KPMG

Why all Public Agency management should care about **Identity & Access Management**

September 2016

kpmg.com

Agenda

Why IAM

Implementing IAM

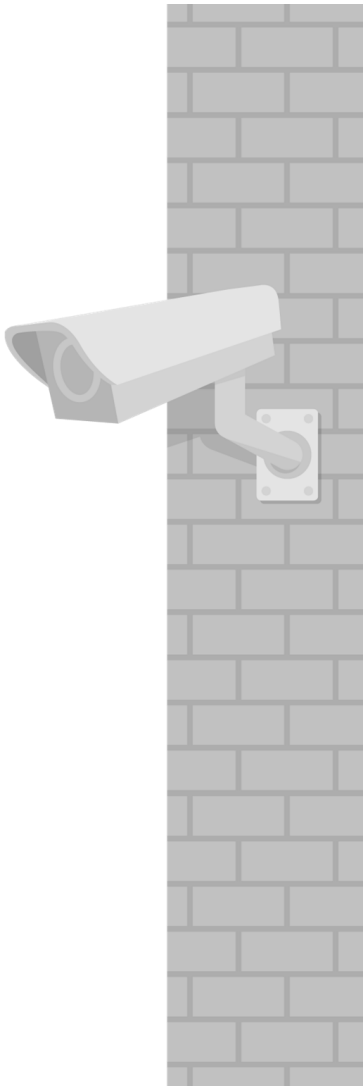
The CSO Viewpoint

Q&A

KPMG

Why Identity & Access Management?

Digital Identities – Risk Considerations



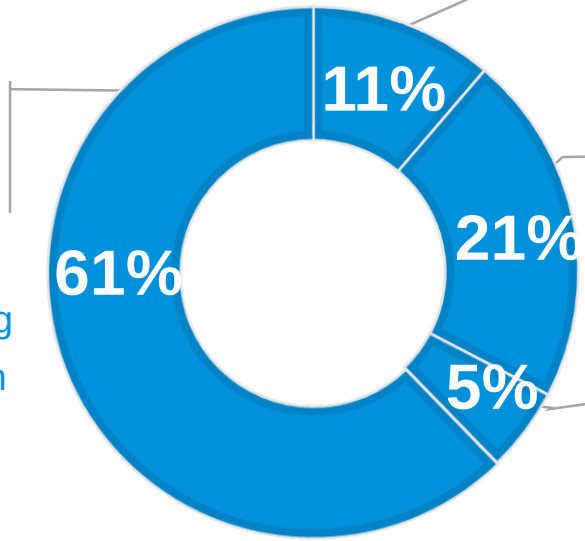
If you think Identity & Access Management is just another IT issue, you may have reason to worry.

Digital Identities – Risk Considerations

Technology enables and weak controls fuel the fraud

Weak Internal Controls

- Access Controls
- User Provisioning
- User Certification
- Roles
- Monitoring



Collusion circumventing good controls

Reckless dishonesty regardless of controls

Other

Digital Identities – Business Value of Identity & Access Management

The security benefits associated with Identity & Access Management are obvious:

- Improved ability to provide audit data
- Improved efficiency in onboarding new staff
- Removes IT from the (non IT based) provisioning loop

KPMG

Implementing Identity & Access Management

Scope of Our Discussion

Identity & Access Management

Processes + Controls + Technologies

Changing approach towards IAM

Creating, maintaining and using a single digital identity.

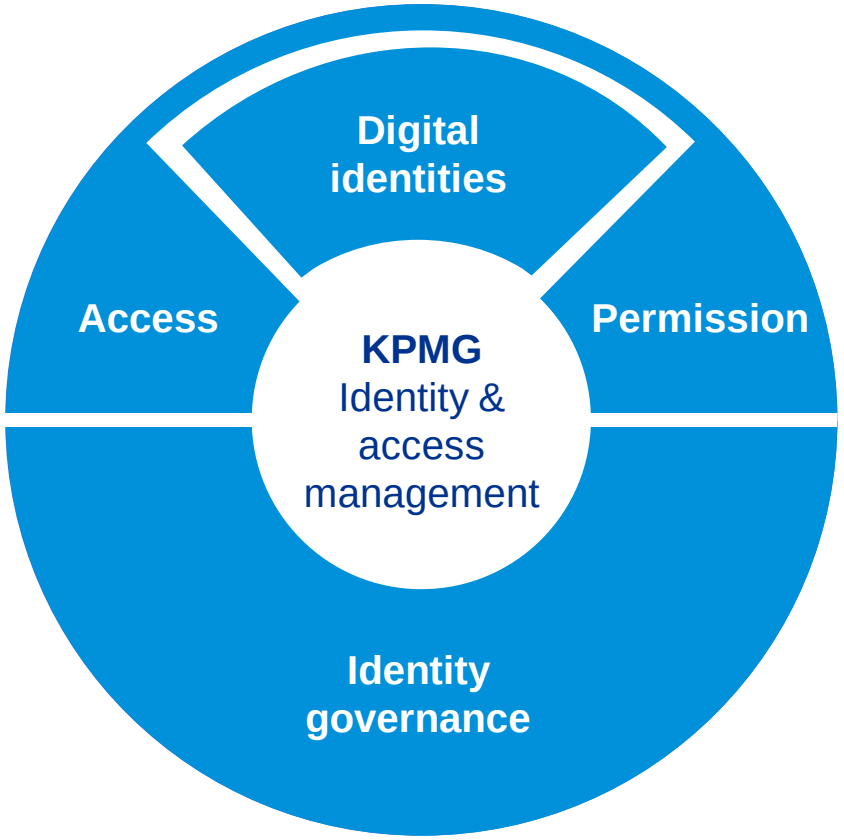
Mitigating risk by focusing on getting the *right people* the *right access* to the right information at the *right time*.

Importance of Identity Governance

Identity Governance

=

Rationalization of access to IT Assets i.e. Who has access to what and why?



Managing Access in Your Organization

Identity Management is gateway for digital identity into enterprise systems

Good practice

HR owns

- Ensure employee is who she claims to be.
- Job Role, Job Responsibility & place in organization

IAM is

- One degree separation from HR
- Trusts HR data as the source of truth and acts upon it
- Identity and Organization related attributes from HR are immutable

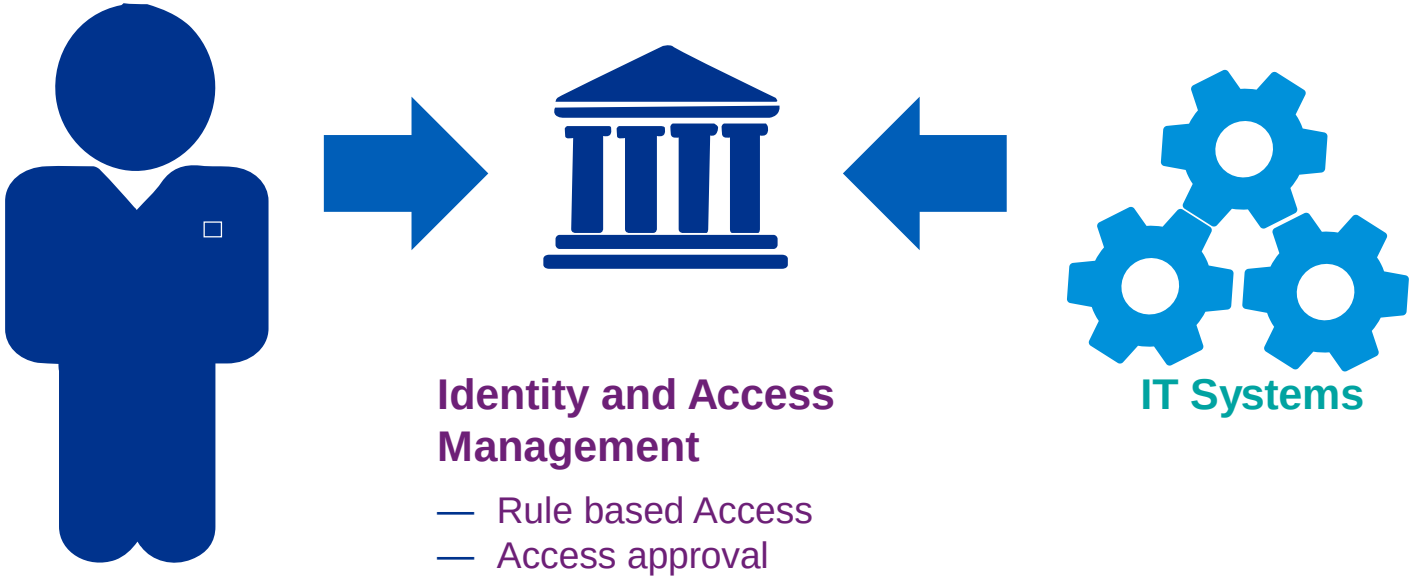
Plan for HR alignment in overall strategy

IAM for Assurance

Identity Risk Profile

Assurance Measures

Risk of Access

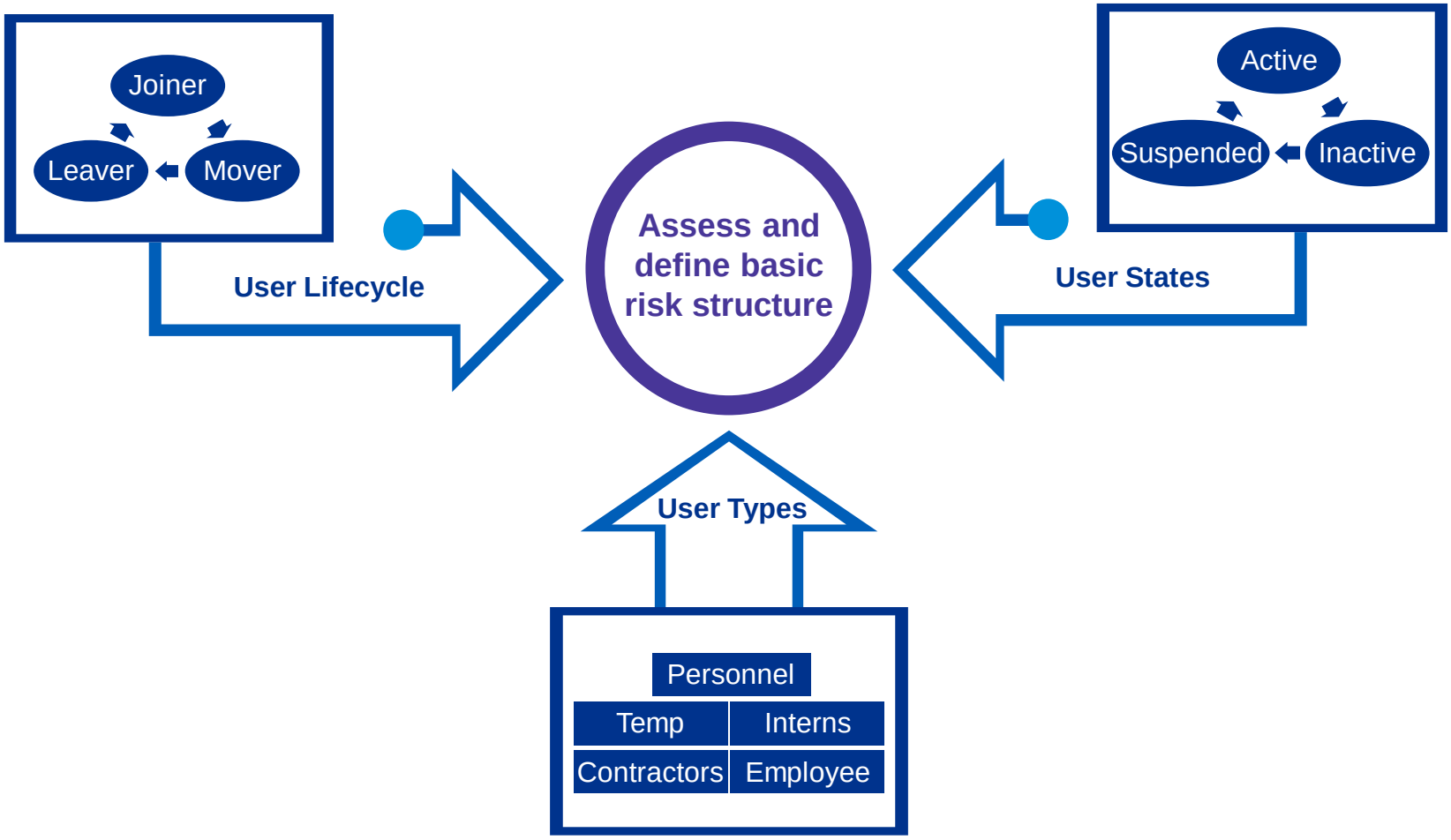


Identity and Access Management

- Rule based Access
- Access approval processes
- Access Review/ Attestation/ Certification

IT Systems

User Access Lifecycle

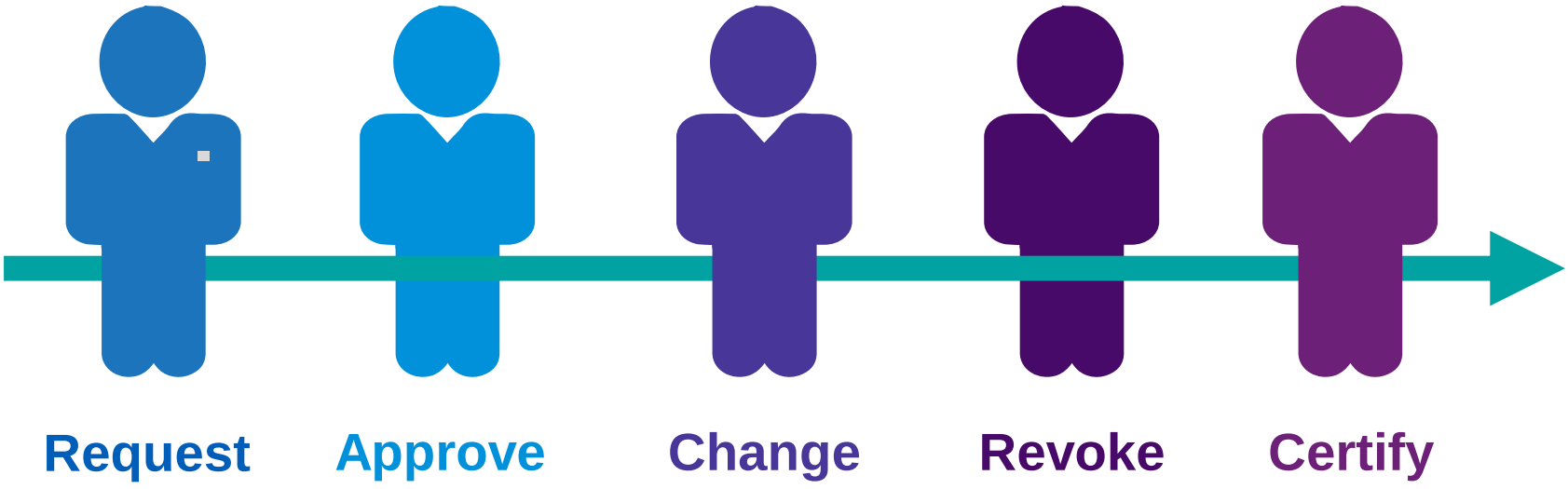


Good Practice

- Collaborate with Information Security, HR and other responsible teams to assess risk posture and define onboarding process
- Align with organization's culture
- Access to systems is automated (Birth right role)

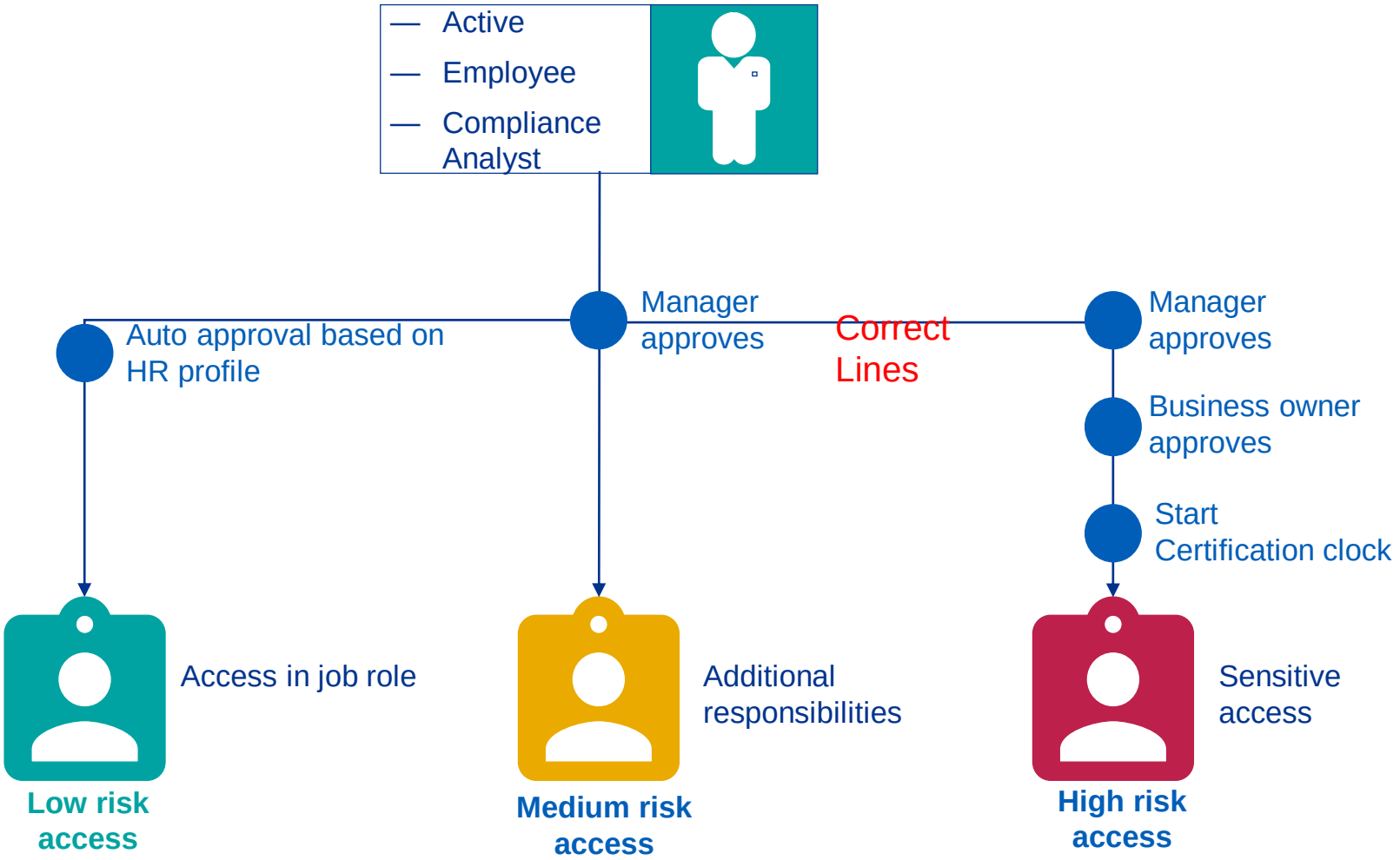
Identity management process

Access lifecycle must encompass all workforce members.



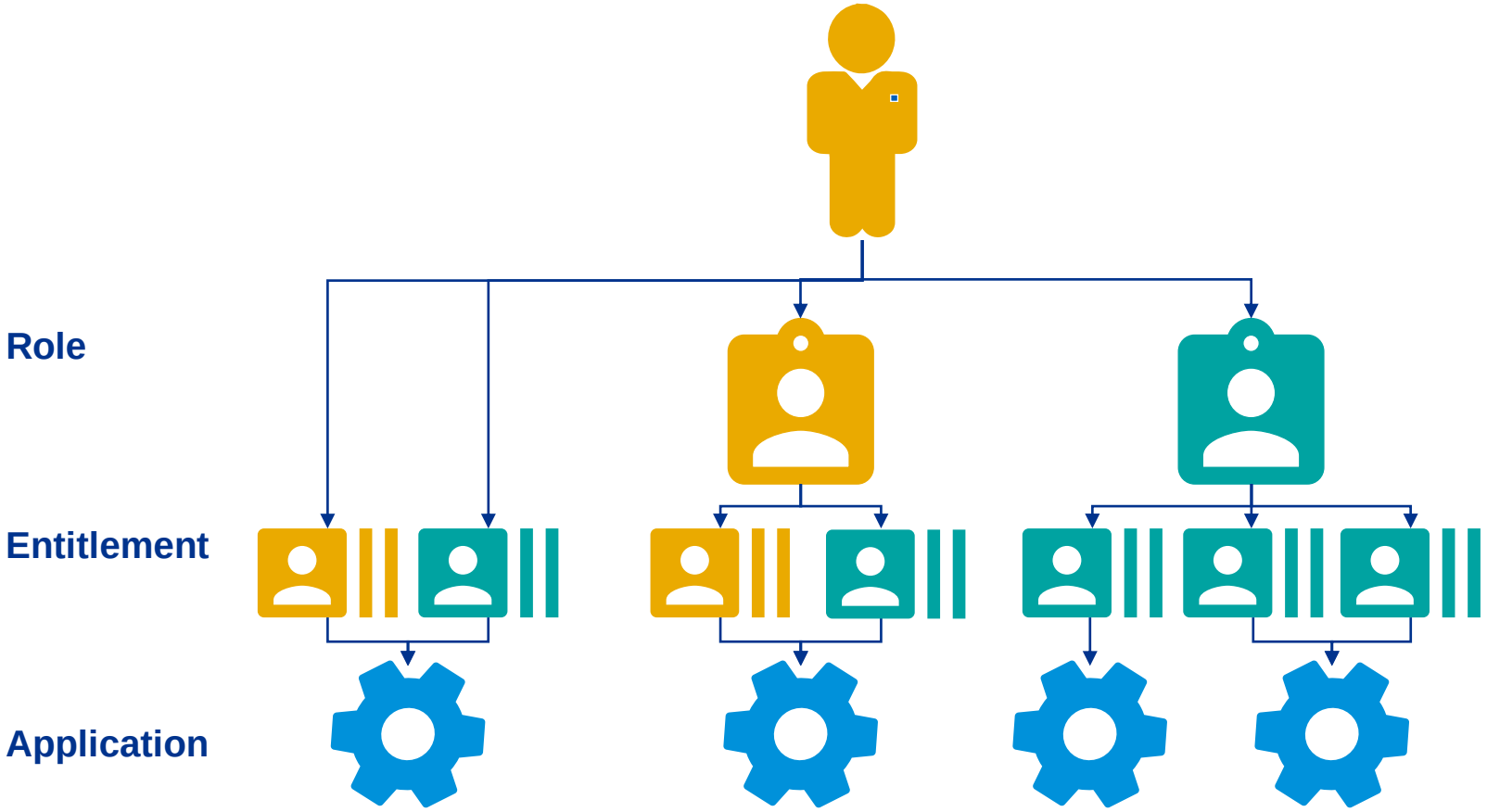
Principle of least privilege requires implementation of complete lifecycle.

Managing Access - Joiner

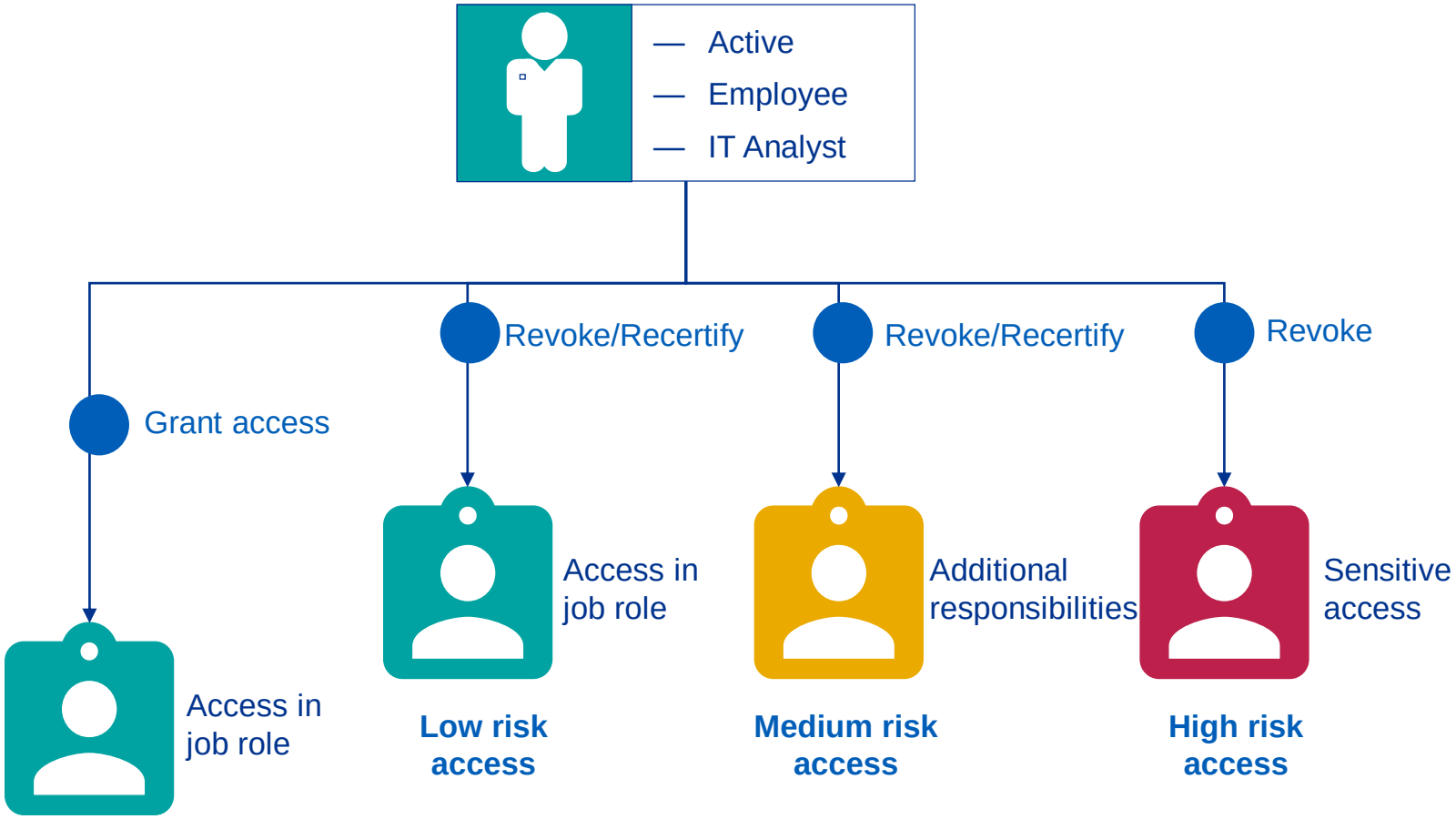


Managing Access - Over a period of time

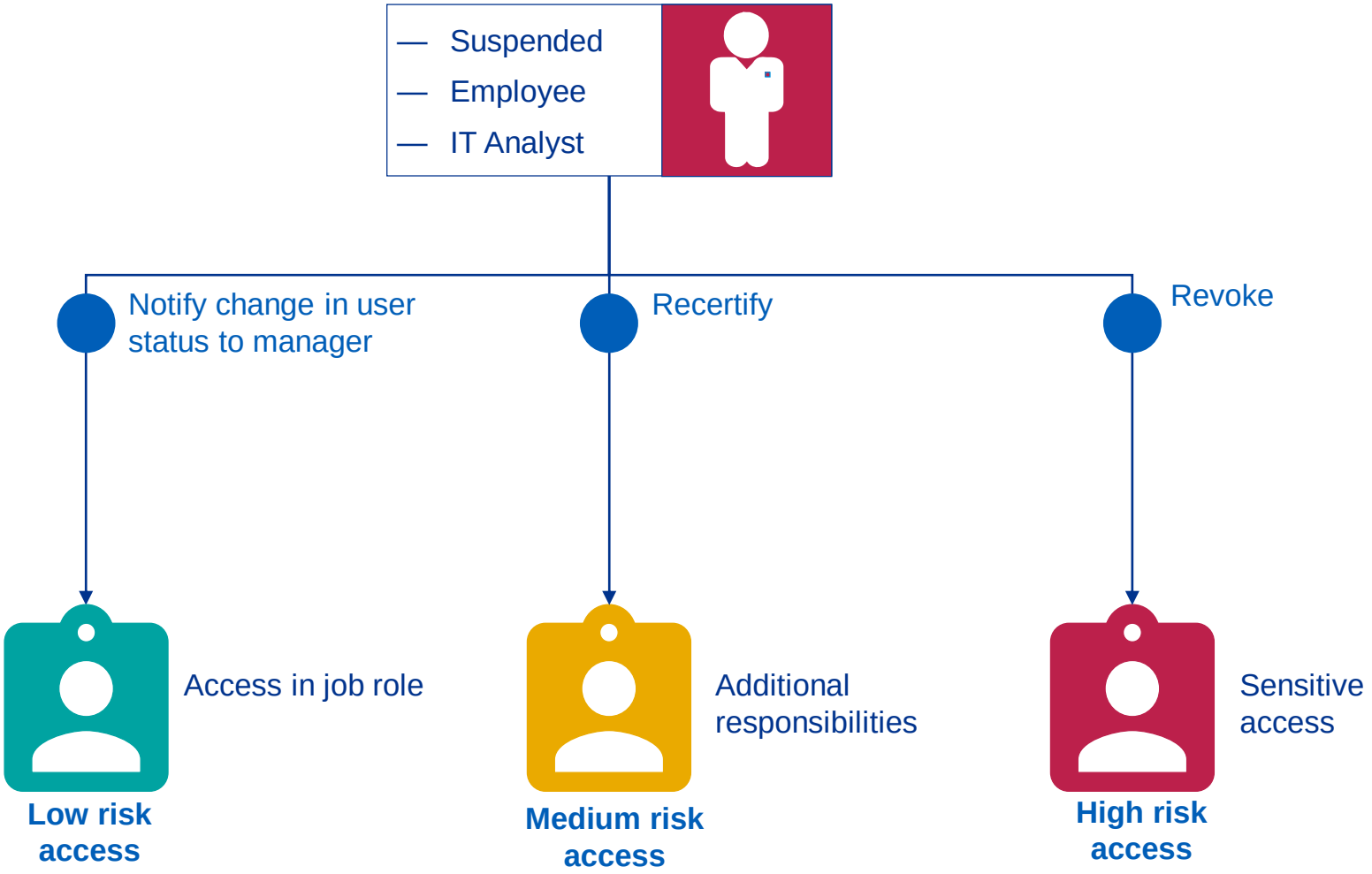
Access evolves and risk profile changes/improves.



Managing Access - Mover



Managing Access – Change in user status



Managing Identity Risks

Quantify identity's risk and take action to manage high risk identities

Good Practice

- Eliminate “phone a friend” request
- Business defines roles and access rules
- Derive roles from business function of user
- Too many access request approval requests = rubber stamp approval.
- Risk based access reduces number of access requests
- Explain what an access entails in business language

Managing Identity Risks – Accumulated Access

Users develop increased collections of access over time, increasing risk.

Certification

Certification ensures removal of access that is no longer needed

Manager revoked access

— No longer needed

— Segregation of duty policy violated by “entitlement creep”

Good Practice

- Too many certification = rubber stamp certification
- Indirect certification such as role certification mitigates risk
- Risk based certification helps prioritization
- Event based certification significantly reduces risks

How to start - Understand your Drivers

Regulatory Compliance

— 360º View of User Access and Activity

— Compliance-Driven Reporting and User Access Reviews

— Protection of Sensitive Information Assets

Risk Reduction

— Detective and Preventative Policy Enforcement

— Risk Measurement and Analysis

— Discovery of Rogue / Orphan / Privileged Accounts

Operational Efficiencies

— Automated Fulfillment and Password Management Processes

— Closed-Loop Attestation and Remediation

— Streamlined Business Processes

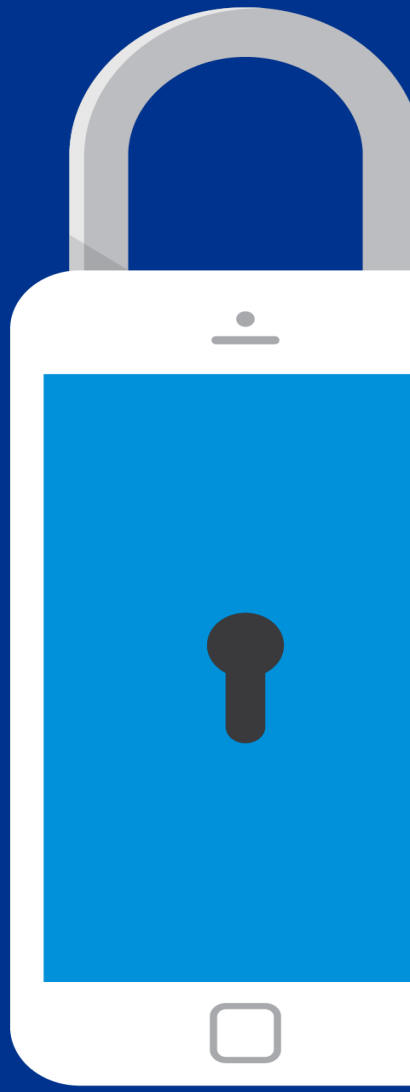
— Faster Onboarding and Provisioning

KPMG

Q&A

Thank you

kpmg.com/socialmedia



kpmg.com/socialmedia