust is a top cyber investment priority by business executives

% of CXOs and IT professionals placing IAM as a top 5 priority investment

Year	%
2017	34%
2018	36%
2019	32%
2020	30%
2021	34%
2022	29%
2023	26%
2024	30%

64% of organizations expect to increase their cybersecurity budgets by more than 10%

	%
Up to 10%	28%
More than 10%	64%
Unsure	8%

Key takeaways

We are at an inflection point where:

- Cyber incidents can be traced back to IAM
- IAM is a top 5 investment priority by execs
- Majority of orgs. expect budget increases by more than 10%

Historically, we have seen a focus on IT- and **Cyber initiatives that are misaligned** with the overarching **business model** and **strategies** of organisations.

There is an **opportunity** to capitalise on attention and focus to **develop and implement** the right, **strategically aligned initiatives.**
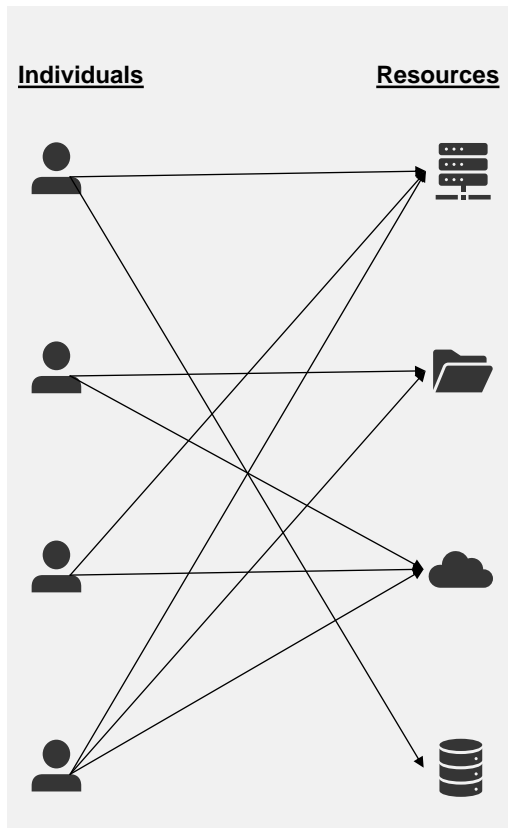
Today, you will see an example focused on combining **ABAC with RBAC to evolve the access control capabilities** of fictitious organisations to better support their underlying business model.

Access control has evolved from 1970s to today to increase security, compliance and streamline business processes

Discretionary Access Control (DAC)

Individuals   Resources

Mandatory Access Control (MAC)
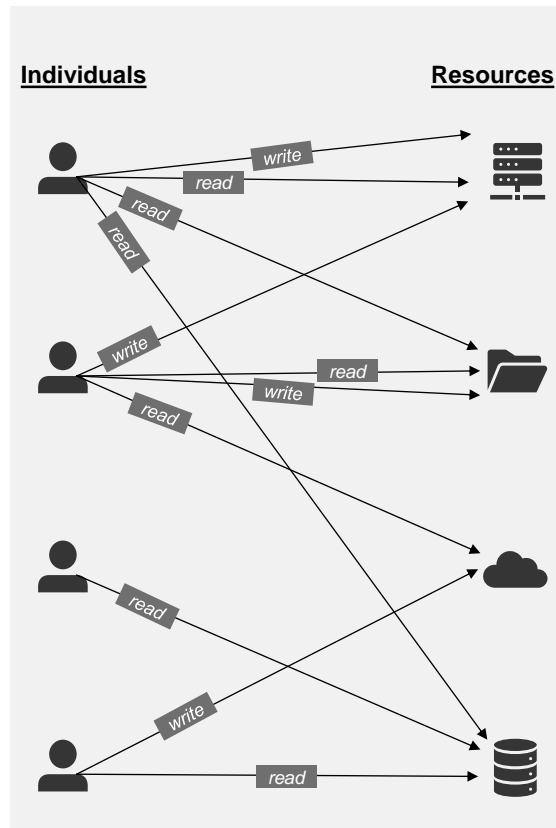
Individuals   Resources

write
read
read
read
write
read
write
read
read
write
read

1970s - 1990s

Role-Based Access Control (RBAC)

Individuals   Roles   Resources

Role 1
Role 2
Role 3

Groups

1990s - now

Attribute-Based Access Control (ABAC)

Individuals   Resources

Evaluation
Attributes
Context
Subject
Object
Policies
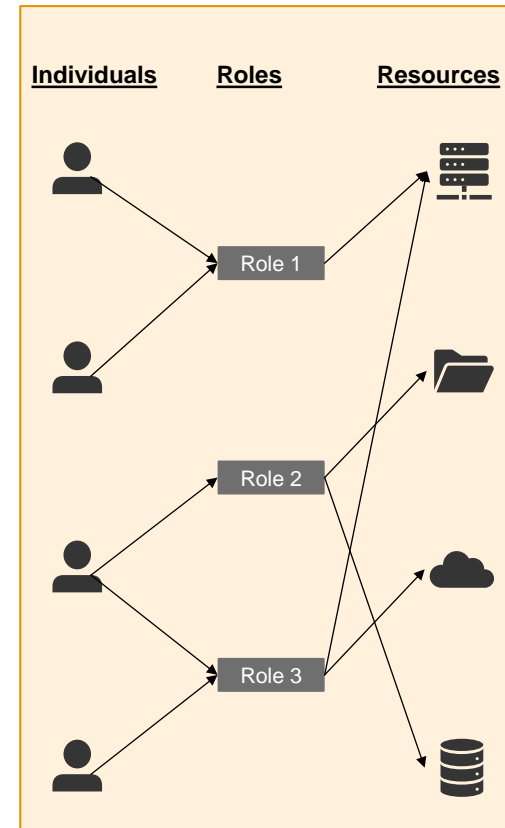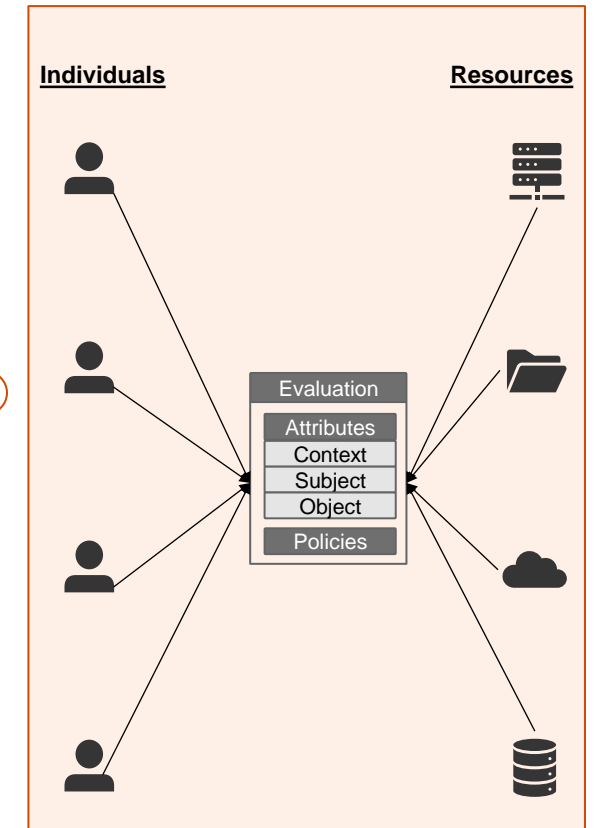
2010s - now

There are some conceptual differences between RBAC and ABAC

Role-Based Access Control (RBAC), static

New employee without access

What is their job function?

Current employees in the department

3 permissions

Role 1

CustomerService_Department_System2

Role 2

Manager_Department_System2

Application portfolio

Application 1
Prod. A | Prod. B
Prod. C | Prod. D

Application 2
Cust. Service | Manager
Read | Sys Admin
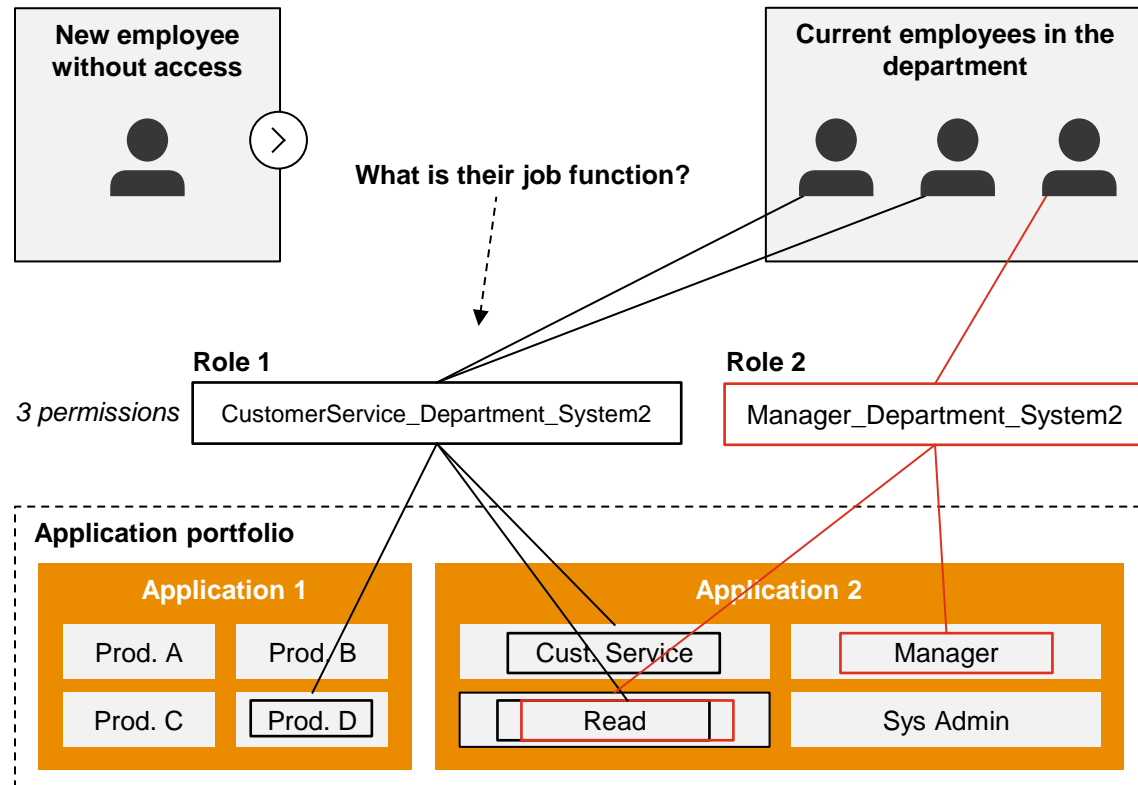
Attribute-Based Access Control (ABAC), dynamic

Attributes Context

| Job Function | Time of Day | Geographical Location | Network | Permissions | Certifications |
| Project Allocation | Device | Country of Origin | Owner | Risk Level | Sensitivity |

User Subject

Manager | External

Customer Service | Sys. Admin

Federated User | Student Worker

Fine Grained Access Evaluation

Rules

Policies

Enforcement

Resource Object

Application 1
Data
Segment A
Segment B

Application 2
Data
Segment A
Segment B

When should you use what, and how do you determine a need for either RBAC or ABAC?

RBAC / ABAC paradigms and interfaces

RBAC	Hybrid	ABAC

A

- Access qualifiers are relatively static

- Logically grouped accesses for automatic permission assignment based on rules or assignment

- Requires well-defined understanding of job functions and responsibilities

- Governance is key (roles and rules)

B

RBAC informs ABAC by providing roles as an attribute

RBAC
You are a nurse and receives access to these clinical applications

ABAC
Your level of access and information available to you depends on your location, device, time of day and assigned patients

C

- Access qualifiers are dynamic

- Dynamic permission assignment based on policy decisions informed by attributes

- Requires classified and categorised data that you can trust

- Governance is key (attribute data and policies)

Things to keep in mind

RBAC and ABAC does **not** have to be an **either/or** – it **can be a both/and**.

The **right model** for you depends on **your use-cases**, **business needs** and **internal readiness**.
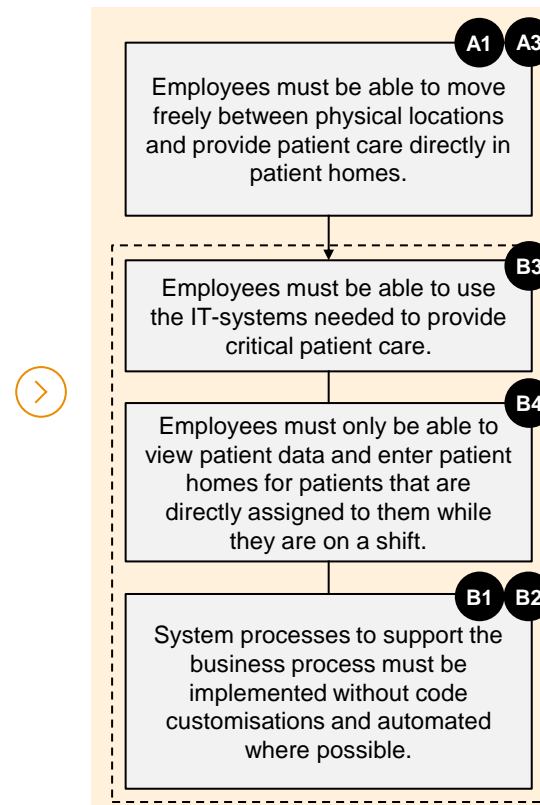
- Do we need to enforce access during runtime? (context)

- Is creating and maintaining required data and information owned and governed by dedicated responsibles? (subject)

- Do we have an implemented process for classifying and categorising data? (object)

Let us take an example where a strategic business requirement leads to an adjustment in your access control choices
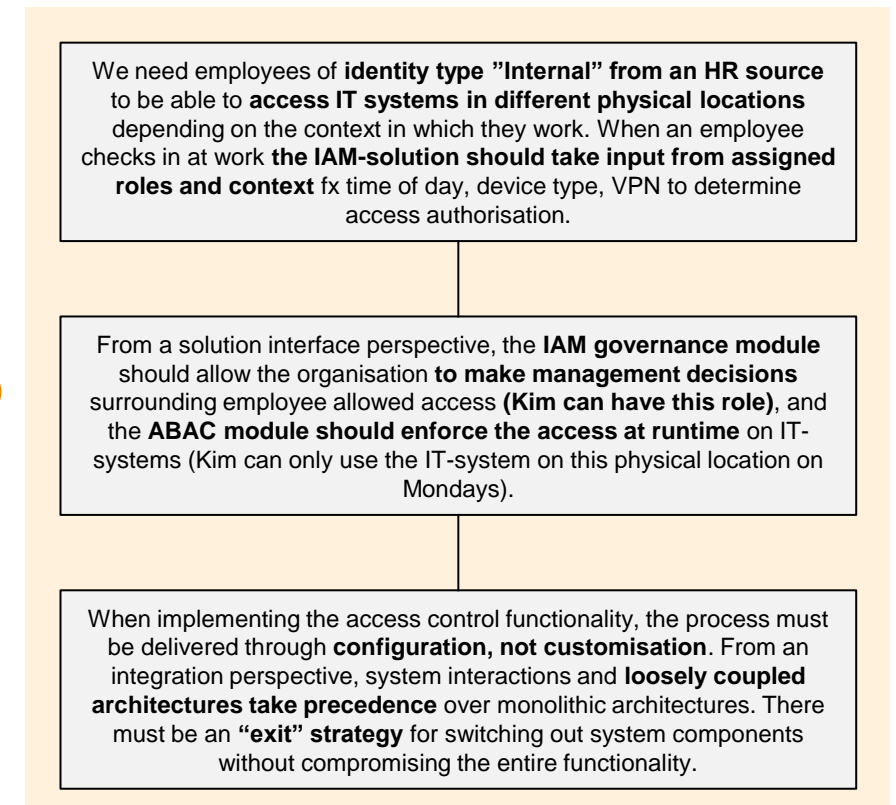
Strategic context for a healthcare provider

Internal Environment

External Environment

Business model ↔ Business Strategy

Strategic Business Objectives

A1 Patient Experience
A2 Ressource Optimisation
A3 Employee Engagement
A4 Clinical Exellence

IT Strategy

B1 Standar-disation
B2 IT Cost Optimisation
B3 Operational Excellence
B4 Security & Compliance

Business and IT requirements

A1 A3 Employees must be able to move freely between physical locations and provide patient care directly in patient homes.

B3 Employees must be able to use the IT-systems needed to provide critical patient care.

B4 Employees must only be able to view patient data and enter patient homes for patients that are directly assigned to them while they are on a shift.

B1 B2 System processes to support the business process must be implemented without code customisations and automated where possible.

Translation to IAM

We need employees of **identity type "Internal" from an HR source** to be able to **access IT systems in different physical locations** depending on the context in which they work. When an employee checks in at work **the IAM-solution should take input from assigned roles and context** fx time of day, device type, VPN to determine access authorisation.

From a solution interface perspective, the **IAM governance module** should allow the organisation **to make management decisions** surrounding employee allowed access **(Kim can have this role)**, and the **ABAC module should enforce the access at runtime** on IT-systems (Kim can only use the IT-system on this physical location on Mondays).

When implementing the access control functionality, the process must be delivered through **configuration, not customisation**. From an integration perspective, system interactions and **loosely coupled architectures take precedence** over monolithic architectures. There must be an **"exit" strategy** for switching out system components without compromising the entire functionality.
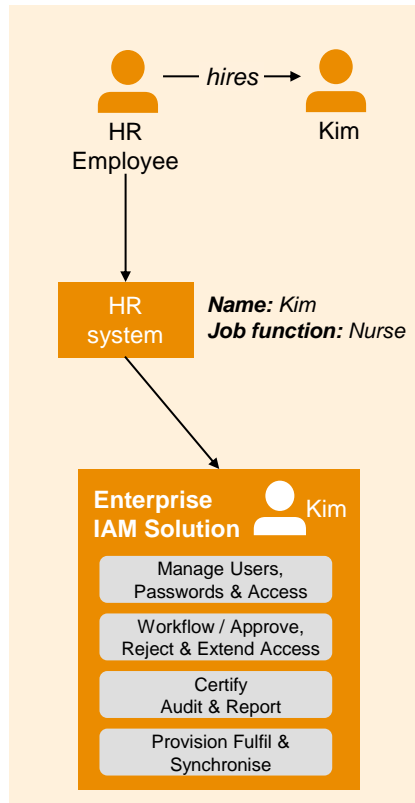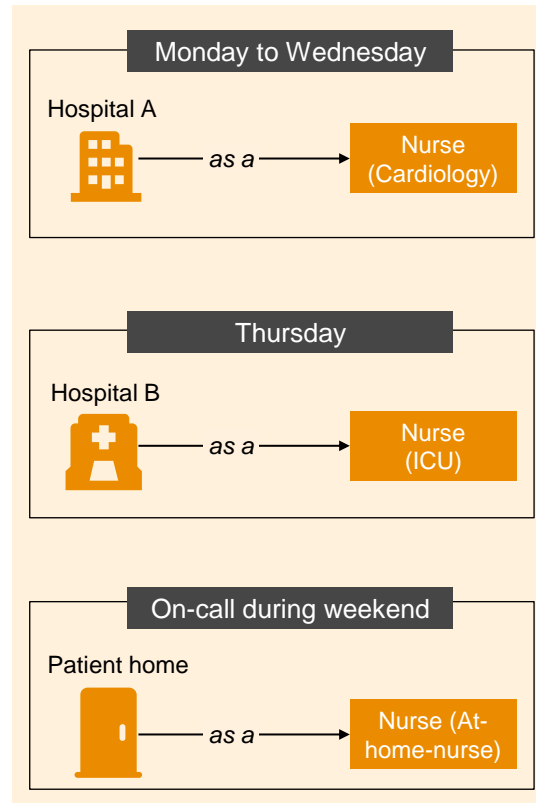
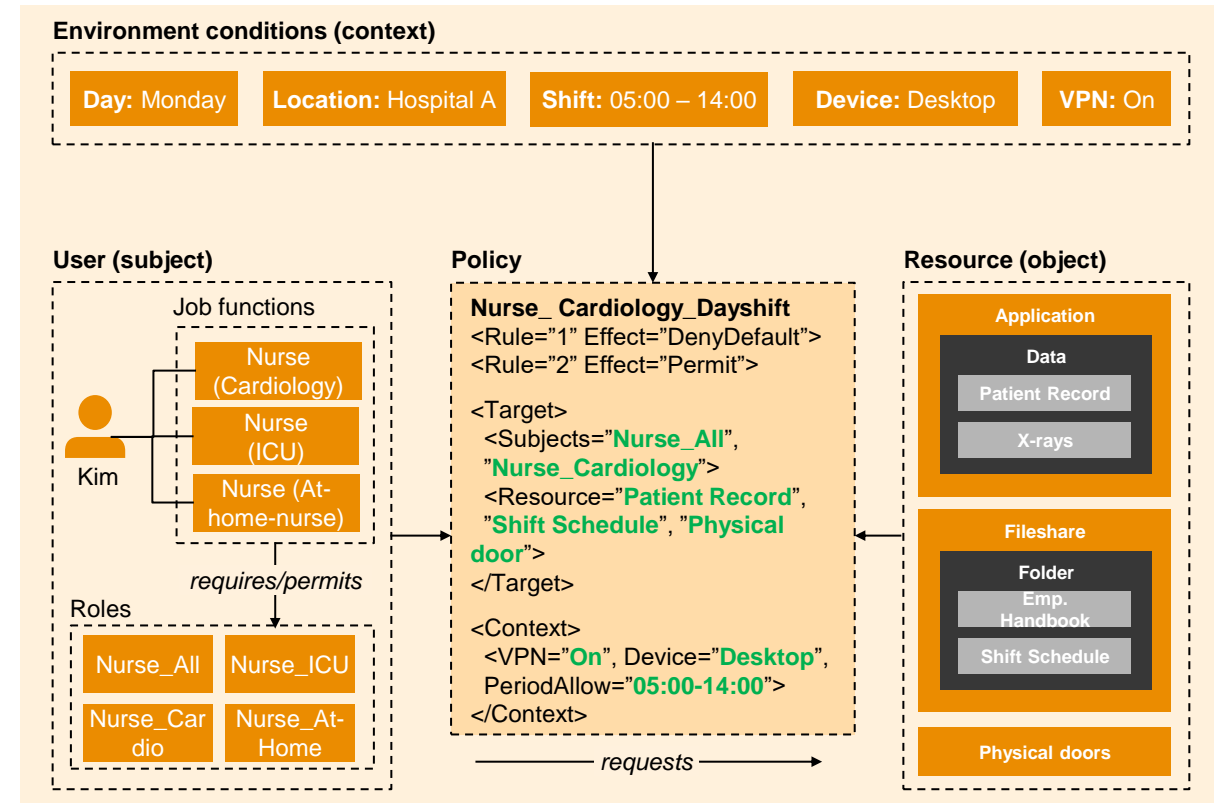# Based on the business requirement, we need a way to grant access based on a dynamically changing context
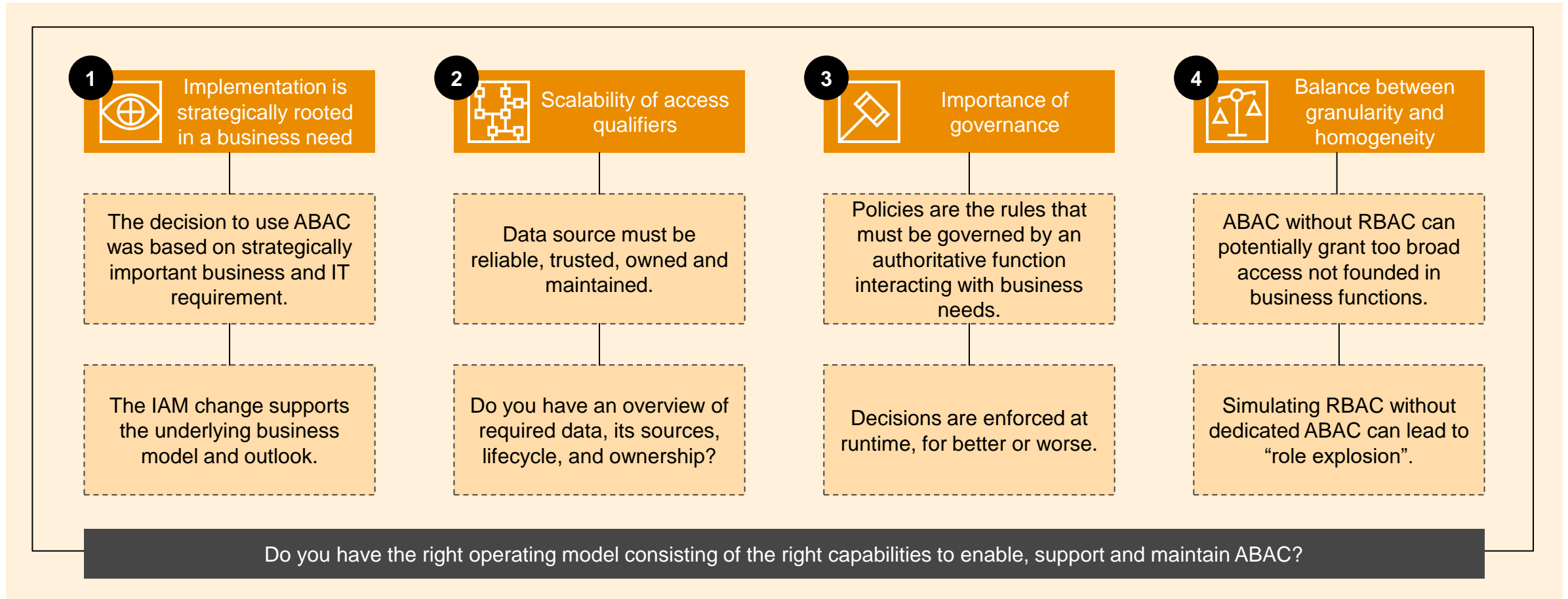
Kim's identity is created

HR Employee — hires → Kim

HR system
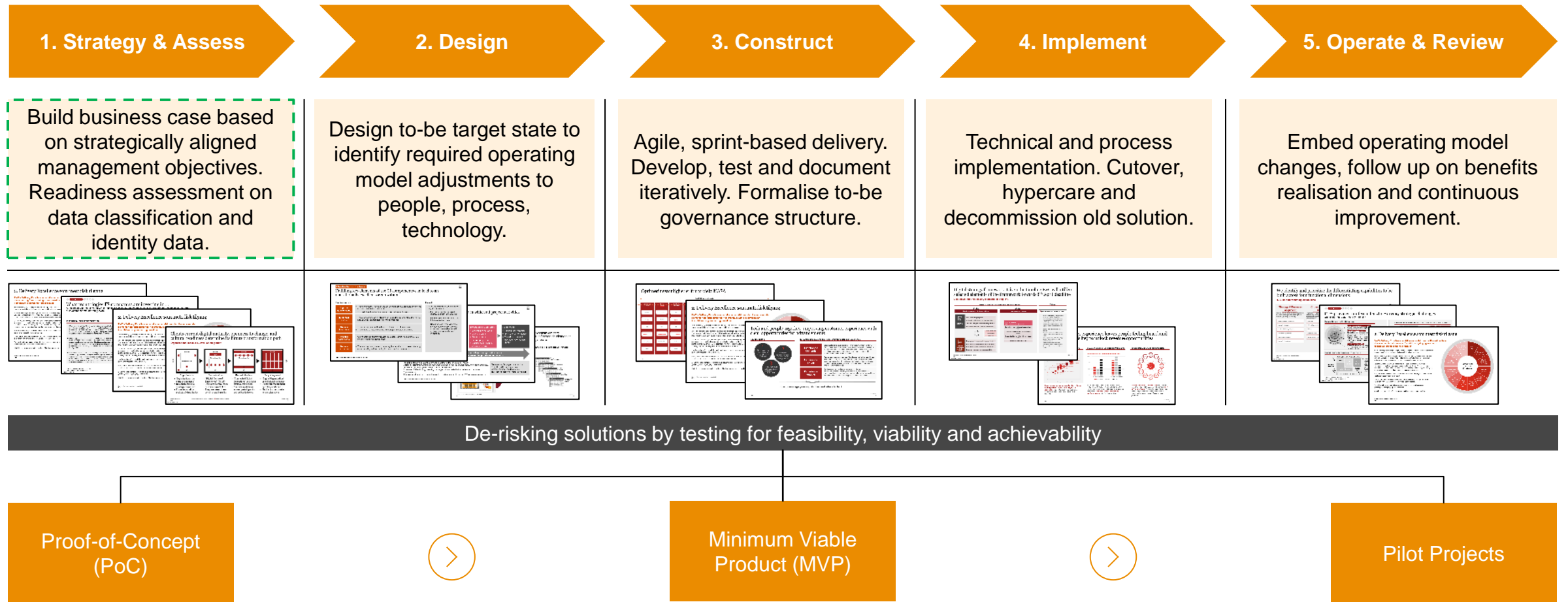
Name: *Kim*
Job function: *Nurse*

Enterprise IAM Solution — Kim

- Manage Users, Passwords & Access
- Workflow / Approve, Reject & Extend Access
- Certify Audit & Report
- Provision Fulfil & Synchronise

Kim's work location and schedule

Monday to Wednesday

Hospital A — as a → Nurse (Cardiology)

Thursday

Hospital B — as a → Nurse (ICU)

On-call during weekend

Patient home — as a → Nurse (At-home-nurse)

Kim is at work

Environment conditions (context)

Day: Monday | **Location:** Hospital A | **Shift:** 05:00 – 14:00 | **Device:** Desktop | **VPN:** On

User (subject)

Job functions

Kim
- Nurse (Cardiology)
- Nurse (ICU)
- Nurse (At-home-nurse)

requires/permits

Roles
- Nurse_All
- Nurse_ICU
- Nurse_Cardio
- Nurse_At-Home

Policy

Nurse_ Cardiology_Dayshift
<Rule="1" Effect="DenyDefault">
<Rule="2" Effect="Permit">

<Target>
 <Subjects="**Nurse_All**",
 "**Nurse_Cardiology**">
 <Resource="**Patient Record**",
 "**Shift Schedule**", "**Physical door**">
</Target>

<Context>
 <VPN="**On**", Device="**Desktop**",
 PeriodAllow="**05:00-14:00**">
</Context>

requests →

Resource (object)

Application
- **Data**
  - Patient Record
  - X-rays

Fileshare
- **Folder**
  - Emp. Handbook
  - Shift Schedule

Physical doors

There are 4 key takeaways from the example to keep in mind

1 Implementation is strategically rooted in a business need

The decision to use ABAC was based on strategically important business and IT requirement.

The IAM change supports the underlying business model and outlook.

2 Scalability of access qualifiers

Data source must be reliable, trusted, owned and maintained.

Do you have an overview of required data, its sources, lifecycle, and ownership?

3 Importance of governance

Policies are the rules that must be governed by an authoritative function interacting with business needs.

Decisions are enforced at runtime, for better or worse.

4 Balance between granularity and homogeneity

ABAC without RBAC can potentially grant too broad access not founded in business functions.

Simulating RBAC without dedicated ABAC can lead to "role explosion".

Do you have the right operating model consisting of the right capabilities to enable, support and maintain ABAC?

If we were the organisation in scope, this is the 5 step-process we would use to approach ABAC

1. Strategy & Assess	2. Design	3. Construct	4. Implement	5. Operate & Review
Build business case based on strategically aligned management objectives. Readiness assessment on data classification and identity data.	Design to-be target state to identify required operating model adjustments to people, process, technology.	Agile, sprint-based delivery. Develop, test and document iteratively. Formalise to-be governance structure.	Technical and process implementation. Cutover, hypercare and decommission old solution.	Embed operating model changes, follow up on benefits realisation and continuous improvement.

De-risking solutions by testing for feasibility, viability and achievability

Proof-of-Concept (PoC) → Minimum Viable Product (MVP) → Pilot Projects

Thank you

www.pwc.dk

Succes skaber vi sammen …