www.pwc.com.au

The erosion of the perimeter in higher education. Why IAM is becoming your first line of defence.

pwc

What are all the things that make up IAM?

Delivery components

People & organisation | Policies & standards | Process & procedures | Tools & technologies | Metrics & measurements

Key drivers

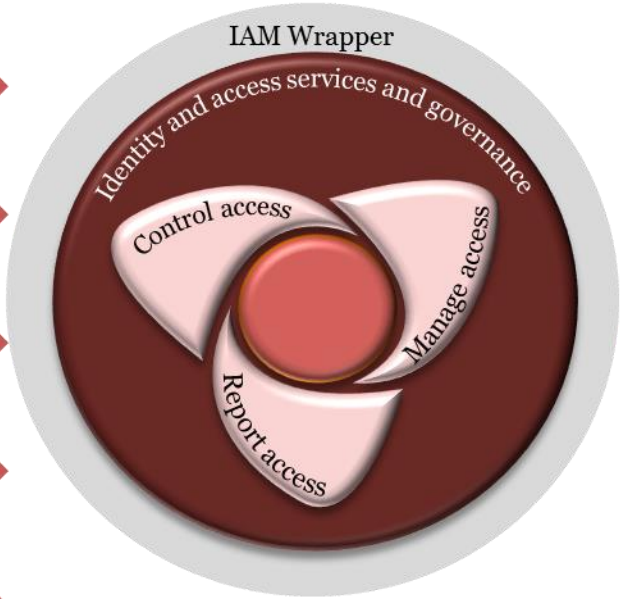
Business enablement

Risk and compliance management

Cost savings and efficiencies

Users

- Employees
- Contractors
- Customers
- Partners
- Services



Assets

- Applications
- Infrastructure
- Data
- Devices
- Cloud

Enterprise integration

Service management

IT infrastructure

Data architecture

Service components

Delivery methodology

Implement with agility: Assess > Design > Build and test > Operate > Enhance

Effectively source: In-house > Out-source > Co-source > Full-source

The identity scope is getting bigger and bigger.

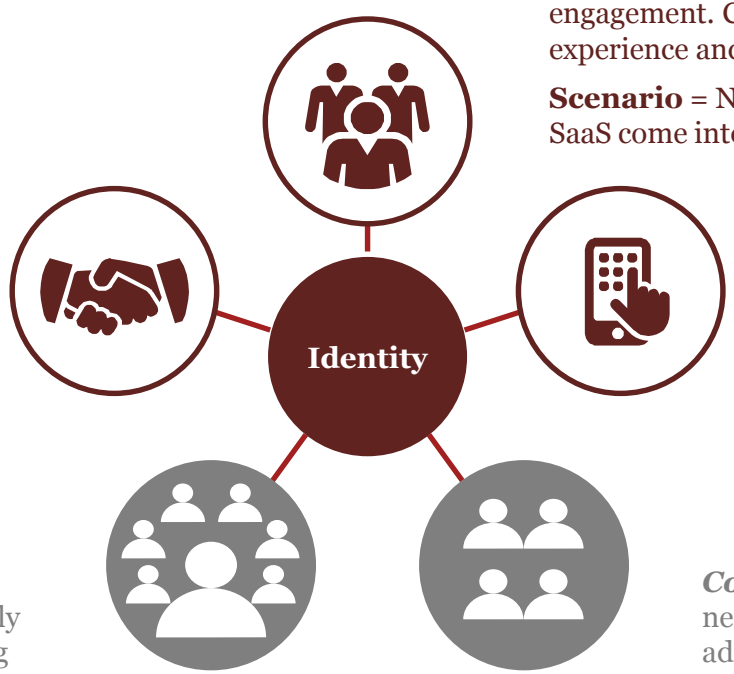
Identity types are expanding to include non-carbon lifeforms where the "people" aspect of your IAM solution now also needs to consider smart devices, sensors, etc., as new identity types.

Students – student experience is becoming a competitive advantage, and digital identity is the first point of engagement. Challenges exist with managing a seamless experience and the volume of identities that this brings.

Scenario = No defined perimeter; federation, cloud, and SaaS come into play.

Partners – Business partners must work as close confidants, yet risks of third-party relationships must be managed.

Scenario = Defined perimeter; federation becomes necessary



Devices – Devices present exciting new possibilities with new challenges on a massive scale. Build for the future with a highly-scalable, device-friendly digital identity platform.

Scenario = No defined perimeter; federation, cloud, SaaS, and mobility come into play.

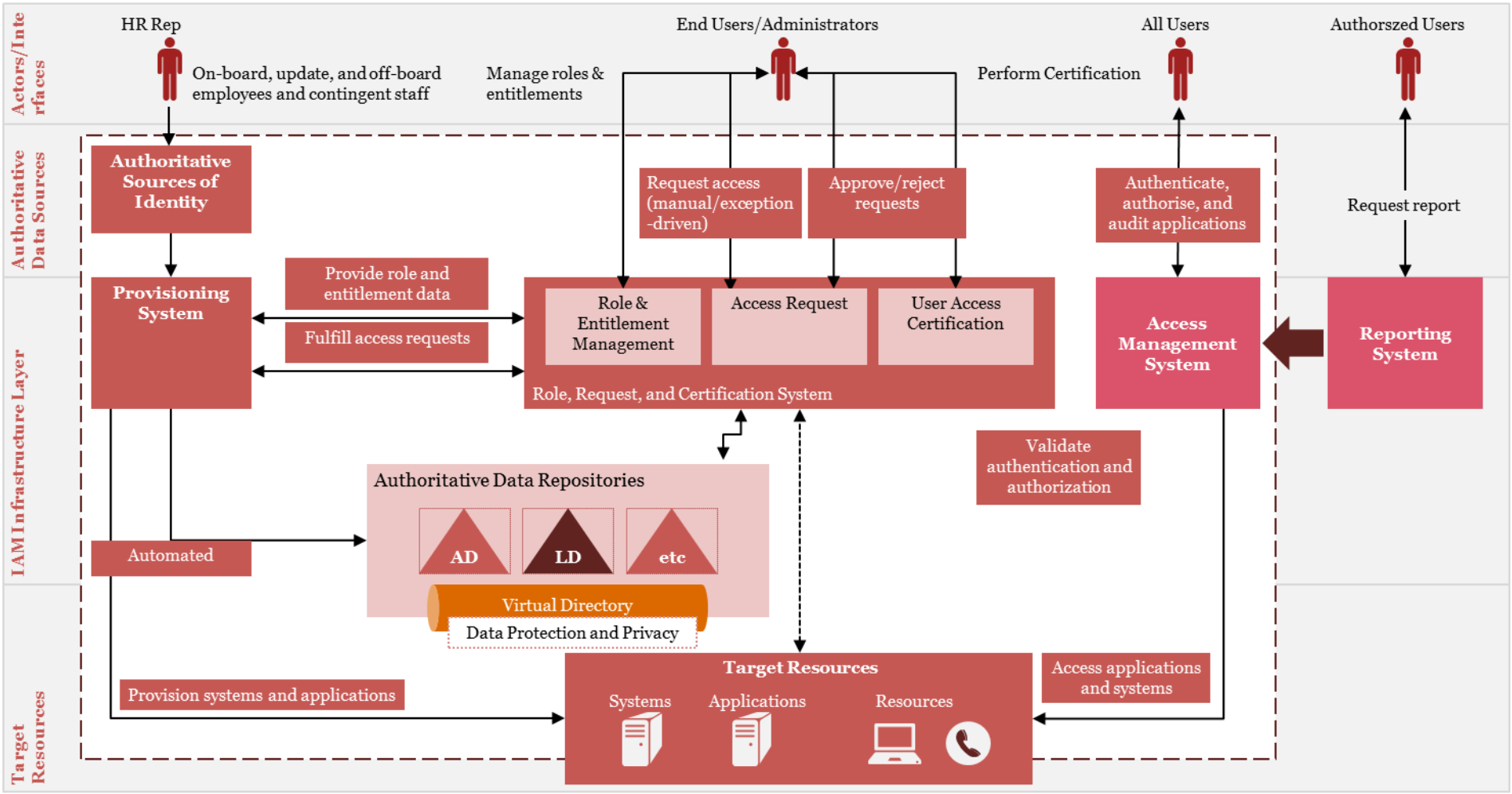
Employees – This is the traditional use case that originally generated the need for managing access within your workforce.

Scenario = Defined perimeter

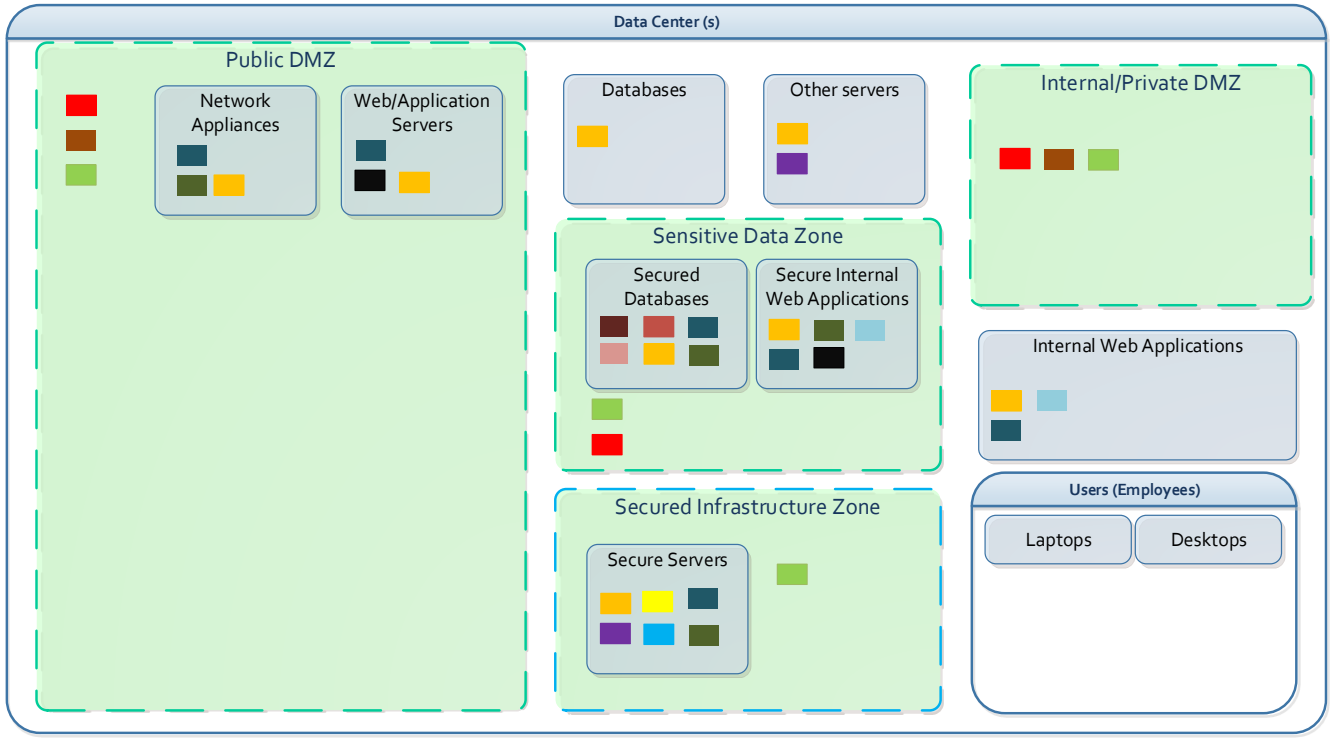
Contractors – The contingent workforce needs to be managed like employees, but additional challenges with regards to governance and expiring contracts.

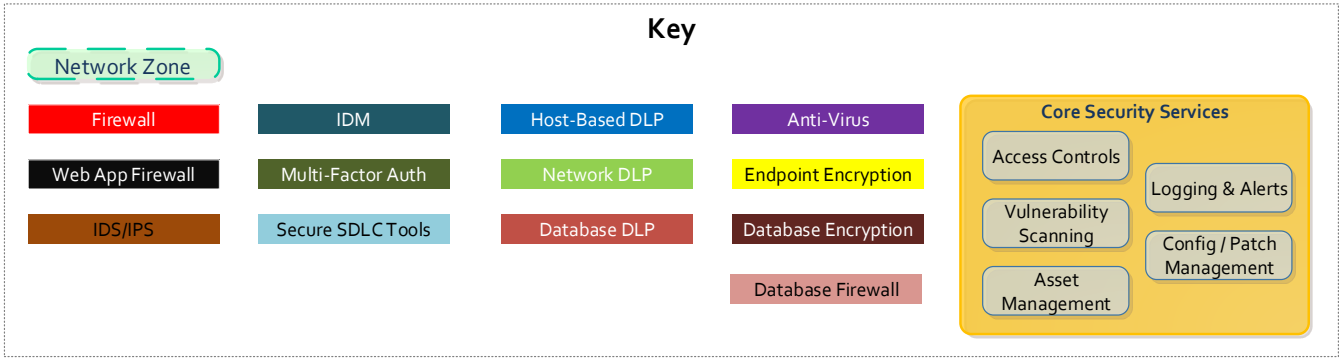
Scenario = Defined perimeter

So how do Banks handle this?



Why can this work for a Bank?





So why doesn't this work for us?

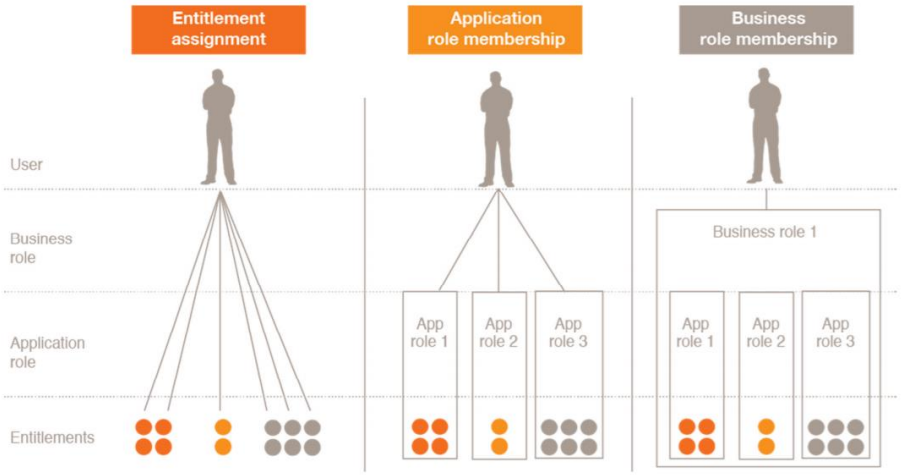
What makes us unique?

- Open
- Accessible
- No distinct boundary
- Where is our perimeter?
- Who are our users?
- Where are our systems?

So what does IAM need to look like in a higher education environment?

- Know who is accessing your systems (identities)
- As you collapse your boundary, treat every user as untrusted.
- Identify and document what access a student should have. How is this different from staff? How is this different from alumni?
- Treat every individual user as the new perimeter. How would you apply a firewall rule to them?
- Re-define your new perimeter. Is it at the application layer? Is it at the data layer? Is it around your key information assets?
- Re-think Role Based Access Control – it helps significantly.
- Consider every aspect of access. Not just the ones that are easy.

The association of roles to users



Logical Grouping of Individuals

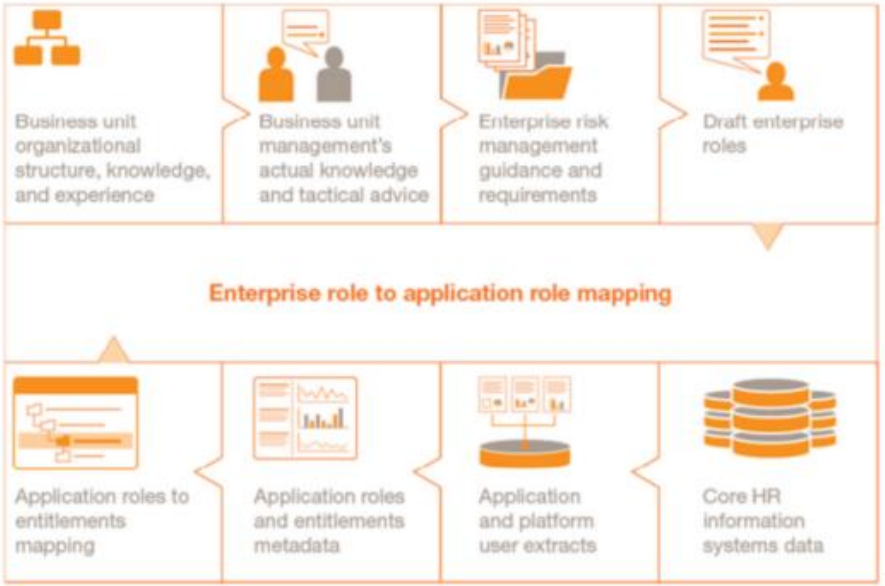
- **Alumni**
  - Blackboard (alumni attributes)
- **Student**
  - Blackboard (course materials)
- **Staff**
  - Blackboard access (course materials + alumni attributes)
  - Internal systems

The key is to identify what the clashes or violations of access exist, and that becomes the boundary of the role. This considers principles of both *Least Privilege* and *Segregation of Duties*.

Roles don't exist on their own

We already have systems, and those systems already have been configured to allow and deny access to individuals. Role definition provides the framework to group access to provide the following benefits:

- Business user experience
- Governance capabilities
- Operational support
- Request and approval workflow
- Transfers
- Compliance



What does roles mean to me?

What is a hybrid approach really mean and how do we build out a proper role definition framework?

Top-down

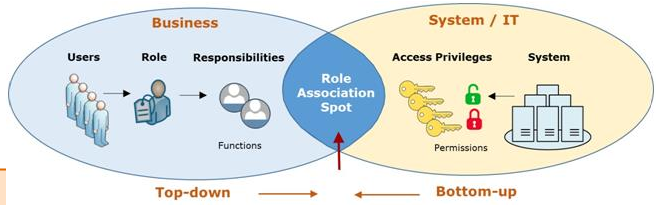
- Job Functions aligned to business hierarchy (organisational chart)
- Business Roles (Security Manager, Staff, Alumni)

Bottom-up

- Application / System information
- Entitlement Data (user specific from Active Directory)

Hybrid Approach

A mechanism that allows pragmatic attribute mapping of user identities to roles and personas that enable automation and governance aligned to business roles.



Task	Task name	Task description
H.	Design University-Wide (Business) Roles	Preliminary **enterprise role definition** and **design** **Map enterprise roles to IT roles**
I.	Design User IT Roles	Preliminary **IT role definition** **Map IT roles to enterprise roles**
J.	Role Mapping Define Rules and Constraints Define Role Ownership	Define **Segregation of Duties** (SoD) Define **rules to assign users to roles** Define **processes for assigning role custodians and stewards**

It's not just about giving access…

Manage Access

Access Request / Approval Service
- Request:
  - Discretionary (eligibility based) access
  - Elective (requires authorisation) access
  - Batch / System / Non-user ID account
  - Bulk
  - Expedited
  - Business rule enforcement
  - Token (fob) access request
- Approval workflow: standard, custom, etc.

Role & Entitlement Lifecycle Mgmt. Service
- Role engineering
- Role management (ownership, definition, approval, etc.)
- Enterprise birth right access
- Entitlement management (metadata mgmt ownership, approvers, data load, etc.)
- Business rule management (e.g., SOD)

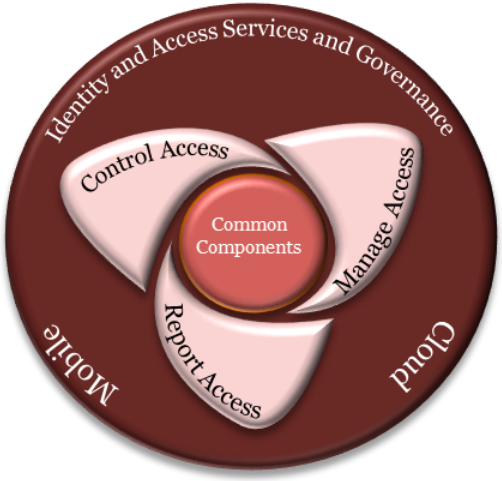
Provisioning / De-provisioning Service
- Fulfilment (add / modify / remove) process:
  - Automated (systematic)
  - Manual (executed by a provisioning analyst)
- Quality Control of manual provisioning

Access Certification Service
- User manager certification (logical & physical entitlements / roles)
- Information owner certification (elective access)
- Resource owner certification (elective access)
- Role definition certification
- Business rule certification (e.g., SOD)

Privileged Access Management Service
- Creating and managing policies that govern special needs of privileged accounts, including their provisioning and life cycle management, authentication, authorisation, password management, auditing, and access controls

Control Access

Authentication / Authorisation Service
- Single factor authentication
- Multi-factor and adaptive authentication
- Single / Simplified Sign-On
- Federation (internal / external)
- Externalising authentication and authorisation
- Role (and/or attribute) based access control
- Password Management



Report Access

Access Reporting Service
- Collection, correlation and reporting of access and events
- Role and entitlement membership reporting
- Logging and activity monitoring
- Risk-based reporting
- Regulatory / compliance reporting
- Identity & access dashboard (metrics)
- Business rule-based reporting

Common Components

- Standardised:
  - Approval workflows
  - Delegation & proxy function
  - Search capabilities and displays
  - Notifications
  - Activity tracking
- User account & data reconciliation (including rogue and orphan accounts)
- Directory and data management services (including virtualisation and meta directory)

Remember to use identity attributes as your levers for access rights.

Transition Activities Supported

- Rapid on-boarding model for platform and application on-boarding
- Transformational change management (organisational and technical)

Questions?