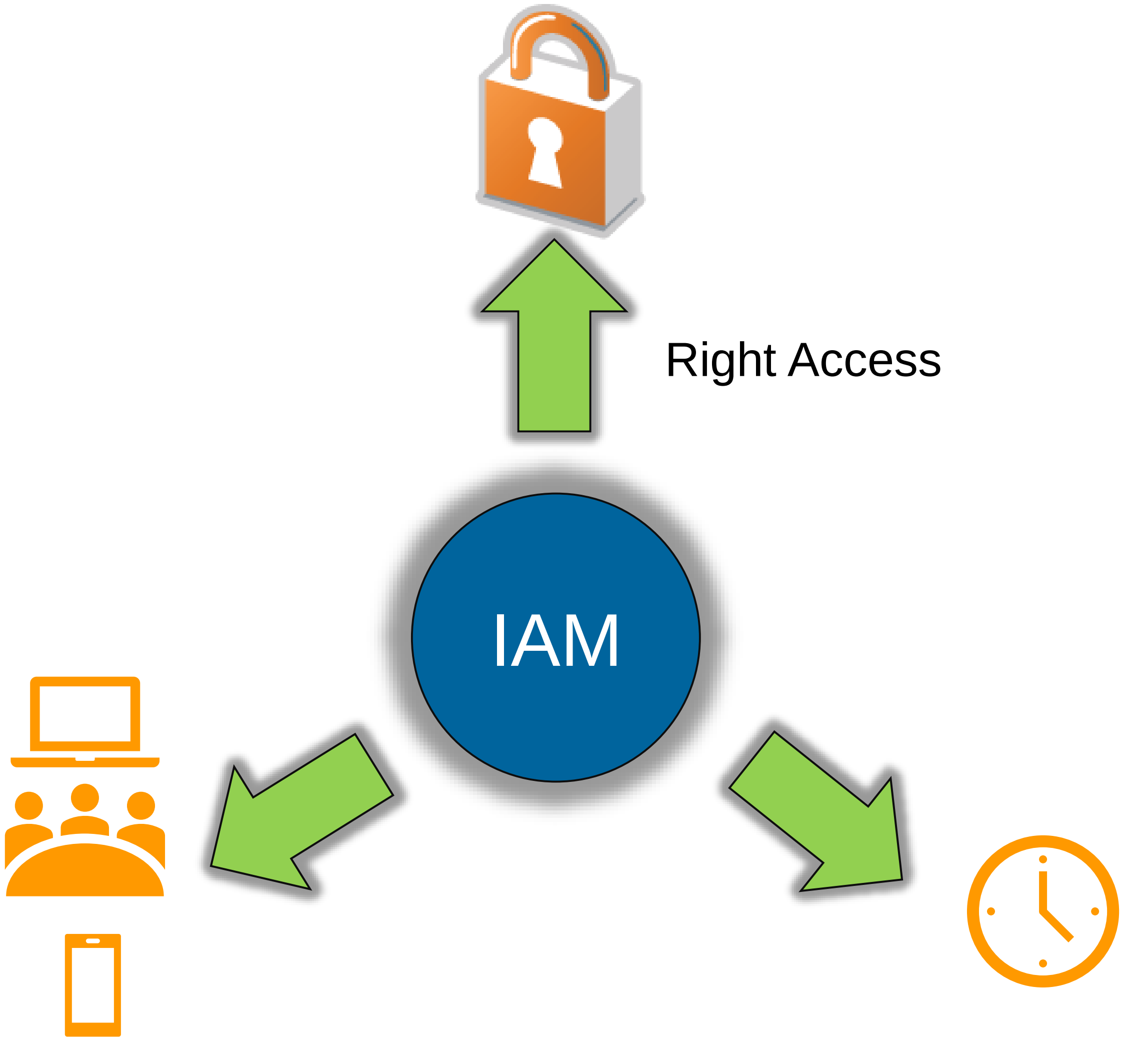
Managing User Identities

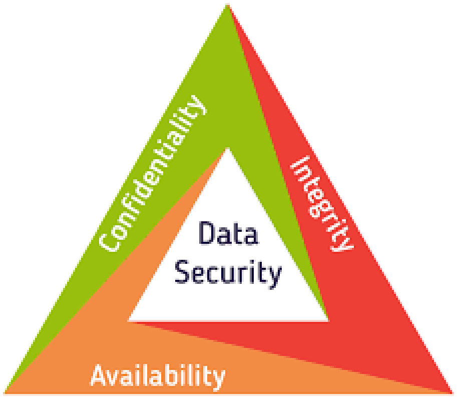
Identity & Access Management



Right Access

Right People,
Systems & Devices

Right Time



Identity & Access Management

Identity and Access Management (IAM) is the set of business policies, processes, and a supporting infrastructure for managing the creation, maintenance and use of digital identities.

IAM enables organizations to:

- Provide secure access to resources
- Efficiently control this access
- Respond faster to changing relationships
- Protect confidential information from unauthorized users

For those needing access to computer system or physical resources, IAM:

- Verifies who you are
- Manages what you can and cannot do based on business rules and your attributes such as departmental affiliation or role within the university

Identity Management vs Access Management

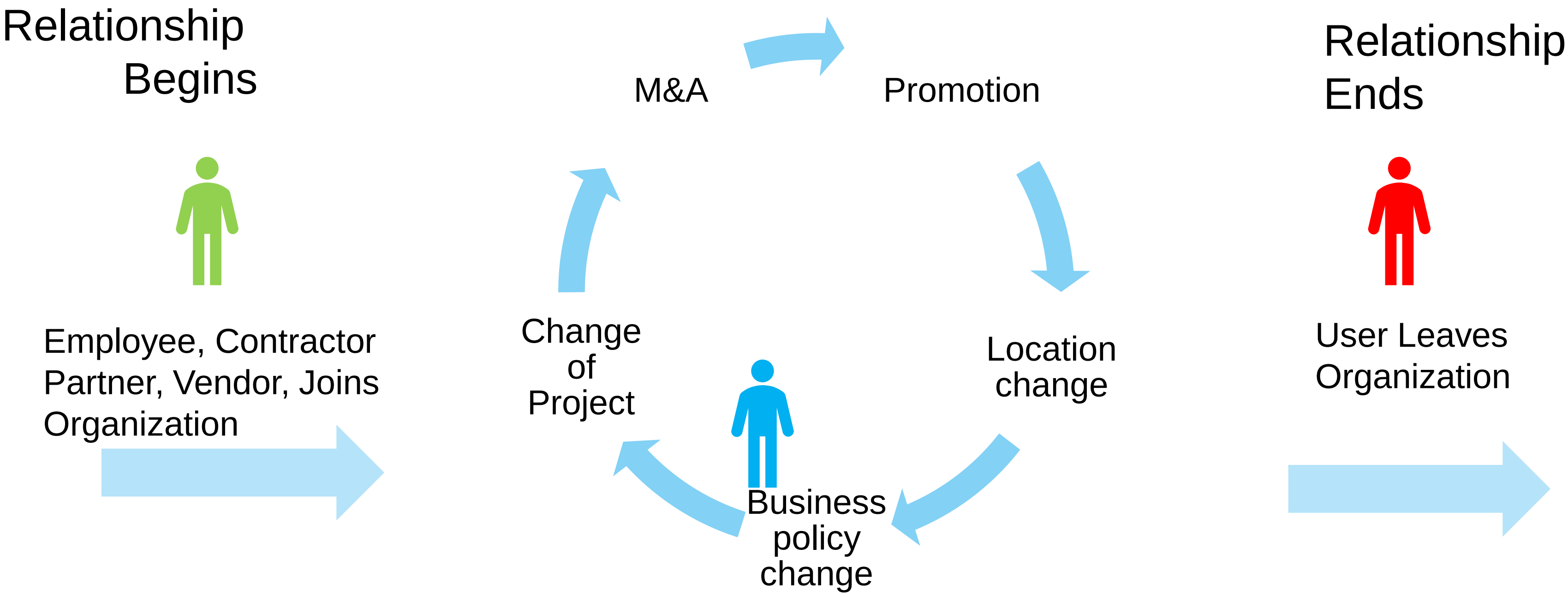
Identity Management is all about managing Identities and access

Access Management is about authorizing access and thus indirectly includes authentication

IAM Goals!

- Increase **Operational Efficiency**
  - Automate Identity & Account Lifecycle Management, Streamline Access request process.
- Increased **Agility and Scalability**
  - Single Sign-On & Self-Service Management for end users.
  - Role and Rule based provisioning for Accounts & Access Entitlements
- Reduce Access Control **Risk** in the Enterprise
  - Implement automated controls to reduce the access control risk
  - Implement higher levels of security for privileged access
- Meet **Compliance** requirements
  - Audit & Compliance Reports (i.e. who has access to what)
  - Access Review & Attestation
- Provide a **Security Framework** for Enterprise
  - Authentication, Authorization and Audit framework for enterprise applications.

Identity Lifecycle



Relationship Begins

Employee, Contractor Partner, Vendor, Joins Organization

M&A

Promotion

Location change

Business policy change

Change of Project

Relationship Ends

User Leaves Organization

- Create Identity (User Accounts)
- Assign Resource Access

- Access request & Approval
- Password Self Services
- Profile Management
- Access Recertification

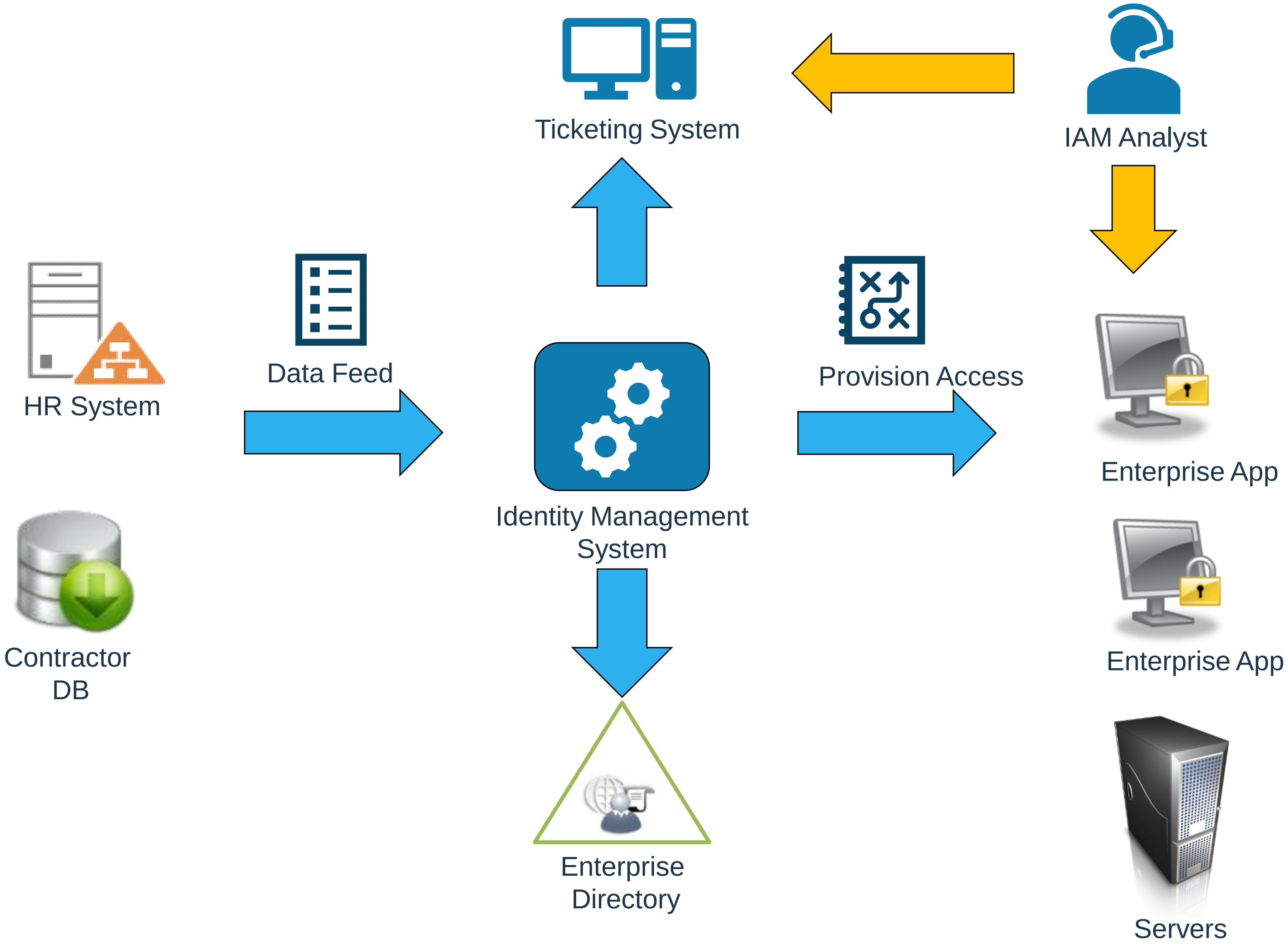
- Revoke Access
- Delete Accounts

Provision Access

Manage Access

Deprovision Access

Identity Management System



Identity Management Use Cases

Joiner/Mover/Leaver
Detect user events from Source of Record and create/manage/revoke identities within identity management system. Evaluate job roles and assign birth right access and roles

Self Service
Manage the users own profile and passwords.

Access Request and Approval
Process and workflows to request additional access and provisioning the access with appropriate approvals.

Access Certification
The process and workflow to periodically review the access my managers/application owners and rectify outdated access.

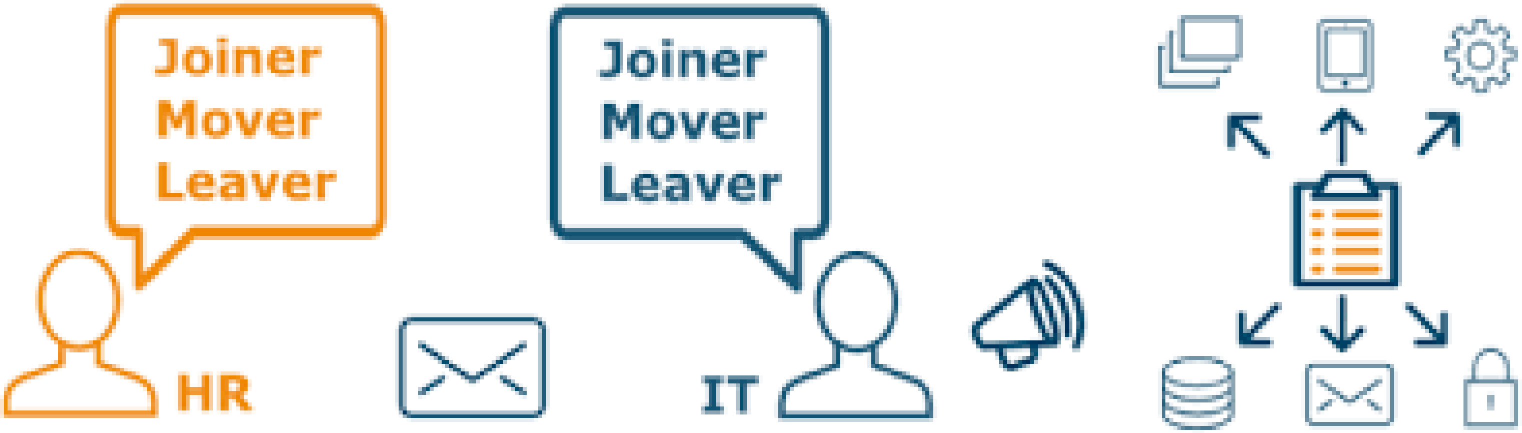
Role Management
Grouping of access into roles based on Job function and managing the lifecycle for Roles.

Enterprise vs Consumer IAM

	Enterprise IAM	Consumer IAM
Focus	Internal Enterprise focused	Enterprise, Partners and Consumer focused
Actors	Employees & Contractors	Employees, contractors , Partners, Suppliers, Consumers, Mobile, Smart devices and Wearables
Authentication	UserID + Password , Hard /Soft Tokens, SAML	User ID + Password, OTP, Phone Tokens, Biometric (Fingerprint, Voice, Face, Heartbeat), Touch ID and wearable device authentication, Social Login, Federated access, OAuth , OpenID Connect
Directory	Enterprise AD / LDAP	Enterprise Directory , Consumer Directory, Social Directory
Primary Use Cases	Provisioning, Access Recertification , User access and SSO	Consumer & Device Registration, Self Service, Social Integration, Biometric authentication, Device Authentication, PII Data Governance, Risk based authentication, Federated access, Cloud Access
Access Channel	Web Channel	Multi Channel (Web, Mobile & API)
Services Outlook	Inside Out view	Outside In view
Business Driver	Regulatory Compliance, Risk Mitigation, Cost Optimization	Business Enabler, Agility, Customer Satisfaction, Regulatory Compliance, Risk Mitigation and Brand Protection

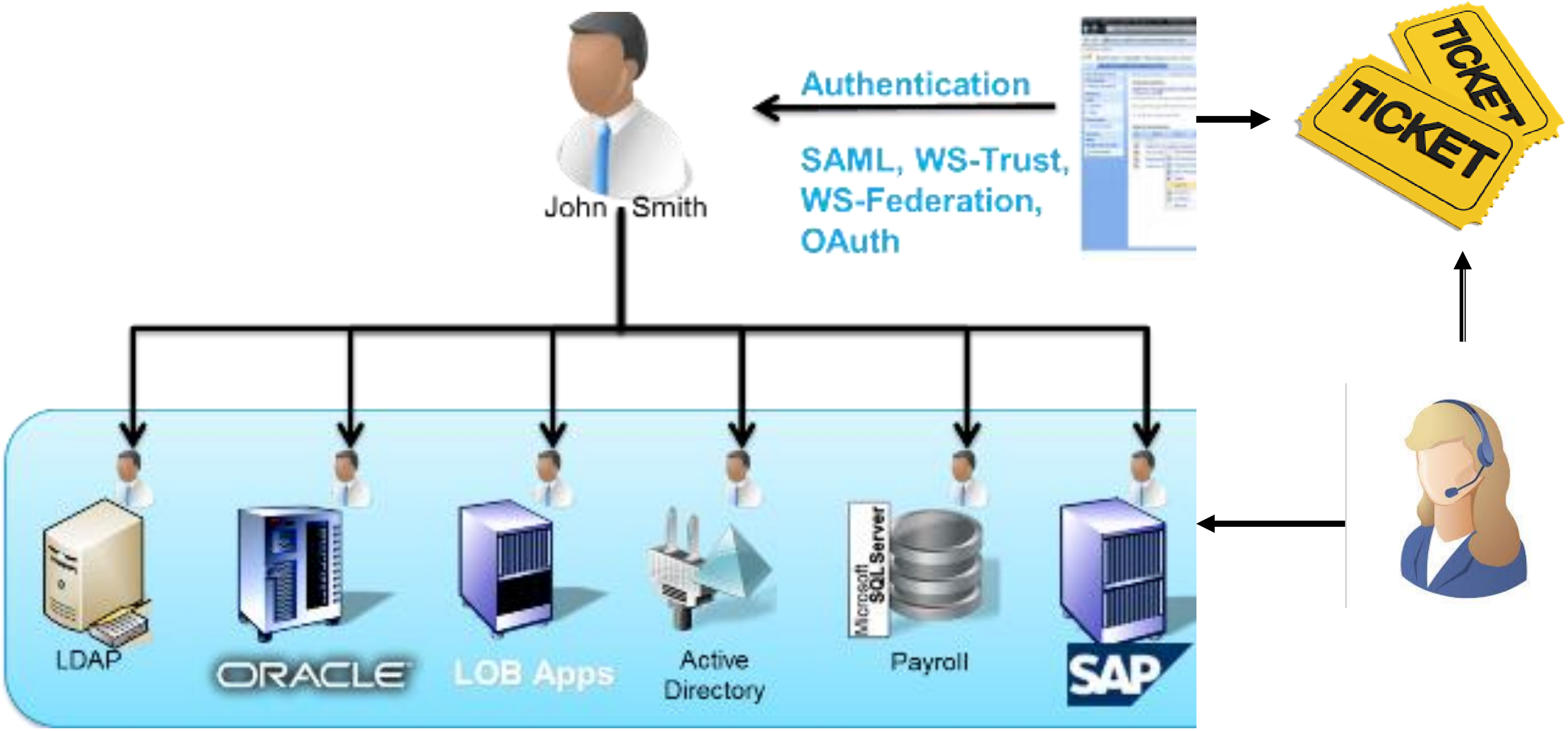
Enterprise Identity Management Use Case

Joiner Mover Leaver - JML



- *Ensure user accounts are created in the right systems in a timely manner*
- *Send notification on new accounts & access*
- *Trigger approval workflow and notification for critical access*
- *Monitor user job change and trigger revalidation*
- *Ensure user access are revoked with SLA*
- *Maintain audit trail of all change*

Provisioning & De-Provisioning

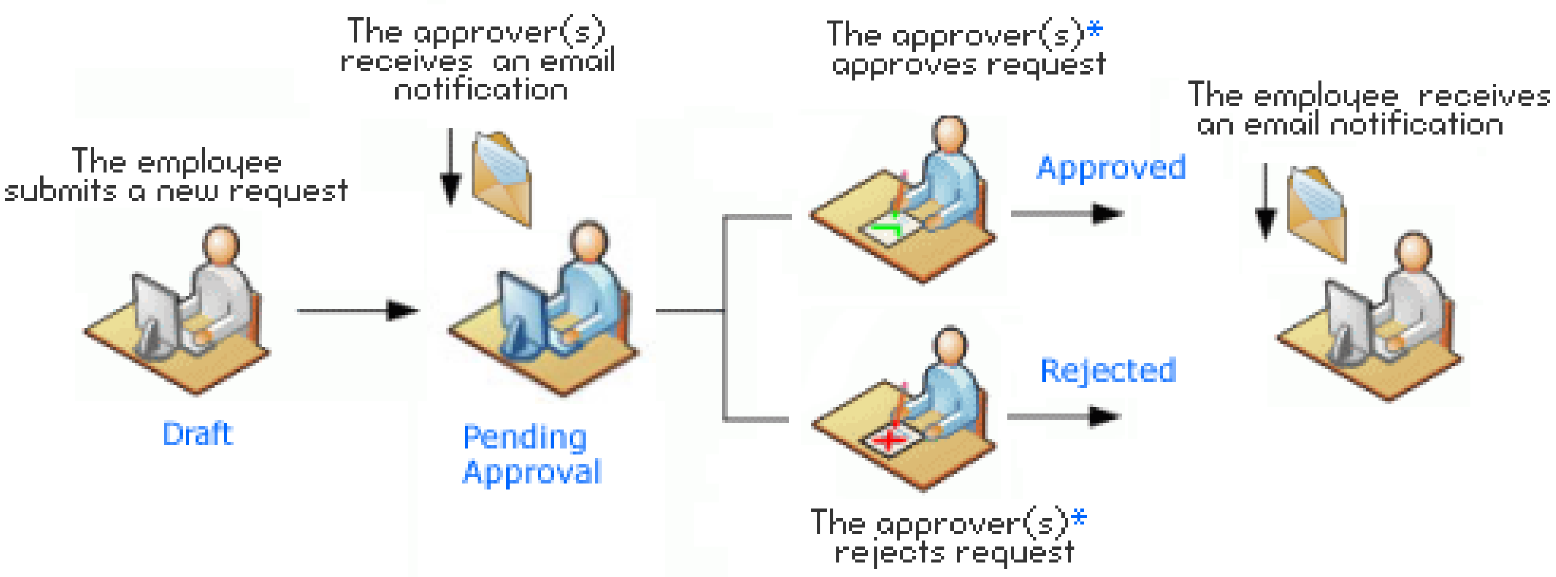


- *Build & manage integrations to target application*
- *Automated for connected provisioning*
- *Ticket creation and manual provisioning for non integrated applications*
- *Periodic reconciliation to detect orphan & rouge accounts*

Self Service

- *Self Service Password Reset*
- *Security Q&A*
- *Profile Updates*
- *Access Request*

Access Request



The employee submits a new request

Draft

The approver(s) receives an email notification

Pending Approval

The approver(s)* approves request

Approved

The approver(s)* rejects request

Rejected

The employee receives an email notification

* - for multiple approvers: once approved, the approval request goes to the next approver.

Reporting

Key Requirement for supporting audit and compliance evidence

Some of the common IAM reports include

- *List of users with access to an app*
- *List of user access revoked on a date*
- *List of app an user has access to*
- *List of users with a particular role*

Application Onboarding

Integrate applications into the IAM platforms to

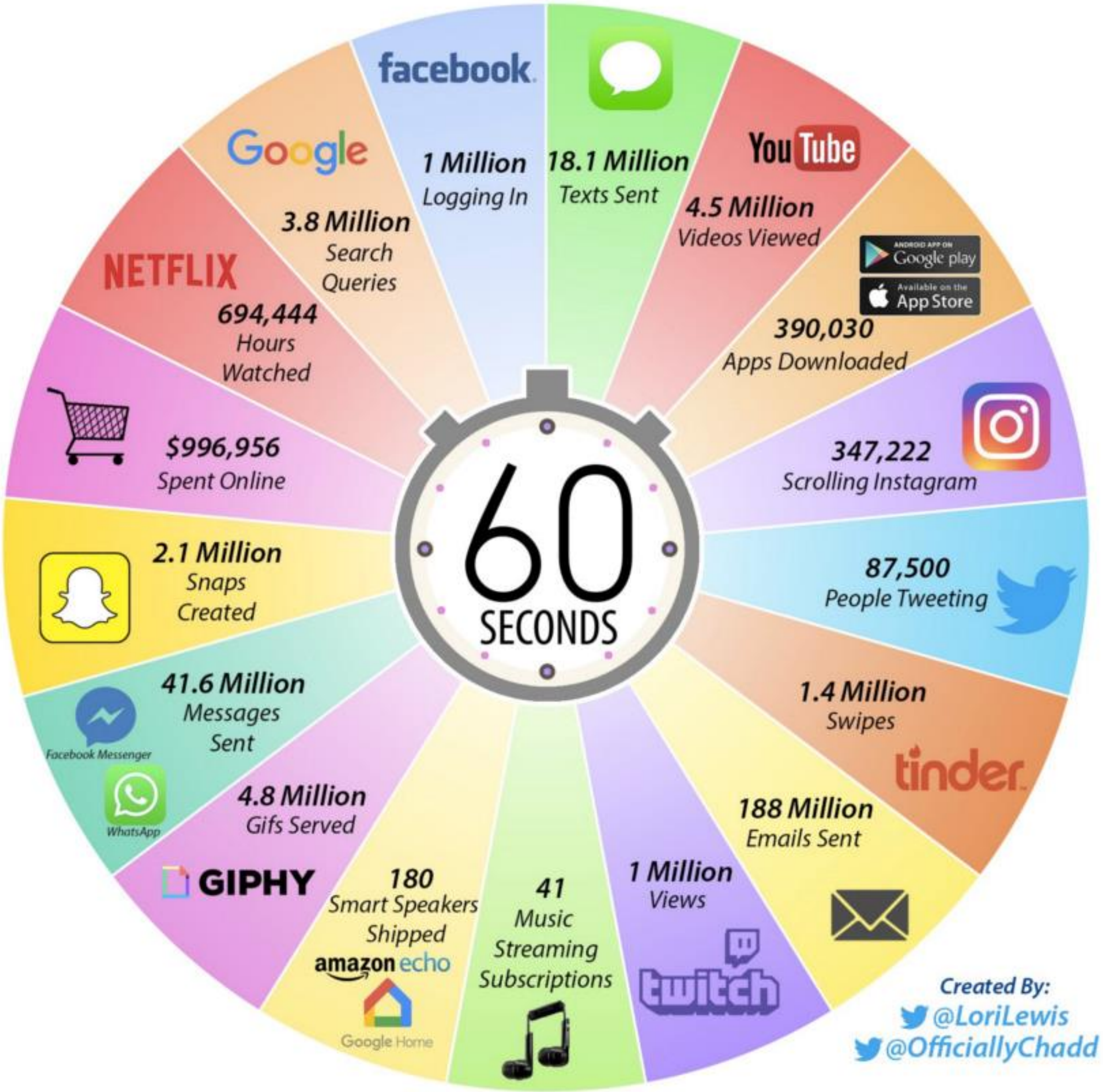
- *Enable users to request access to the apps*
- *Enable access governances and re certifications*

Application onboarding entails

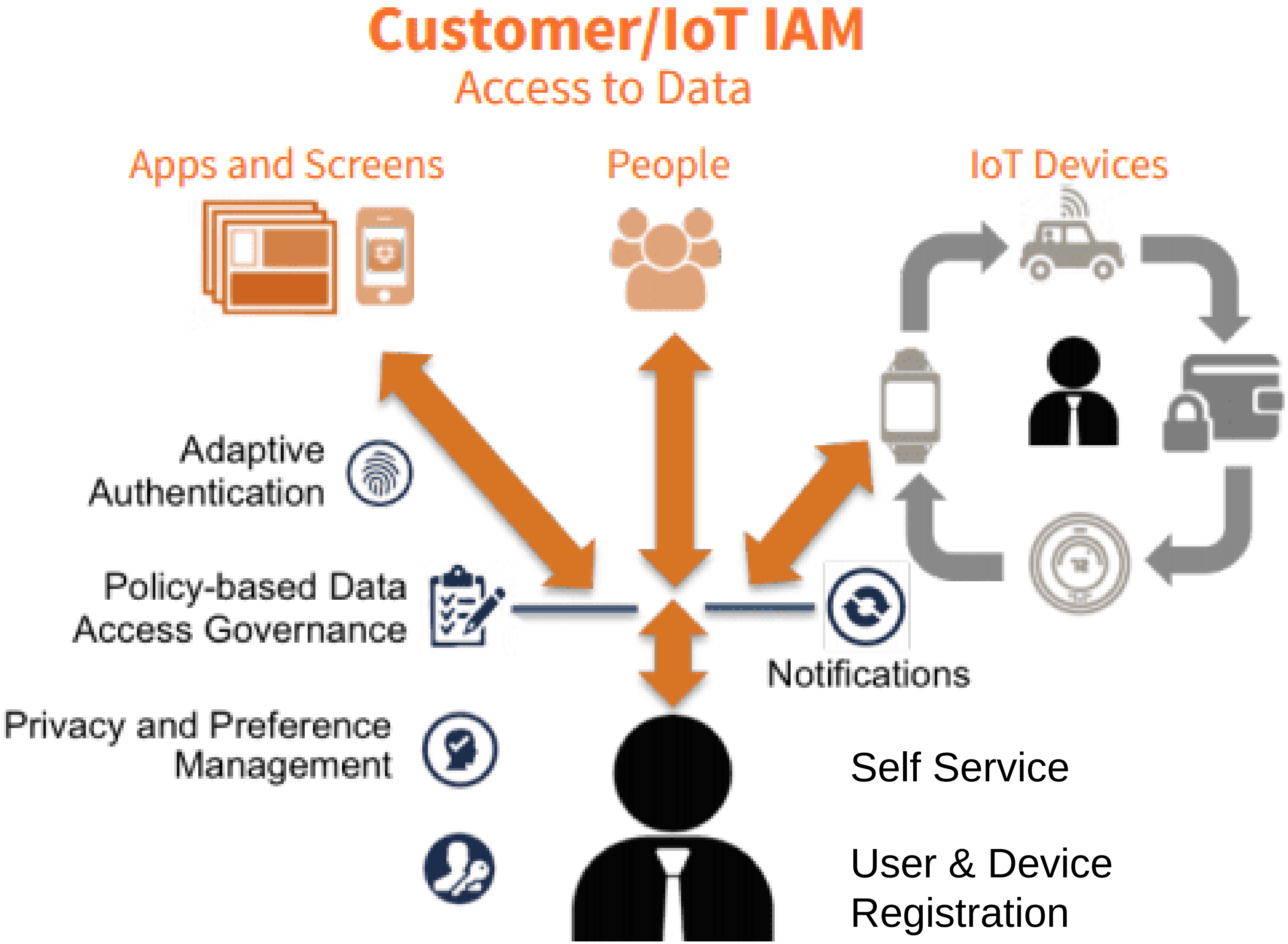
- *Understanding the data needed for application provisioning*
- *Approval workflows before access can be provisioned*
- *Governance process for access revalidation*
- *Role membership of applications*

Consumer Identity Management Use Case

2019 – This is what happens in an Internet Minute



Consumer IAM



Self Service

User & Device Registration

Identity Assurance Levels

- **IAL1**: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).

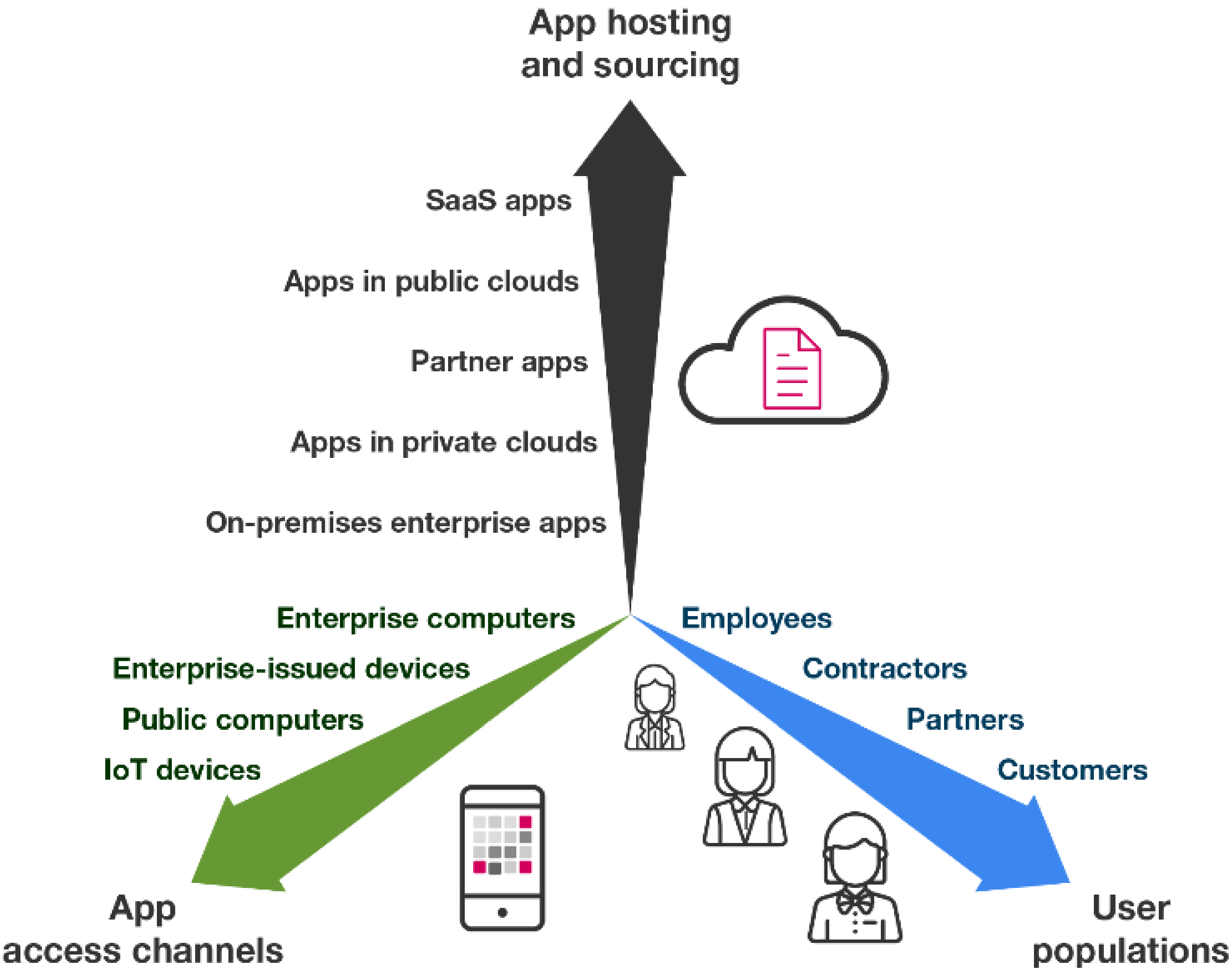
- **IAL2**: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing.

- **IAL3**: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP.

Source : NIST **SP 800-63**

IAM Challenges

Expanding Boundaries



App hosting and sourcing

SaaS apps

Apps in public clouds

Partner apps

Apps in private clouds

On-premises enterprise apps

Enterprise computers

Enterprise-issued devices

Public computers

IoT devices

App access channels

Employees

Contractors

Partners

Customers

User populations

IAM Challenges

- Multiple Identities
- Orphan & Rouge Accounts
- Manual Tasks
- Complex Business Process
- IAM as the Swiss Army Knife
- Lack of Governance
- Lack of Clear Roadmap & Architecture & Planning
- Budget

IAM Challenges – Financial Services

Authenticating a Customer's Identity

This is especially important for the financial services sector as they have KYC requirements & need to corelate multiple identities

Multifactor Authentication

Enabling higher levels of security while maintaining ease of use.

Regulatory Requirements

Regulatory bodies such as Sarbanes Oxley (SOX) require controls for auditing and reporting. This can be an expensive task. Maintaining compliance to an ever changing regulatory landscape is an added challenge

On Prem Mindset

Financial intuitions have a need to adopt to latest technology advancements but their On Premise mindset can be a barrier to early adoption of technology

Multi Channel support

Customers should to be able to utilise the services via multiple channels (Web, mobile, Phone etc.) but the complex business services are hosted in legacy systems

Cloud Based Services

Financial services CIOs cannot abdicate responsibility for security to the cloud hosts as strict regulations hold them responsible for protecting their customer’s accounts against fraud.

Retail industry has a different set of challenges

- Geographically dispersed User Base
- High Staff Turnover Rate
- Same Services delivered under multiple brands
- Long Technology Refresh Cycles
- Regulatory Compliance
- Access Control to PoS and Portals

Cross functional teams without alignment

I need full control of IAM?

I do not have the bandwidth to support this

How does this help me?

Not from my budget

CIO : Lets get this to work

I need to retain control of my application access

IAM benefits

Positive User experience

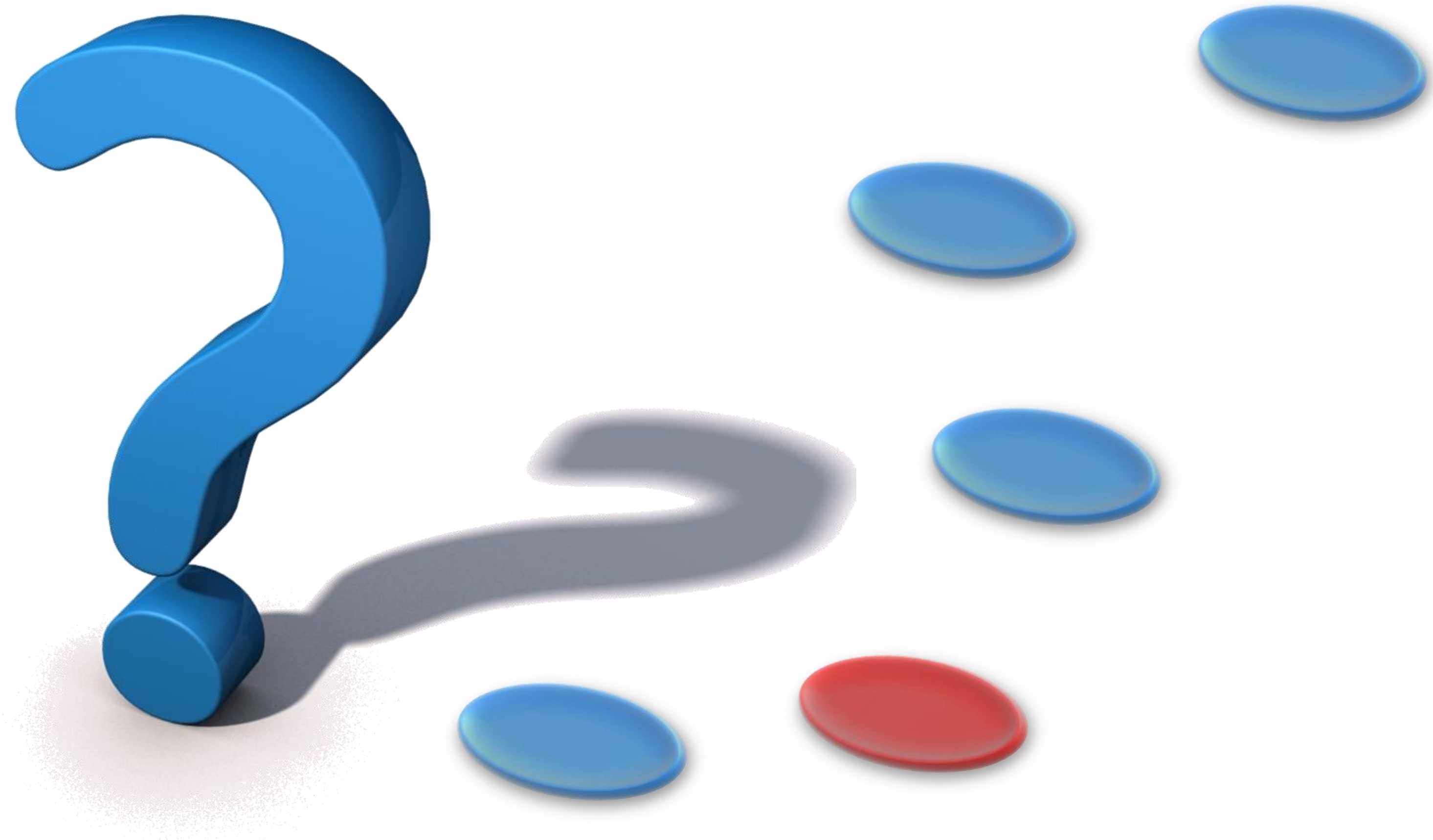
Increase Operational Efficiency

Increased Agility and Scalability

Reduce Access Control Risk in the Enterprise

Meet Compliance requirement

Q&A



IDaaS

Identity as a Service (IDaaS)

- Standardized IAM services enabled on a cloud platform
- Can be public or private services
- Faster Roll Out of IAM platform
- Significant savings on TCO for customers and Fixed operating cost with pay as you go model thereby reduce risk and exposure
- Avoid the effort & costs involved in IAM platform setup, HW / SW maintenance & upgrades
- Service catalog driven change management

Why move to an IDaaS model

Applications shift to the Cloud model, and are no longer being managed by Client.

Huge drive of the market towards SaaS and other Cloud models (Azure, Office365, Salesforce, Adobe, Google, etc.)

At the same time, some key on-premises applications still need to be securely accessed (remotely & on-premise)

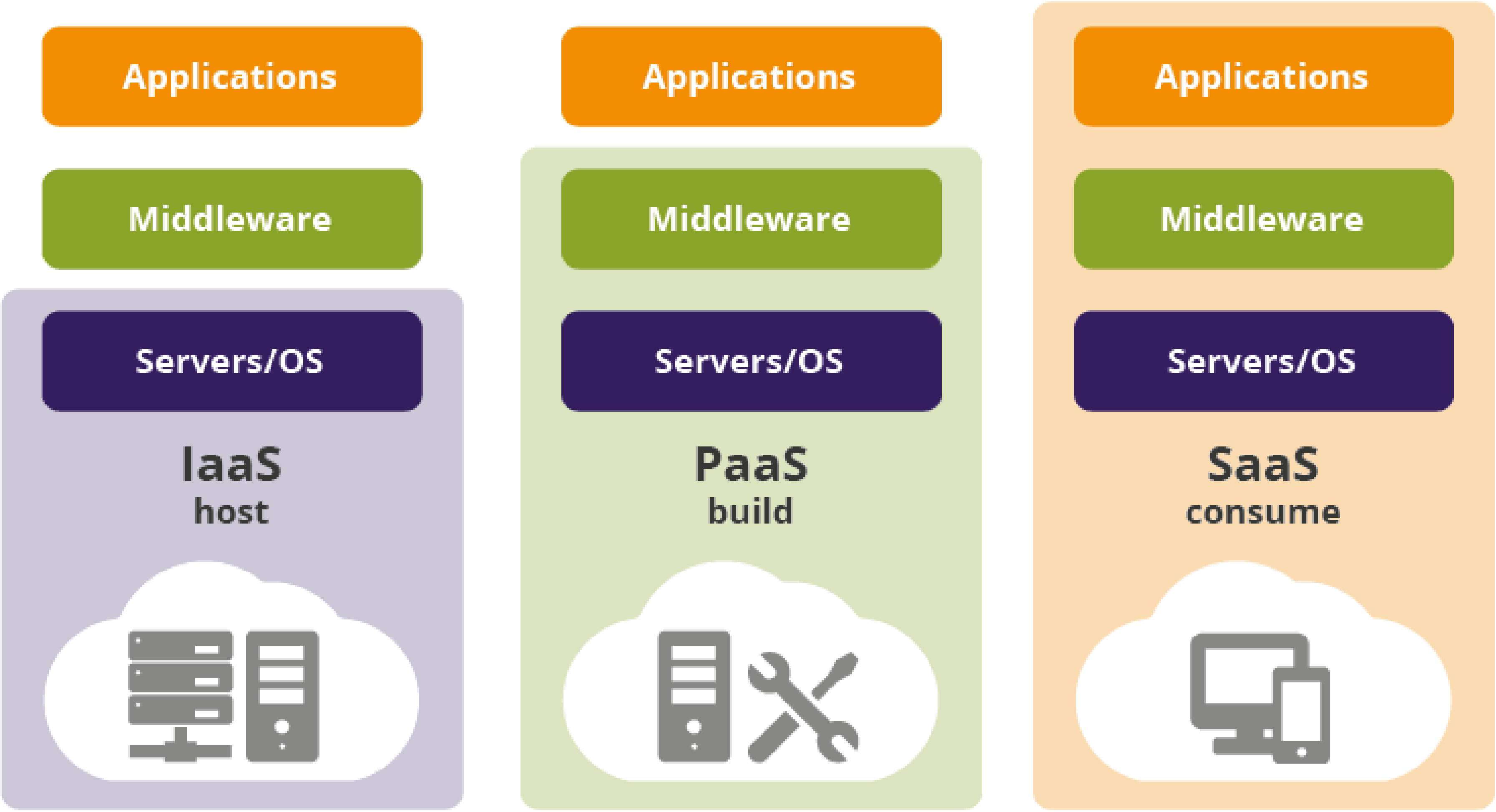
Users working from anywhere over any type of connection. VPN is a thing of the past.

B2B: External Users and Internal Users need to collaborate. But no more provisioning of External Users in corporate AD!

Role based application authorization and the decoupling of security logic from applications

Bring Your Own Device (BYOD): smartphones, tablets etc. Users not only allowed, but ENCOURAGED to access from their own device.

As a Service Models



IDaaS Challenges

Sensitive Data

- **Data Leakage and Data Privacy issues; Loss of control over data**
  - Classifying the data and applications to decide what resides in public cloud and what resides in private cloud . Data Ownership issues and losing control over data

Cloud Security

- **Risks of data security, access control, integration**
  - Risk of data access to third parties
  - The ability to store encrypted data and securing data in transit

Interoperability & Portability

- **Integration with existing infrastructure, closed platforms**
  - Compatibility with more than one cloud provider and ability to run components written for one environment in another environment
  - Ability to freely select and manage the solutions that are best suited to their needs

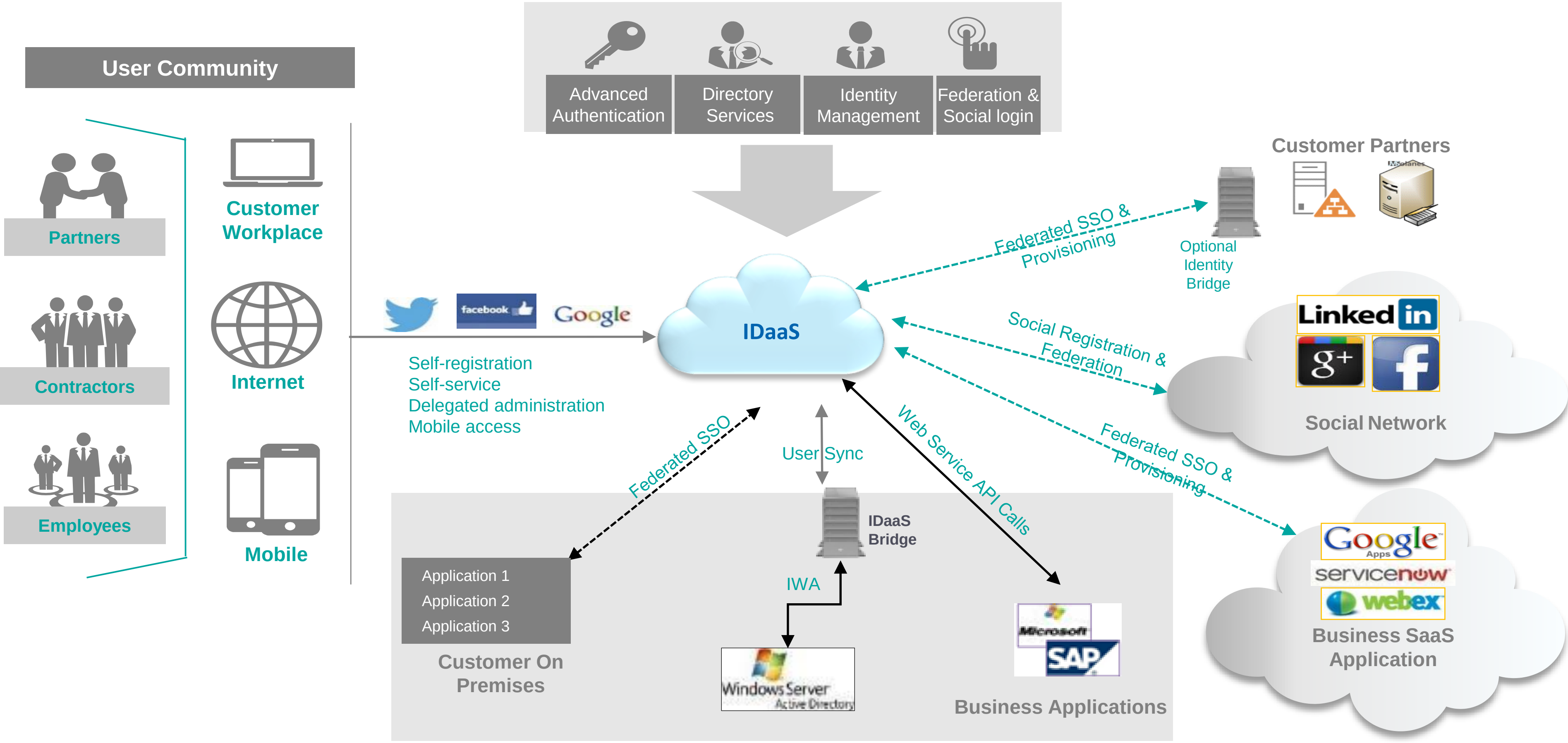
Adapting to cloud computing

- **Changes in, authority, funding and staffing**
  - Service quality, availability and reliability dependence on Cloud Service Provider

Compliance

- **Regulatory requirements, Service Level Agreements (SLAs)**
  - A set of metrics to determine whether the provider is delivering the services as promised
  - Regulatory standards and compliance

IDaaS Logical View



Benefits

Reduced Capex Cost

Optimized Operational costs.

Reduce time to deploy IAM foundation & automate processes

Best of Breed Technology platform coverage of IAM and associated functional areas

Predictable Costs for IAM operations and automation cycles

Stronger Process Security -Pre-baked Best Practices Process implementation

No complexities of product version upgrades. The Hosted solution will have the latest version deployed.

No dependency on in-house technical expertise.

Access Controls

Access control models

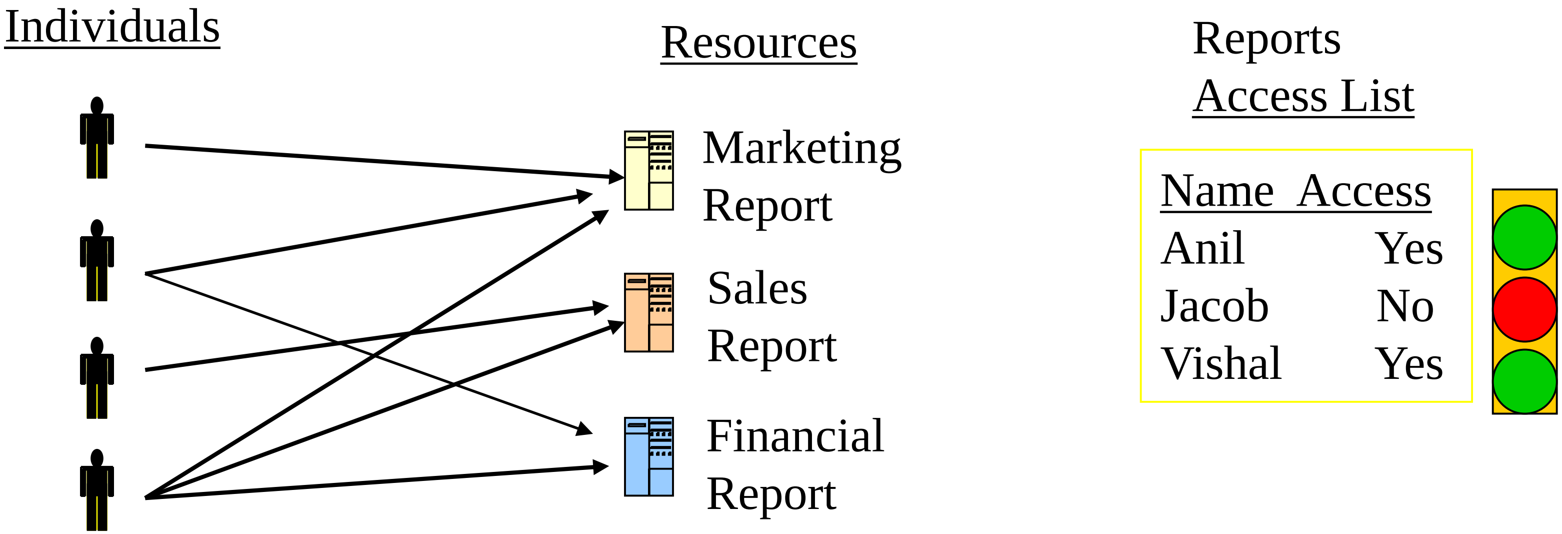
- **Discretionary** access control (DAC): based on the identity of the requestor and access rules

- **Mandatory** access control (MAC): based on comparing security labels with security clearances (mandatory: one with access to a resource cannot pass to others)

- **Role-based** access control (RBAC): based on user roles

- **Attribute-based** access control: based on the attributes of the user, the resources and the current environment

DAC



Individuals

Resources

Marketing Report

Sales Report

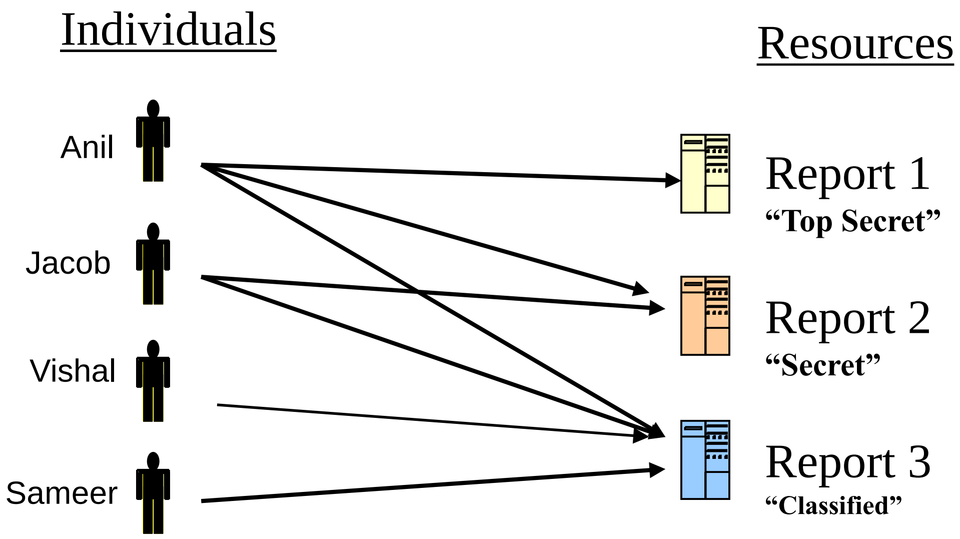
Financial Report

Reports Access List

Name	Access
Anil	Yes
Jacob	No
Vishal	Yes

Restricts access to objects based primarily on the identity of users who are trying to access them.
ACL are applied to the resources

MAC

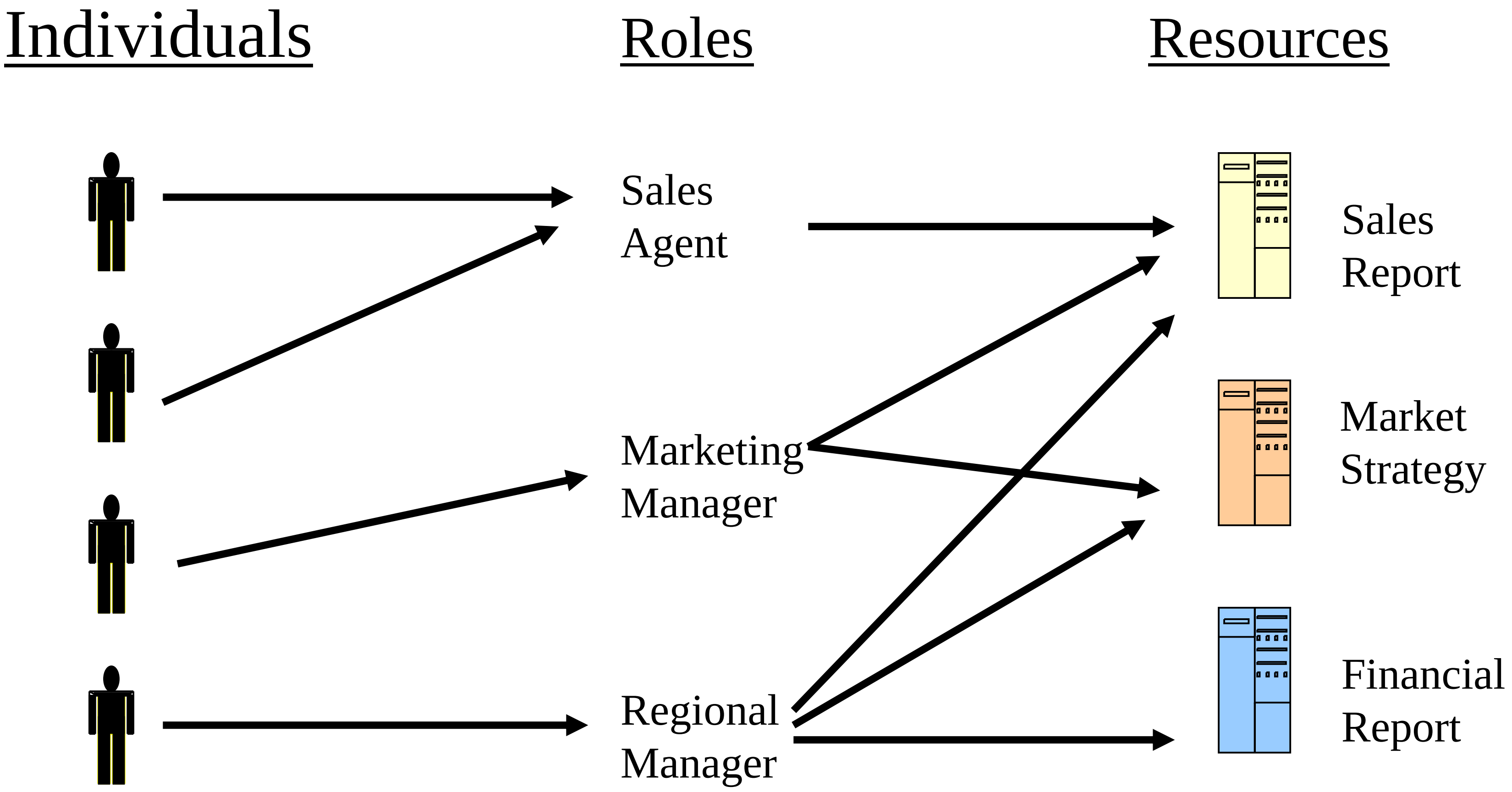


Users Access Levels

Name	Access
Anil	Top Secret
Jacob	Secret
Vishal	Classified
Samer	Classified

MAC mechanisms assign a security level to all information, assign a security clearance to each user, and ensure that all users only have **access** to that data for which they have a clearance.

RBAC



Individuals

Roles

Resources

Sales Agent

Marketing Manager

Regional Manager

Sales Report

Market Strategy

Financial Report

RBAC

- A user has access to an resource based on the assigned role.

- Roles are defined based on job functions.

- Permissions are defined based on job authority and responsibilities within a job function.
-

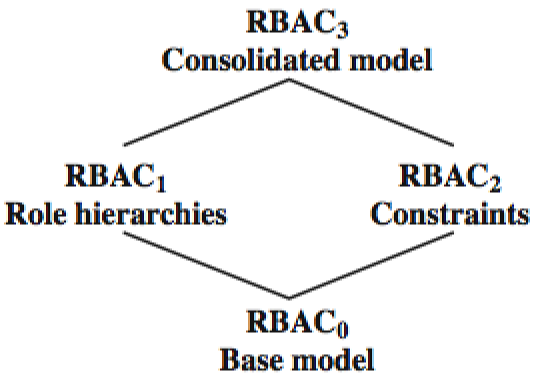
  Operations on an resource are invocated based on the permissions.

- The resource is associated with the user’s role and not the user.

RBAC Variations

A family of RBAC with four models

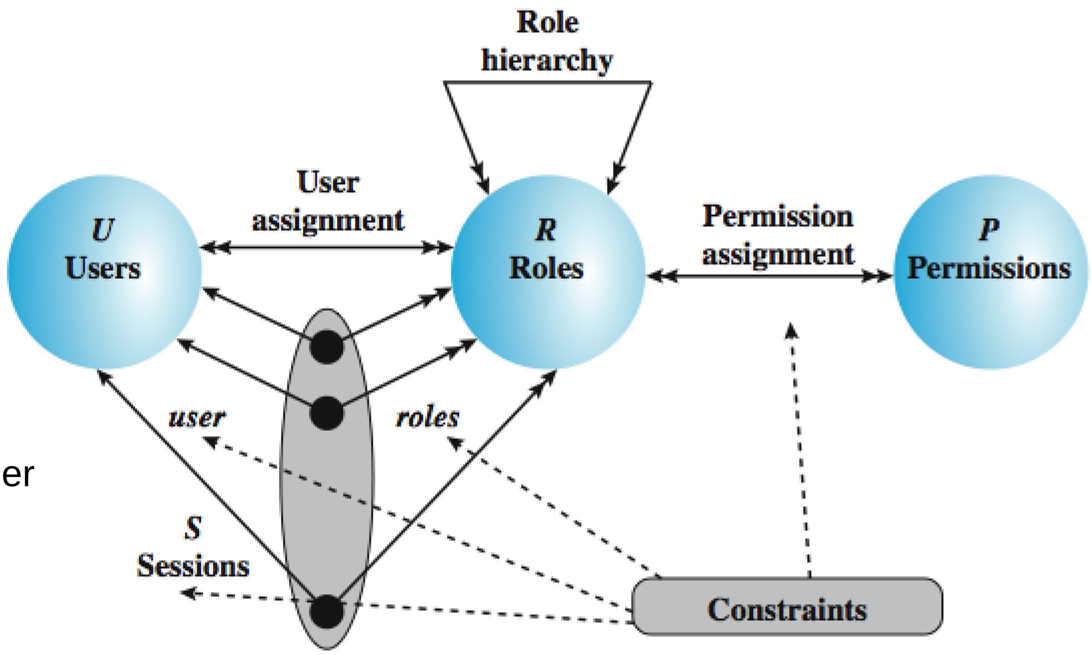
1. RBAC0: min functionality
2. RBAC1: RBAC0 plus role (permission) inheritance
3. RBAC2: RBAC0 plus constraints (restrictions)
4. RBAC3: RBAC0 plus all of the above



(a) Relationship among RBAC models

RBAC0 entities

- User: an individual (with UID) with access to system
- Role: a named job function (tells authority level)
- Permission: equivalent to access rights
- Session: a mapping between a user and set of roles to which a user is assigned



(b) RBAC models

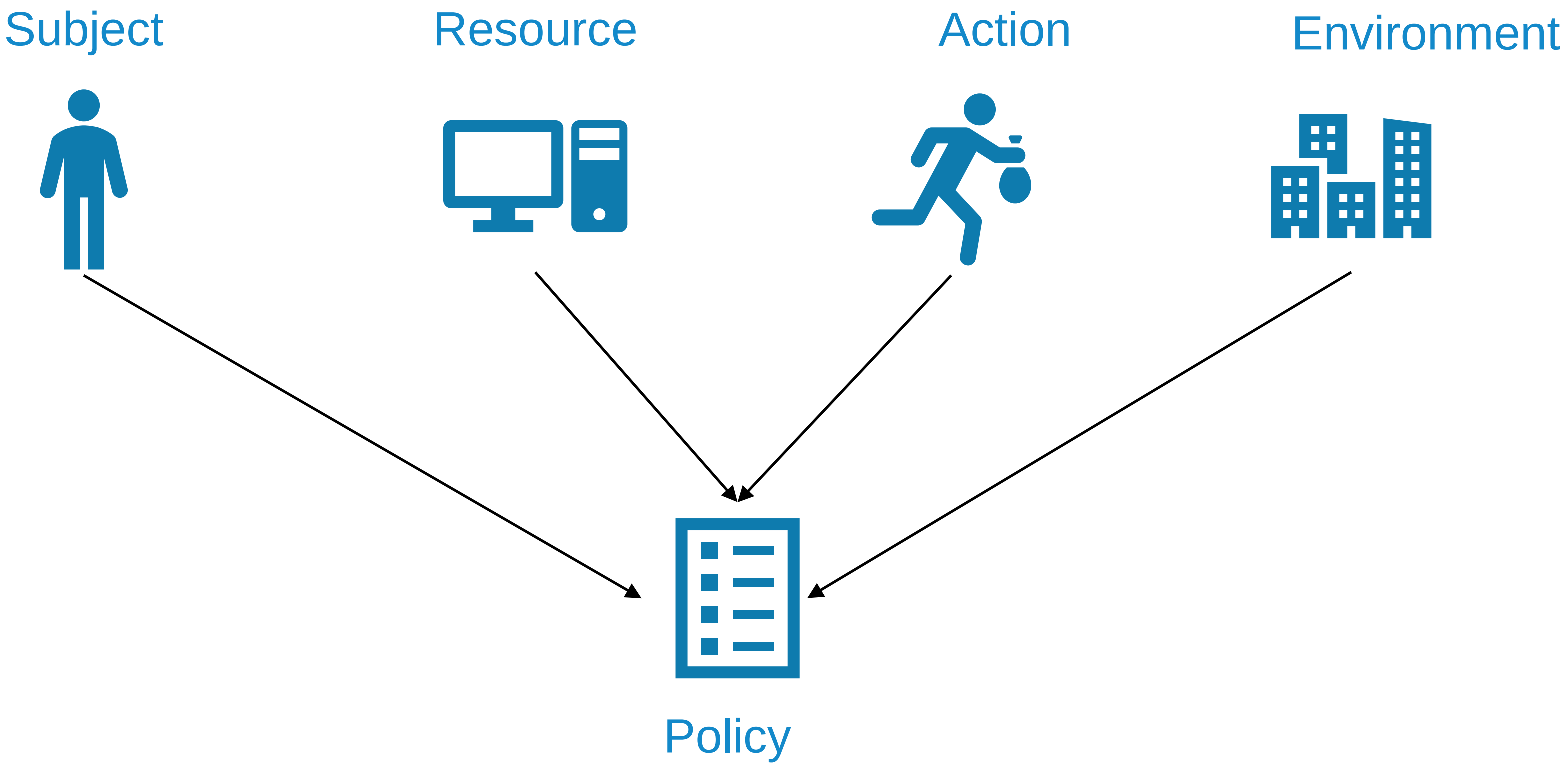
Double arrow: ‘many’ relationship
Single arrow: ‘one’ relationship

ABAC

ABAC is a conditional authorization mechanism based on attributes

Who, What, When, Where, Why, How ?

Attribute assigned to users, Resources, objects & context to indicate time of day, location of the user , IP address.



Subject

Resource

Action

Environment

Policy

Attribute Types

Subject	• Who, Where, Roles, Affiliation, Clearance level
Action	• Create, Read, Update , Delete, execute, GET, PUT, POST
Resource	• Type, Owner, Classification
Environment	• Location, Time, Network

ABAC Policies

Subject	Action	Environment	Resource	Access
Student	Create	IIIT Sri City	Project Report	Allow
Student	Update	IIIT Sri City	Project Report	Allow
Project Guide	Certify	IIIT Sri City	Project Report	Allow
Student	Certify	IIIT Sri City	Project Report	Deny
Project Guide	Certify	IIIT Hyderabad	Project Report	Deny

Permit if
"Student" in Subject.roles and Subject.institute == "IIIT SC" and
action == "Create" and resource.type =="Project Report"

Deny if
"Project Guide" in Subject.roles and action == "Certify" and
resource.type =="Project Report" and Subject.institute != resource. institute

ABAC

- Access control is externalized from Business Logic

- Access controls are maintained as policies centrally

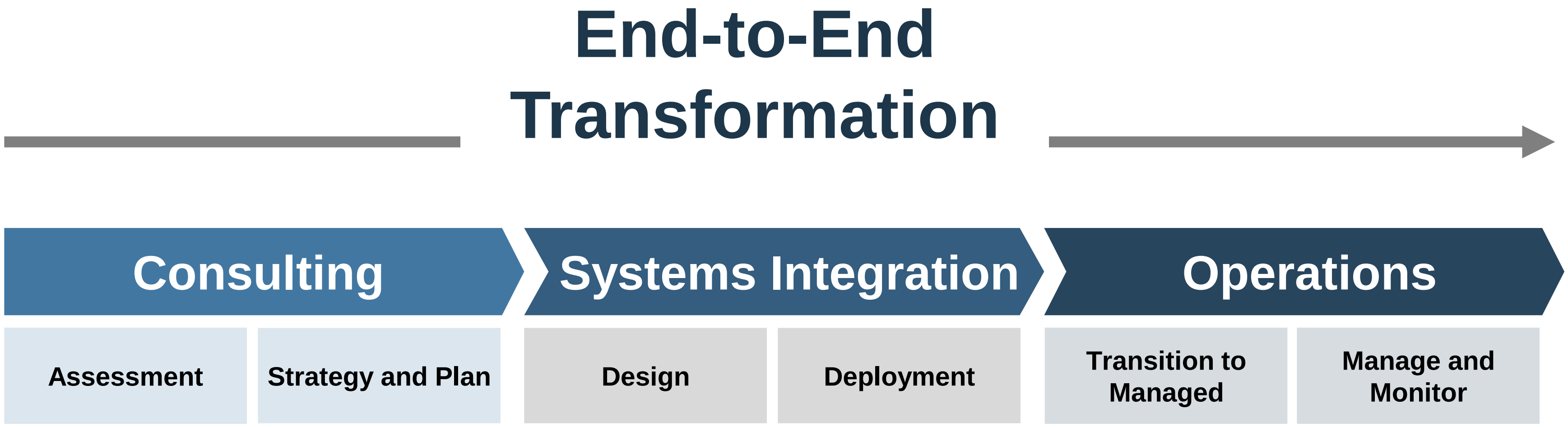
- Access control decisions are made dynamically at runtime

- ABAC helps achieve fine grained access control for a variety of applications especially Web Services & API based apps

- Typically the policies are defined in XACML

IAM in the Enterprise

IAM Transformation



End-to-End Transformation

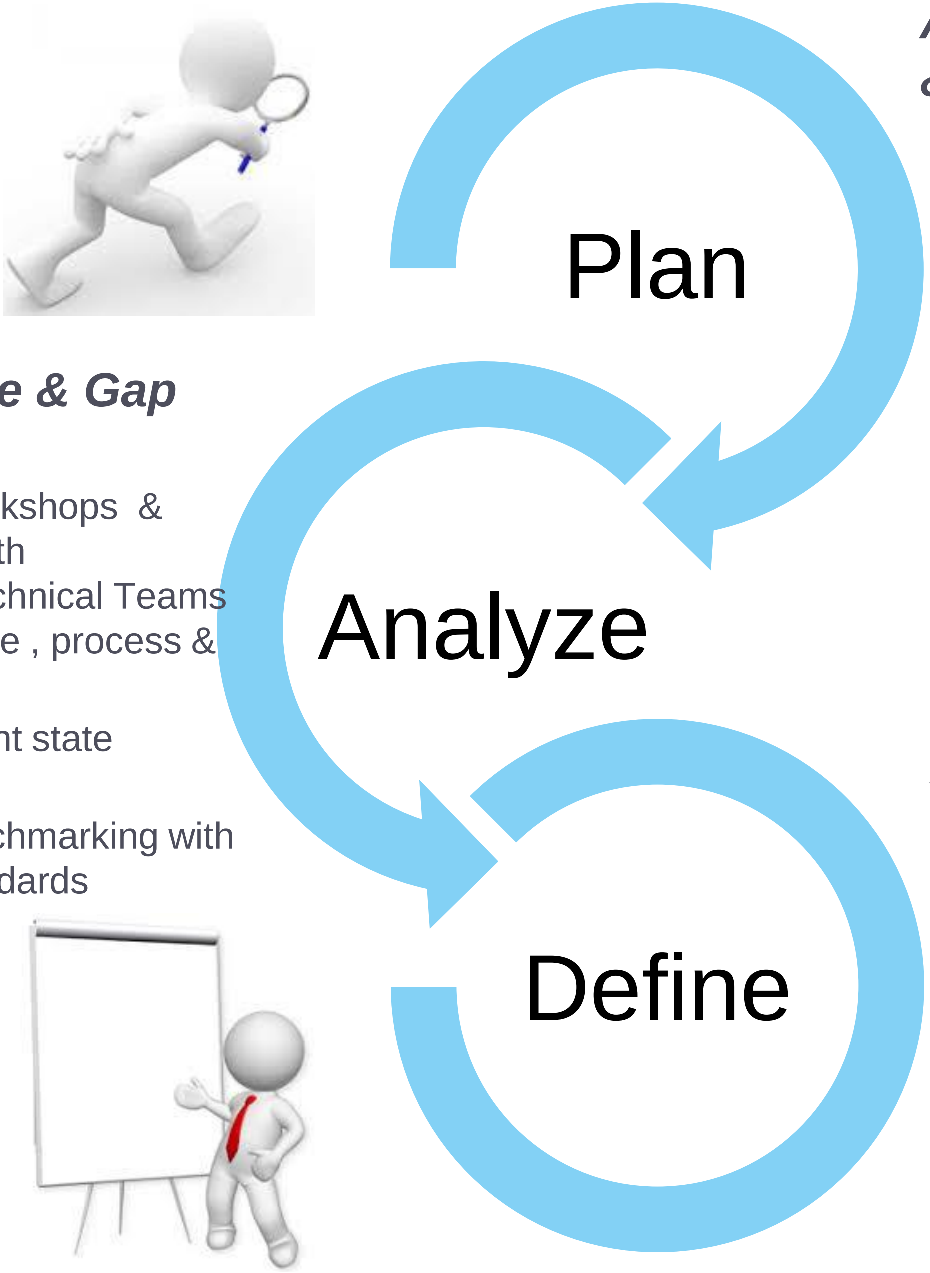
- **Consulting**
  - Assessment
  - Strategy and Plan
- **Systems Integration**
  - Design
  - Deployment
- **Operations**
  - Transition to Managed
  - Manage and Monitor

“Help me understand the options, define and justify an end state and roadmap"

“Create the detailed designs and implement the solution”

“Provide a service to monitor, apply intelligence and alert on significant events”

IAM Planning



Align , Base assessment & Overall Plan

- Set Expectations
- Identify Business & Technical stake holders
- Schedule meetings with stakeholders
- Request As-Is documentation
- Project Plan Review

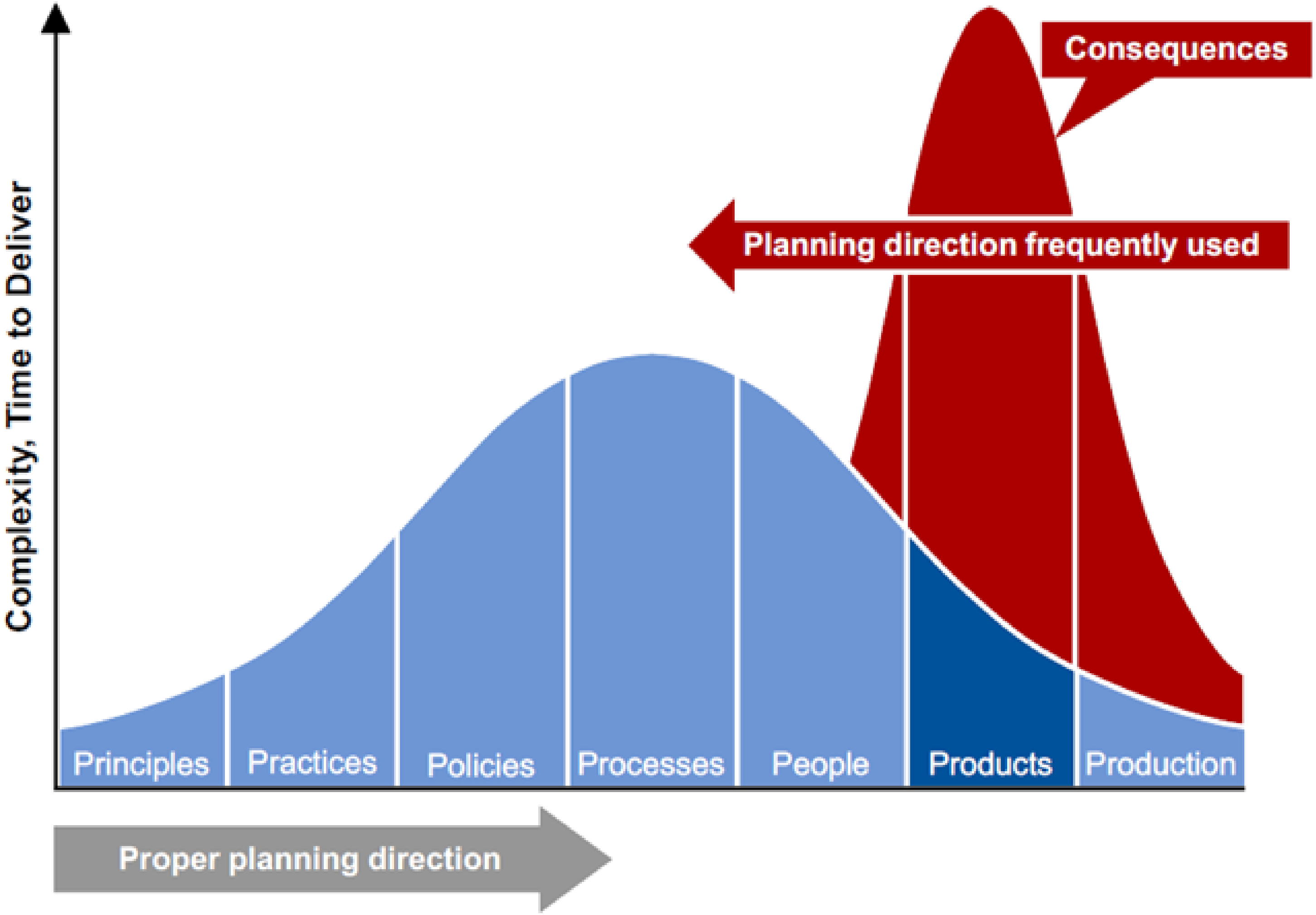
Due Diligence & Gap Assessment

- Conduct Workshops & Interviews with Business/Technical Teams around people , process & technology
- Gather current state information
- Perform benchmarking with Industry standards

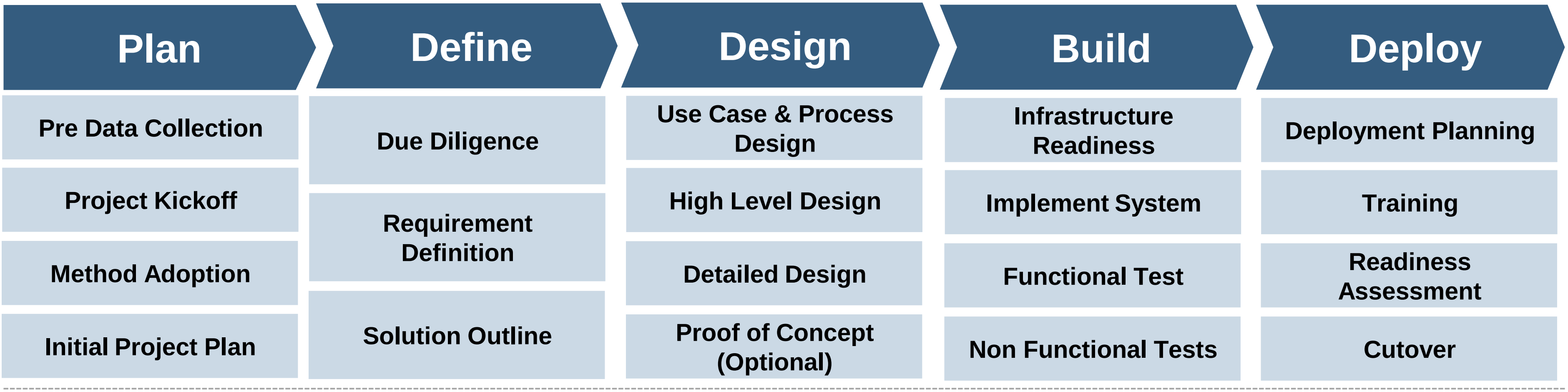
Set Tactical & Strategic Objectives

- Define an appropriate target state
- Design and prioritize guiding principals, Governance framework, Process Architecture, Technical Architecture, Success Factors
- Product Recommendation strategy

50% of IAM projects never reach production


Consequences
Planning direction frequently used
Complexity, Time to Deliver
Principles
Practices
Policies
Processes
People
Products
Production
Proper planning direction

Systems Integration



Plan

- Pre Data Collection
- Project Kickoff
- Method Adoption
- Initial Project Plan

Define

- Due Diligence
- Requirement Definition
- Solution Outline

Design

- Use Case & Process Design
- High Level Design
- Detailed Design
- Proof of Concept (Optional)

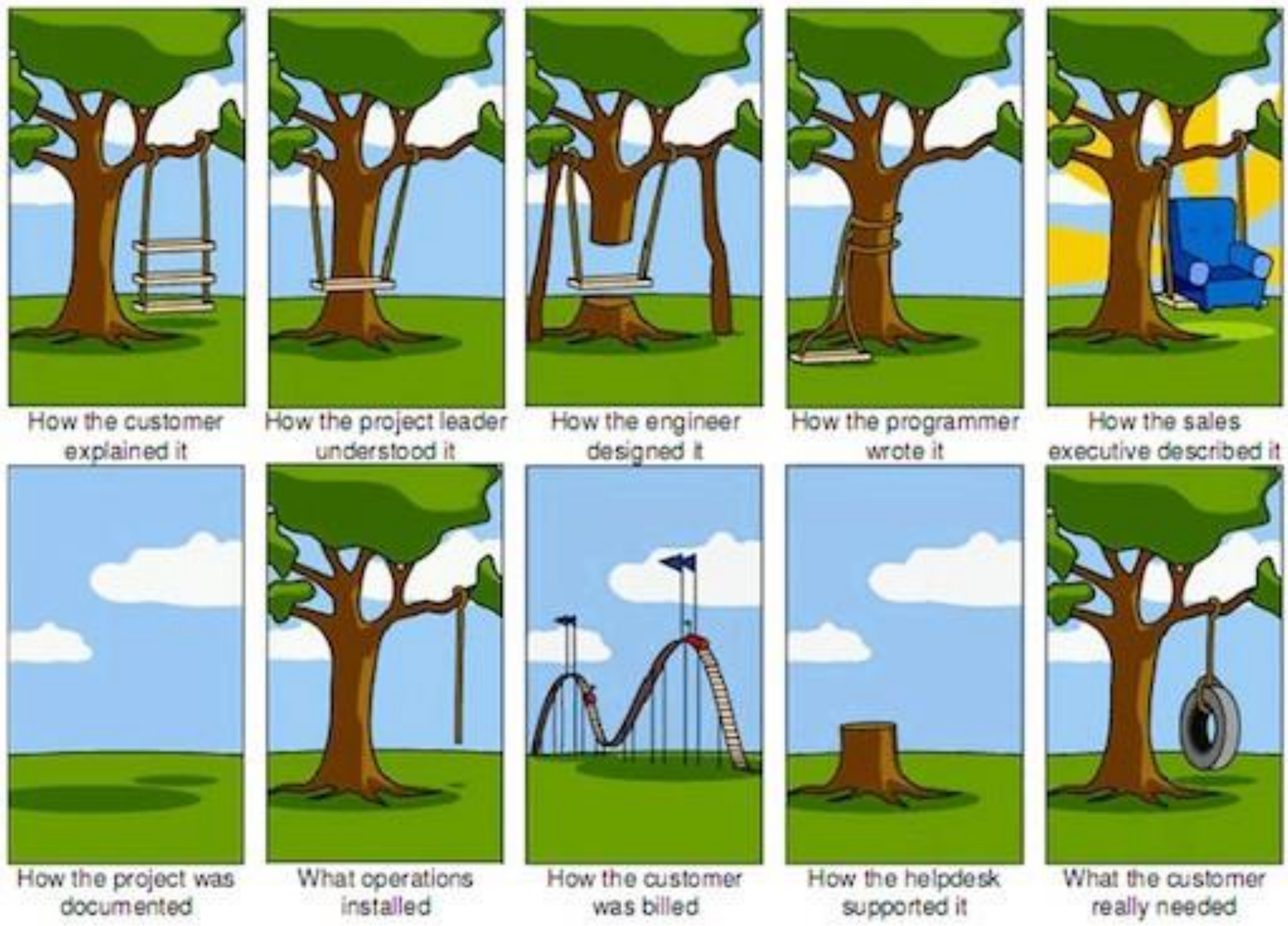
Build

- Infrastructure Readiness
- Implement System
- Functional Test
- Non Functional Tests

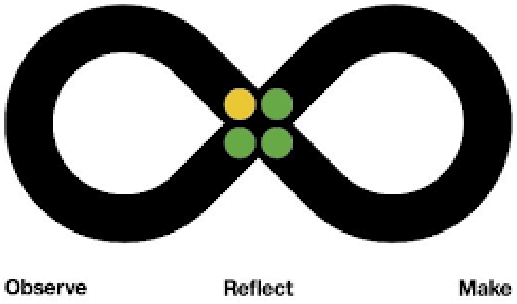
Deploy

- Deployment Planning
- Training
- Readiness Assessment
- Cutover

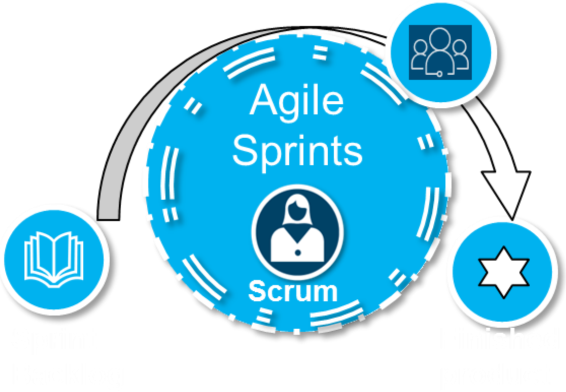
Client Requirements & the communication conumdrum


How the customer explained it
How the project leader understood it
How the engineer designed it
How the programmer wrote it
How the sales executive described it
How the project was documented
What operations installed
How the customer was billed
How the helpdesk supported it
What the customer really needed

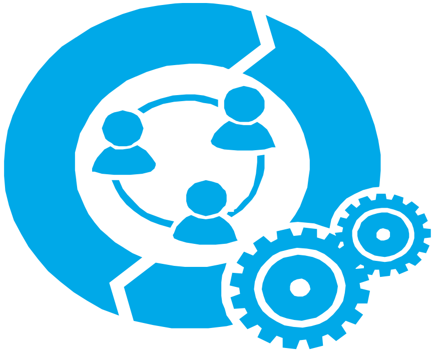
How do we deliver the right solution to meet client needs ?



Design thinking workshops help IAM stakeholders to identify and focus on big problems with clear outcomes for “real” end users

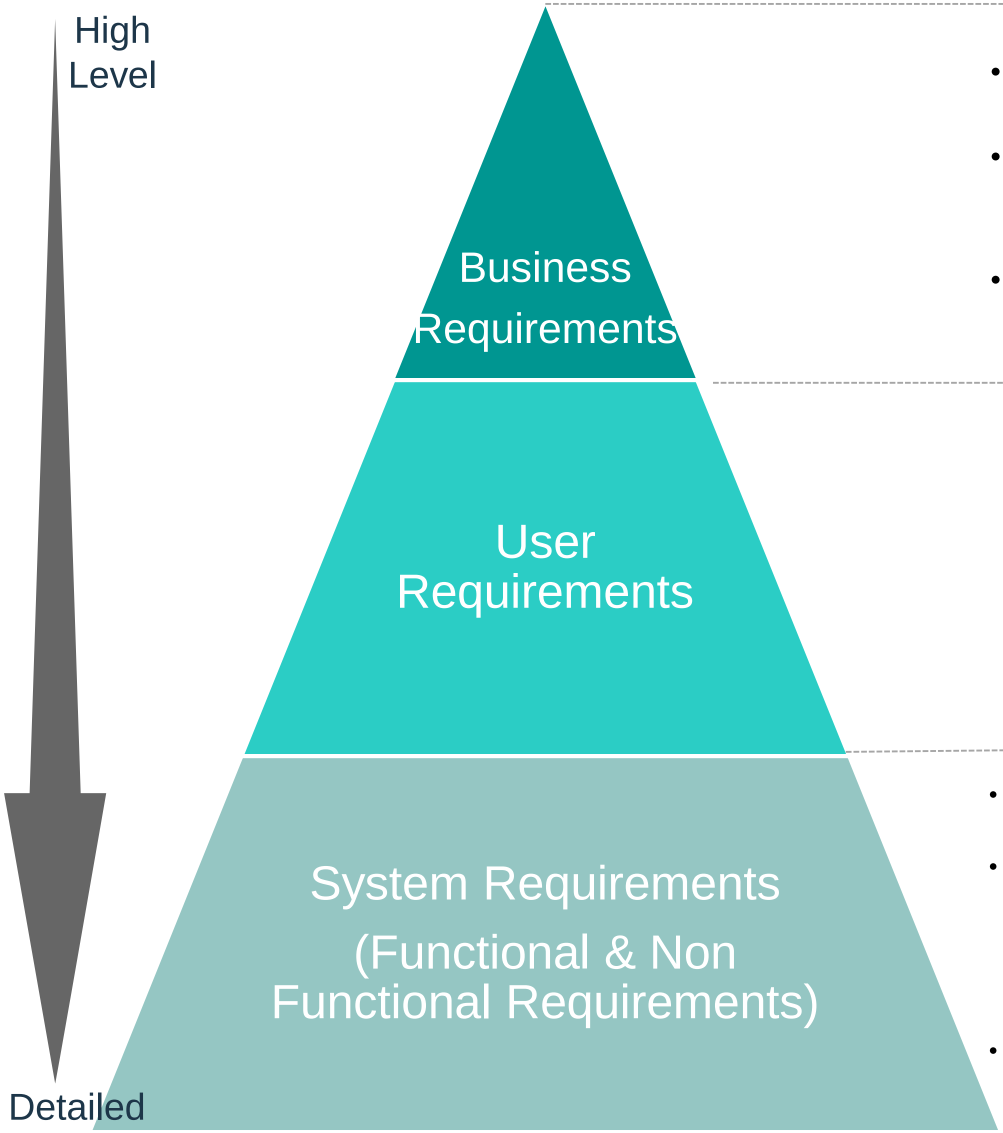


Agile Delivery enables flexible prioritization of requirements and facilitates continuous engagement with business users to ensure right interpretation an implementation of the functionality



Automation with DevOps framework eliminates manual repetitive tasks in the SDLC lifecycle for accelerating deployments and eliminating manual errors

Requirements



High Level

Business Requirements

- Derived from a Business' Vision, Goal & Objective
- High level statements but with adequate clarity and details ensuring the project goals are met
- Defines the scope of the project

User Requirements

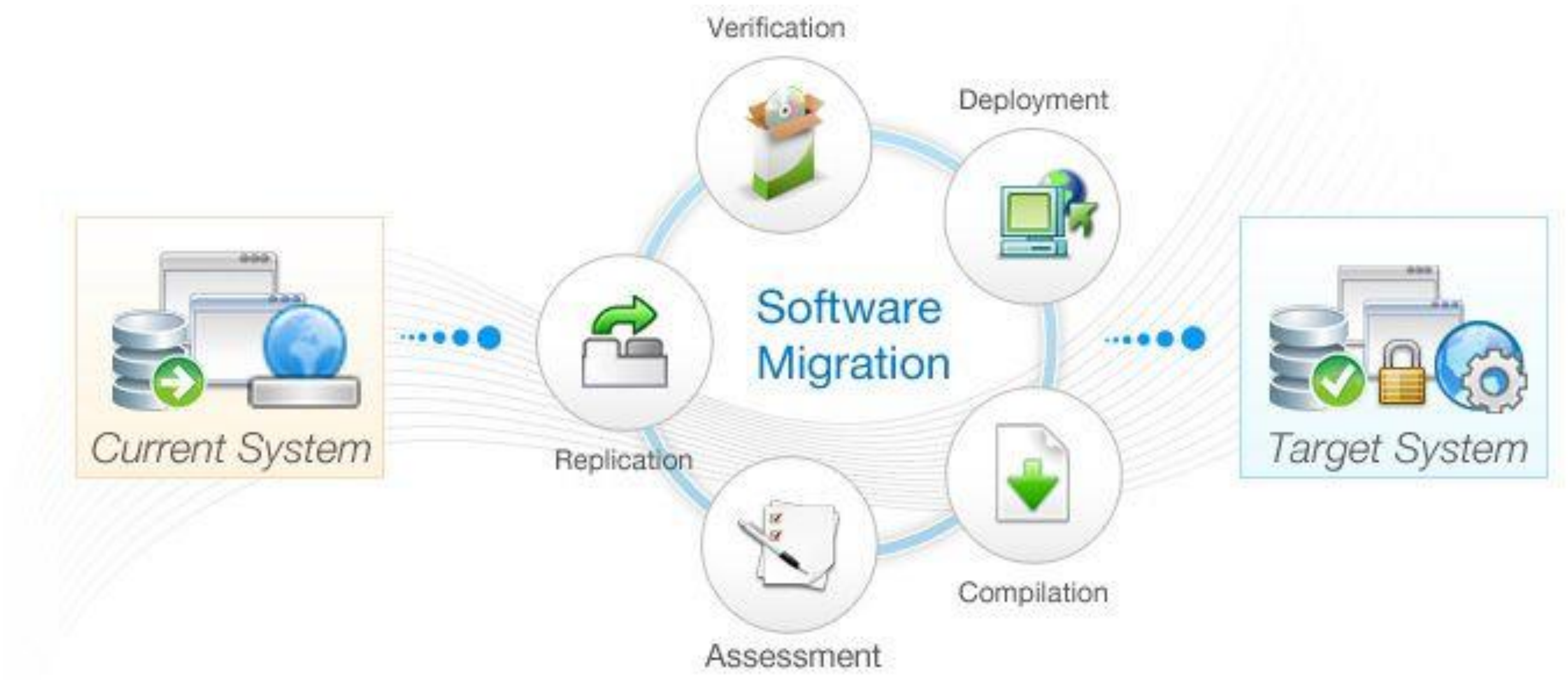
- Defines the requirements from the users point of view
- Specifies the user interactions with the system and the related input & output

System Requirements (Functional & Non Functional Requirements)

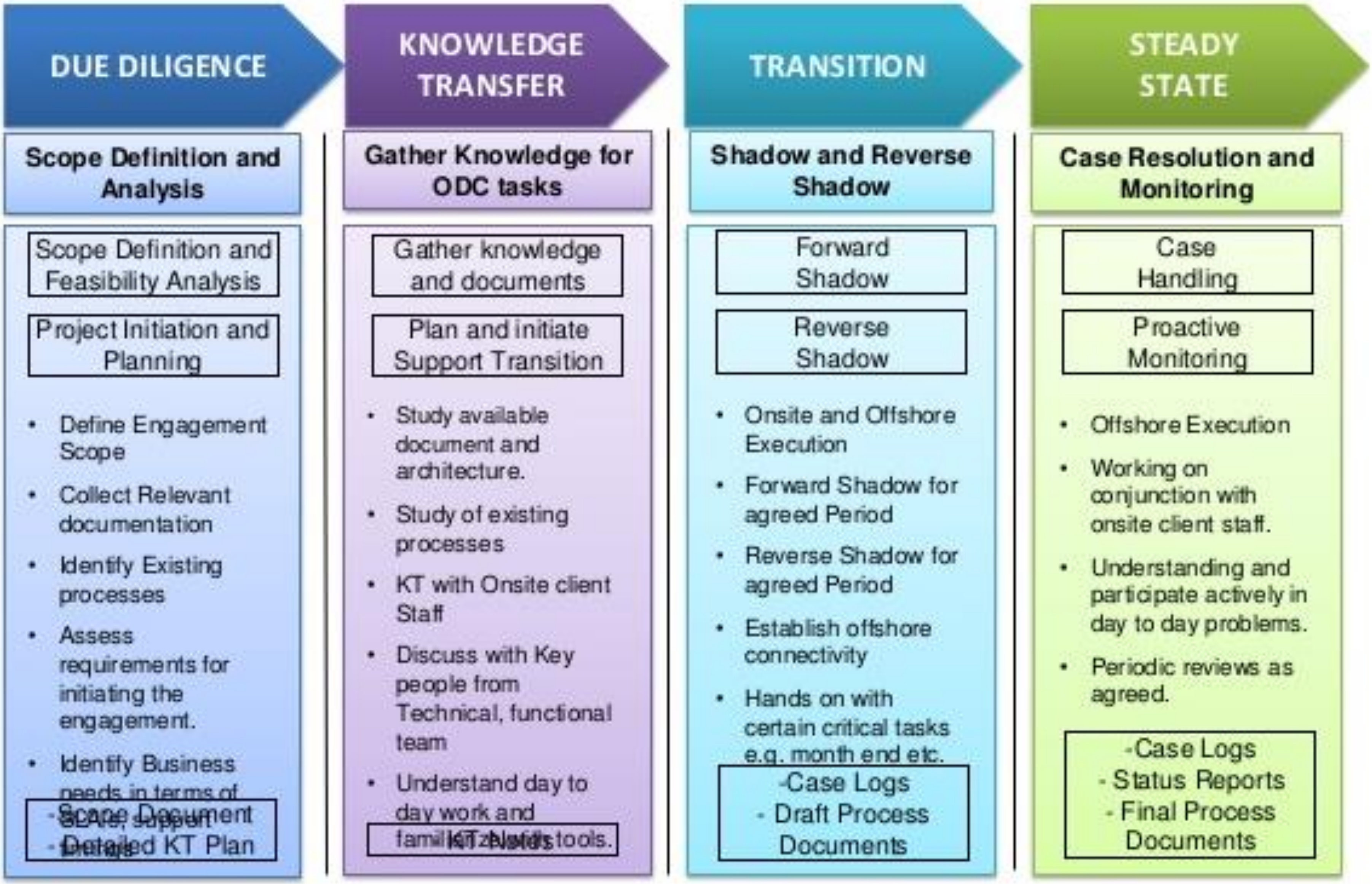
- Systems Requirements describe the functions which the system as a whole should fulfill to satisfy the stakeholder needs and requirements
- Functional Requirements defines the external behavior of the system
  - How the system interacts within it's subsystems & with its users & external interfaces
  - Define the system behavior under various conditions and its response to different inputs
- Non-Functional Requirements define the quality attributes or the constraints of the system

Detailed

Migration


Verification
Deployment
Current System
Software Migration
Target System
Replication
Compilation
Assessment

Transition Model



DUE DILIGENCE

Scope Definition and Analysis

Scope Definition and Feasibility Analysis

Project Initiation and Planning

- Define Engagement Scope
- Collect Relevant documentation
- Identify Existing processes
- Assess requirements for initiating the engagement.
- Identify Business needs in terms of SLAs, support metrics

- Scope Document
- Detailed KT Plan

KNOWLEDGE TRANSFER

Gather Knowledge for ODC tasks

Gather knowledge and documents

Plan and initiate Support Transition

- Study available document and architecture.
- Study of existing processes
- KT with Onsite client Staff
- Discuss with Key people from Technical, functional team
- Understand day to day work and familiarize with tools.

KT Notes

TRANSITION

Shadow and Reverse Shadow

Forward Shadow

Reverse Shadow

- Onsite and Offshore Execution
- Forward Shadow for agreed Period
- Reverse Shadow for agreed Period
- Establish offshore connectivity
- Hands on with certain critical tasks e.g. month end etc.

-Case Logs
- Draft Process Documents

STEADY STATE

Case Resolution and Monitoring

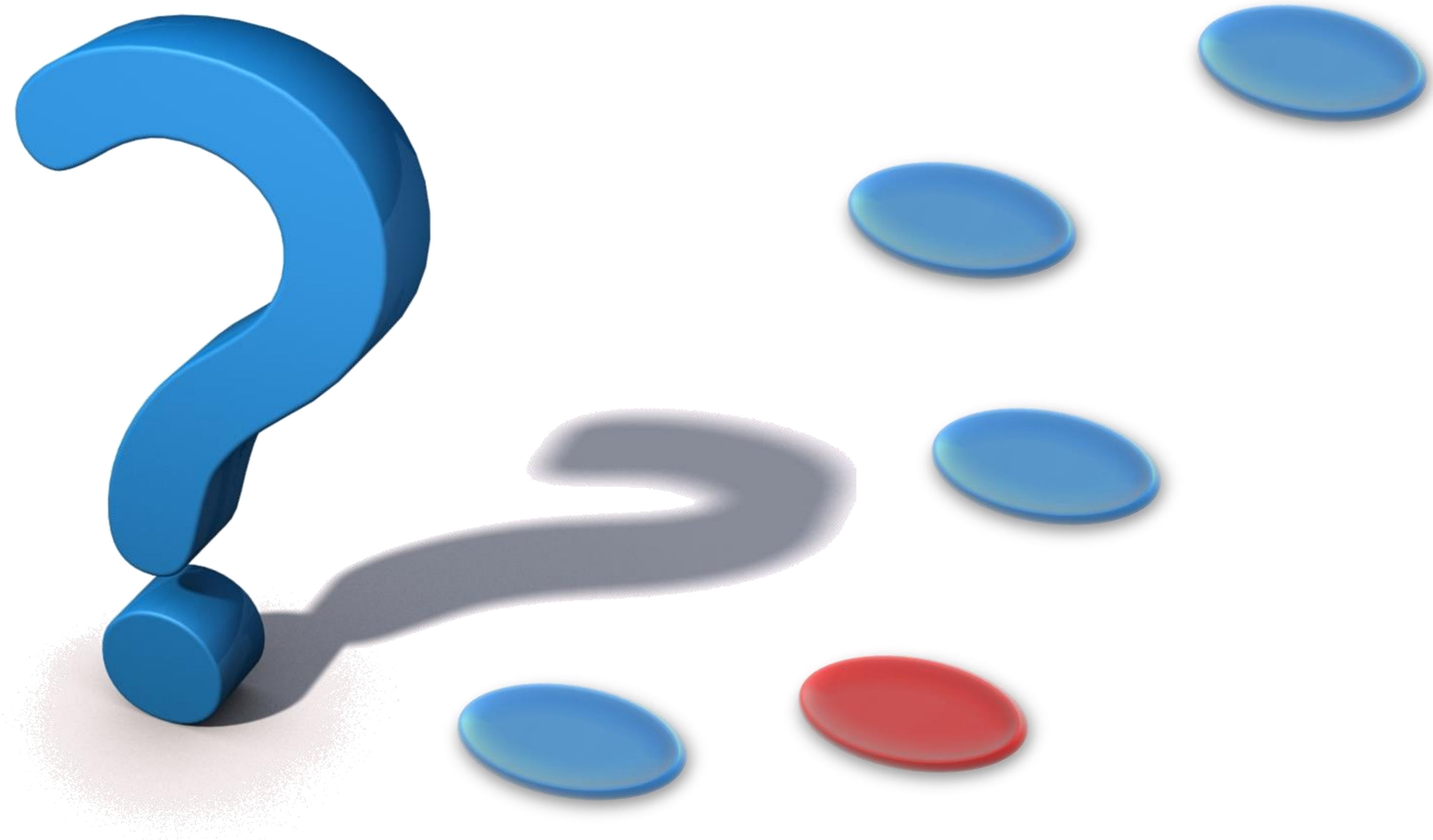
Case Handling

Proactive Monitoring

- Offshore Execution
- Working on conjunction with onsite client staff.
- Understanding and participate actively in day to day problems.
- Periodic reviews as agreed.

-Case Logs
- Status Reports
- Final Process Documents

Q&A



Thank You