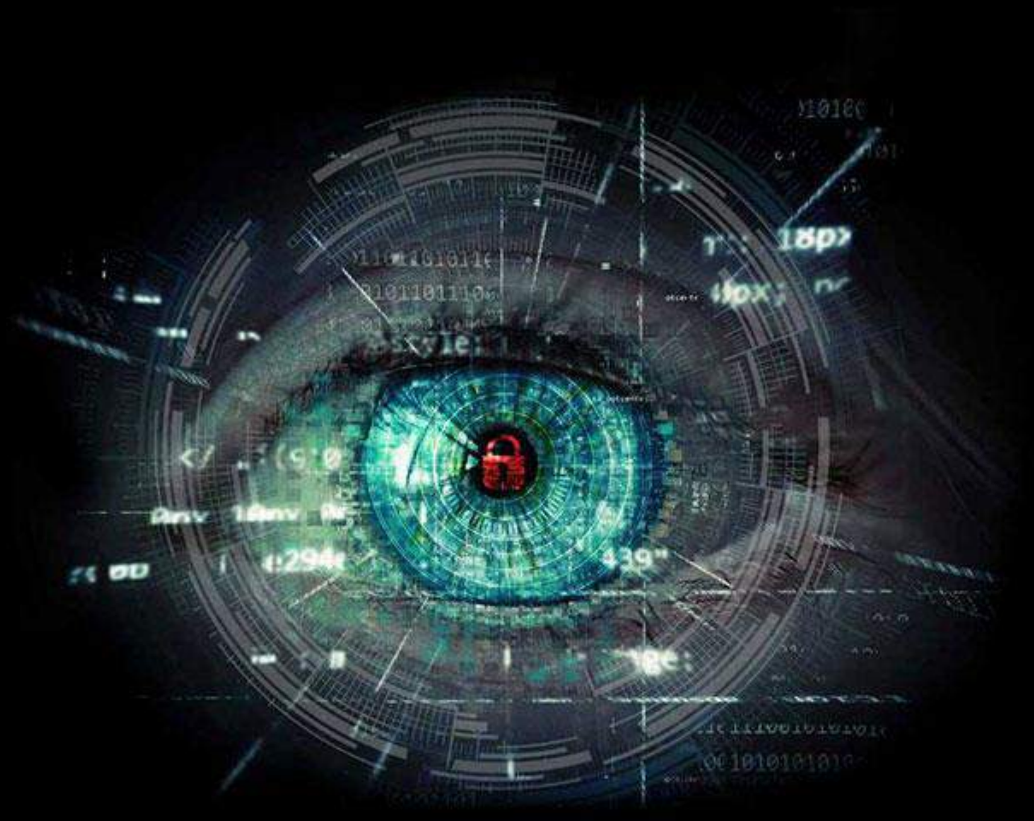
Cyber Security

Identity & Access Management (IAM)

Senthilkumar
Information Security Professional

8th October 2022

Agenda



01

IAM Framework

- JML Processes (Joiner, Mover, Leaver)
- Entitlement Management
- Types of Access Control
- Recertification Process

02

IAM Principles

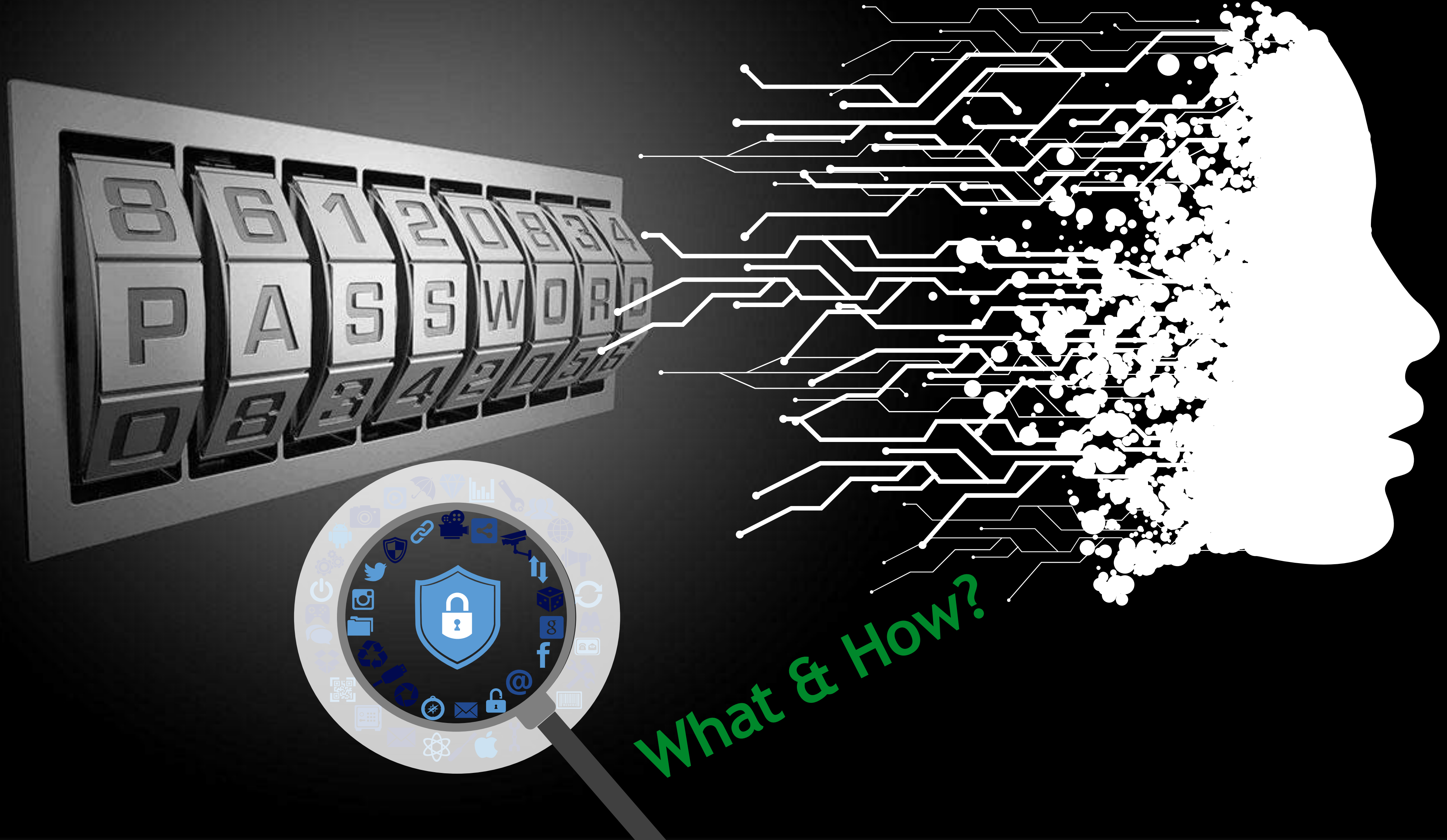
- Authentication
- Authorization
- Accounting

03

Why IAM is important?

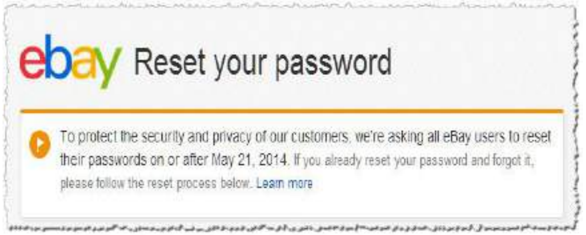
- Identity Risks
- Digital Transformation Impacts & Threats.
- Key Factors for IAM Planning.
- Modern IAM Decisions
- Covid Pandemic and IAM

The Power of Identity



What & How?

Recent Cyber Attacks – Poor IAM Implementations



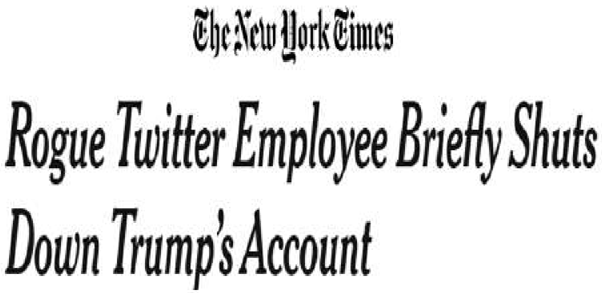
ebay Reset your password

To protect the security and privacy of our customers, we're asking all eBay users to reset their passwords on or after May 21, 2014. If you already reset your password and forgot it, please follow the reset process below. Learn more

The breach exposed the names, addresses, DOB, phone numbers & encrypted passwords of 145 million users.

Hackers spent 7 months inside eBAY.

The Hack of the Century.
100 Terabytes data breach

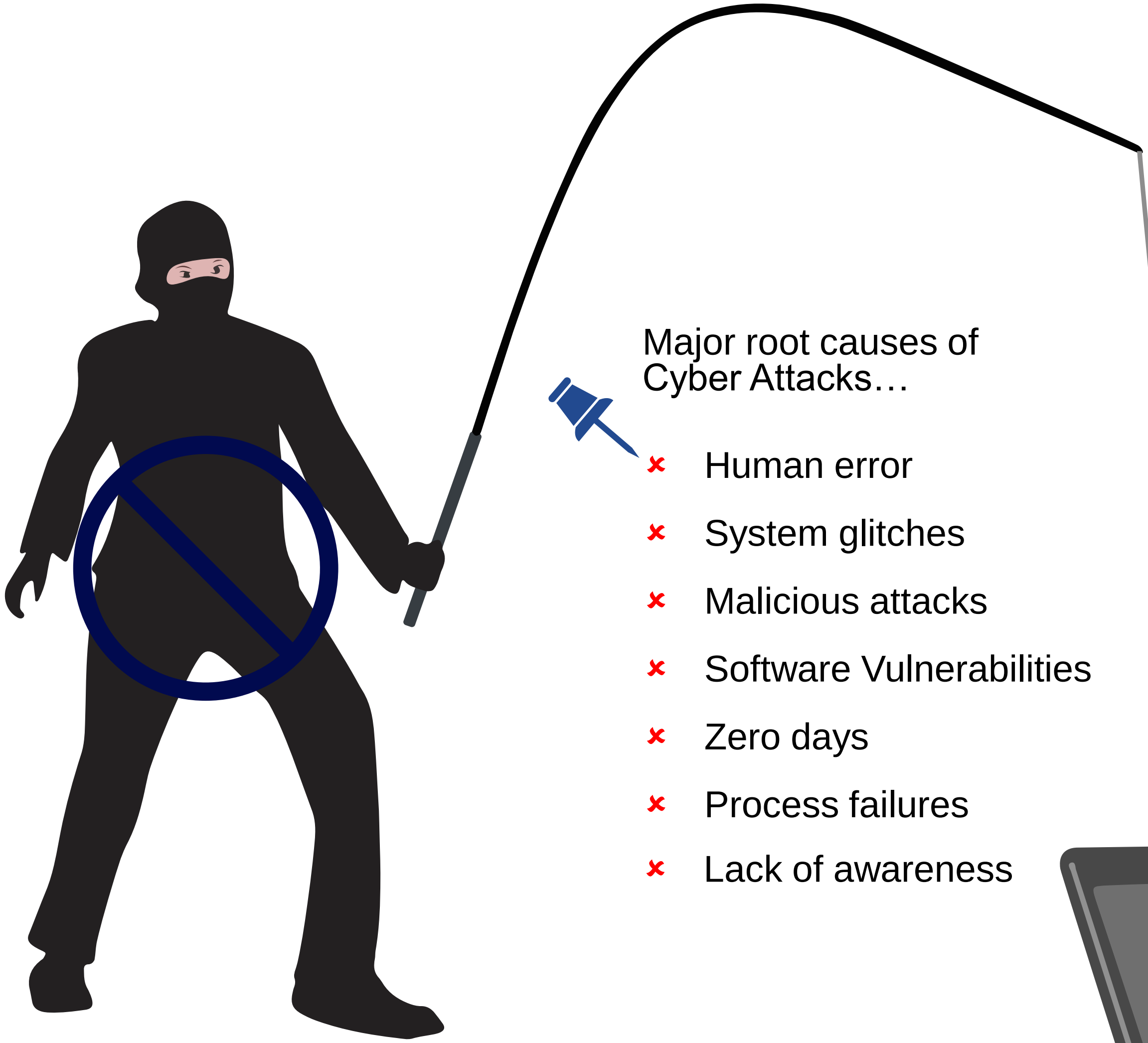


The New York Times

Rogue Twitter Employee Briefly Shuts Down Trump's Account

Deloitte has a robust, multi-layered security system

Deloitte compromised due to poor IAM implementation.



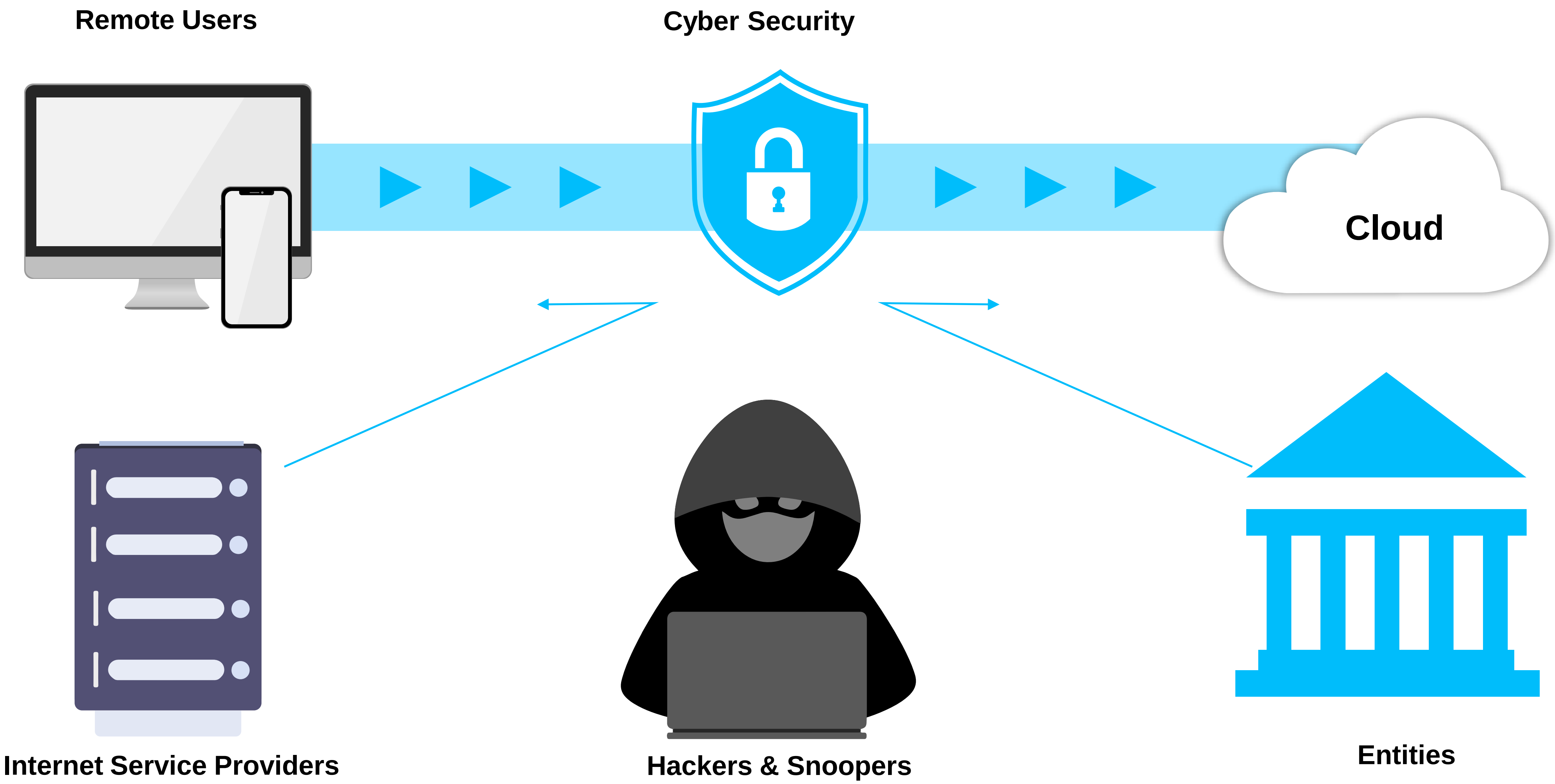
Major root causes of Cyber Attacks…

- ✗ Human error
- ✗ System glitches
- ✗ Malicious attacks
- ✗ Software Vulnerabilities
- ✗ Zero days
- ✗ Process failures
- ✗ Lack of awareness

Cyber Security

- ✓ Security Awareness
- ✓ End-user Security
- ✓ Operational Security
- ✓ Application security
- ✓ Information security
- ✓ Network Security
- ✓ Disaster Recovery Planning

Modern Digital Workspace



Remote Users

Cyber Security

Cloud

Internet Service Providers

Hackers & Snoopers

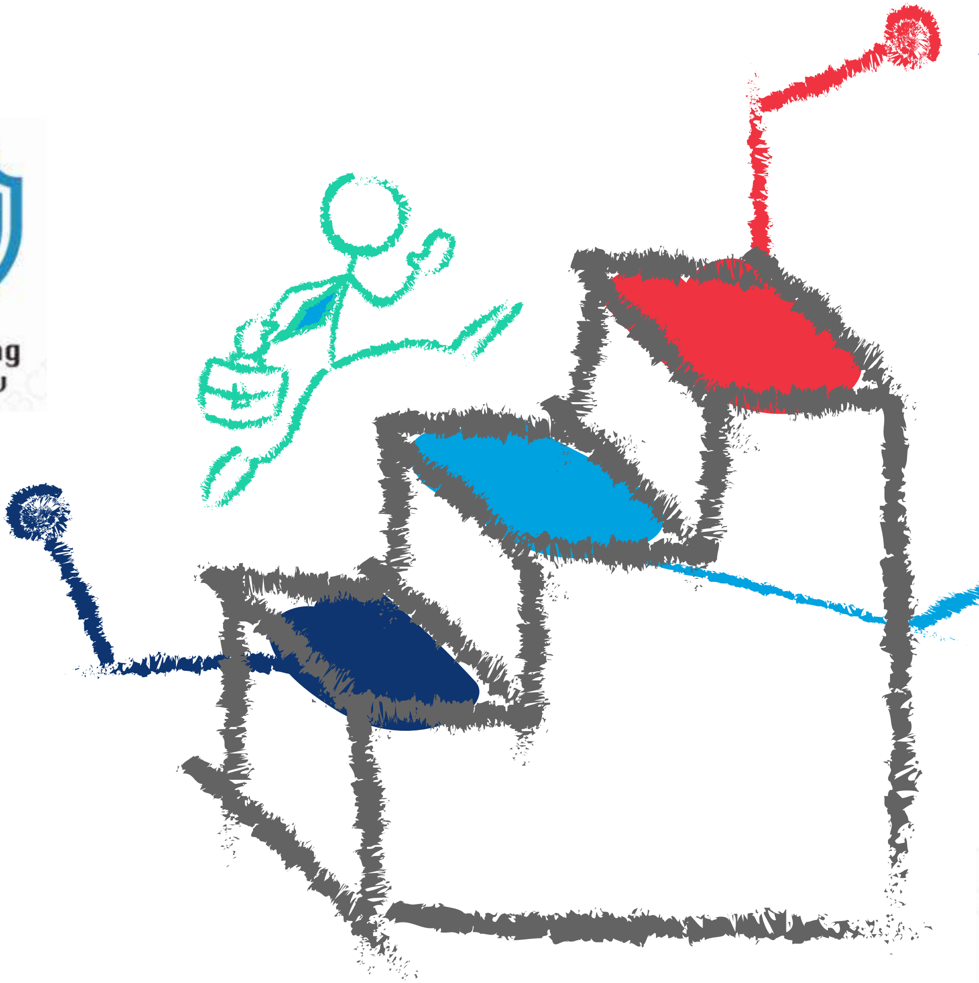
Entities

IAM – AAA Principles

Something you have
Something you are
Something you know

Authentication

- Static passwords which remain active until they are changed or expired,
- One-time password (OTP) such as codes delivered thorough SMS texts or tokens used for each access session,
- Digital certificate
- Biometric credential.

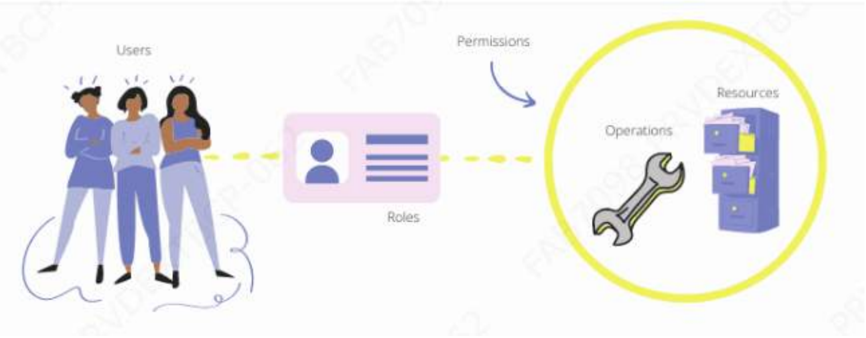


Accountability / Auditing

- The process of keeping track of a user’s activity while accessing the system resources, processes along with time stamp

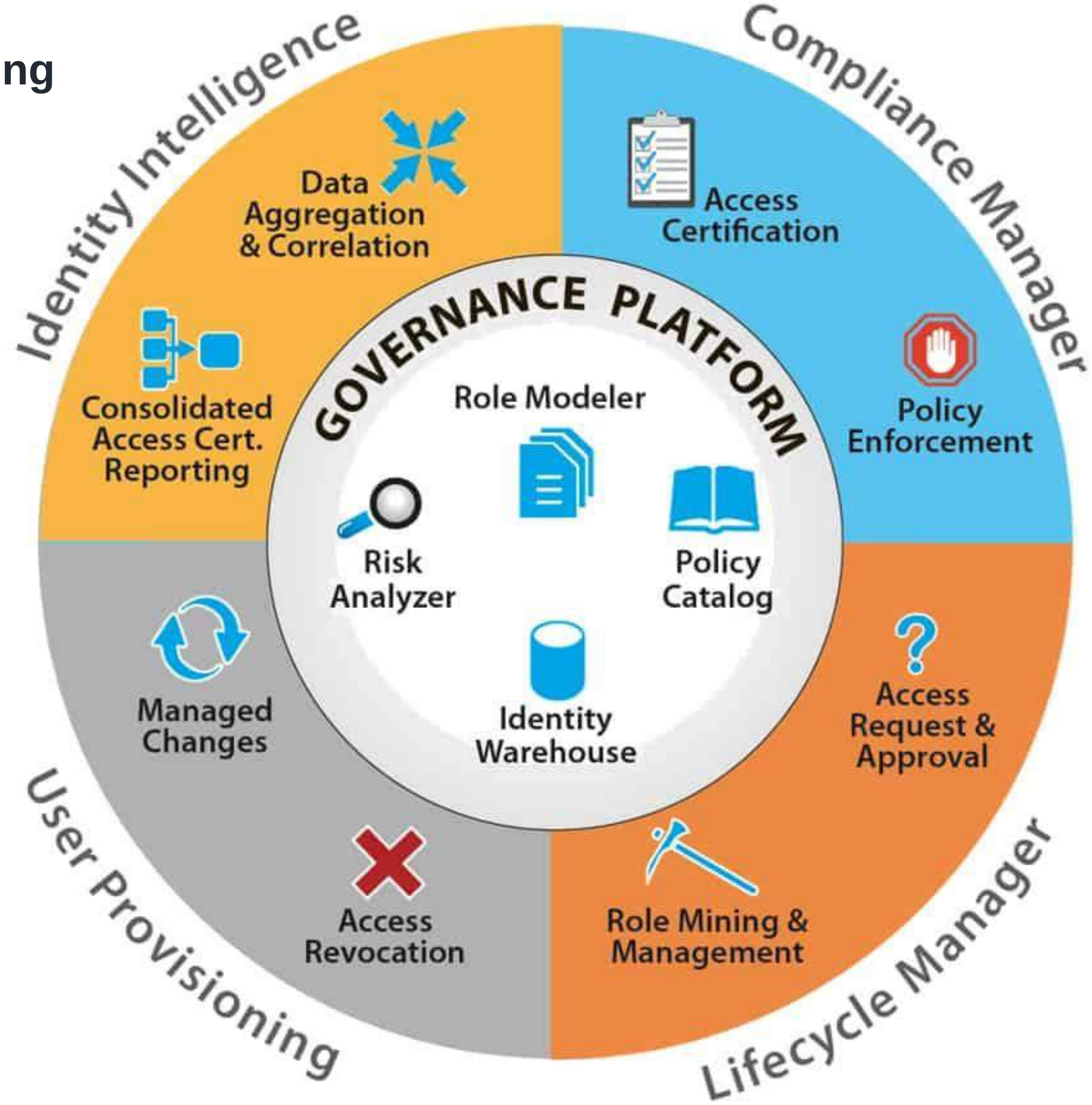
Authorization

- The process of granting or denying a user access to system resources once the user has been authenticated.



IAM Framework

- Automate User Provisioning
- Password Management
- Analytics & reporting



- Access Certifications
- Policy Enforcement
- Risk Assessment

Access Control Models

1

Discretionary Access Control (DAC)

Access to resources is decided by Data owners

2

Mandatory Access Control (MAC)

Access to resources is decided by system/OS based on security labels

3

Rule-Based Access Control (RB-RBAC)

Access to resources is decided based on predefined rules

4

Attribute Based Access Control (ABAC)

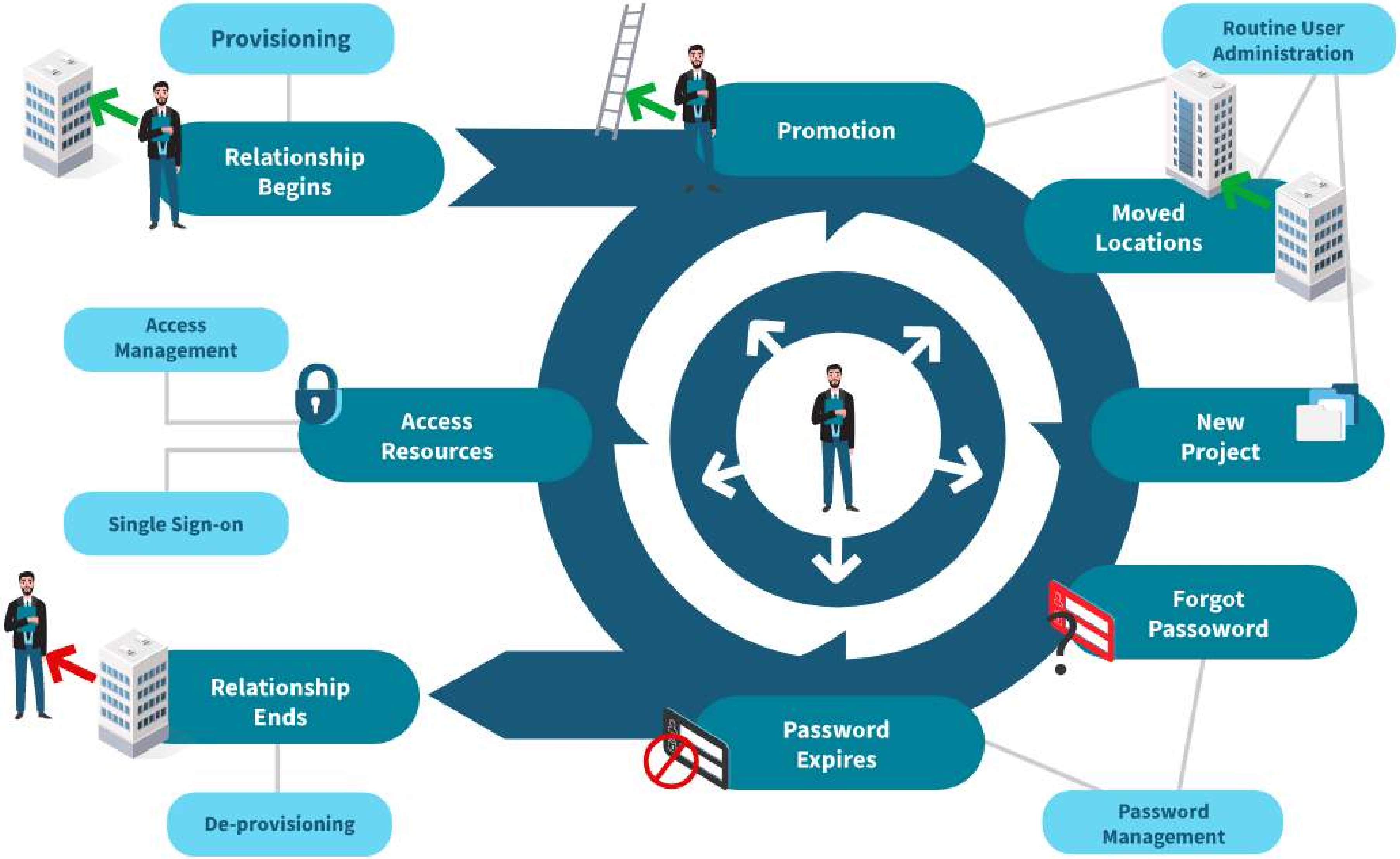
Access to resources is decided based on user's attribute values

5

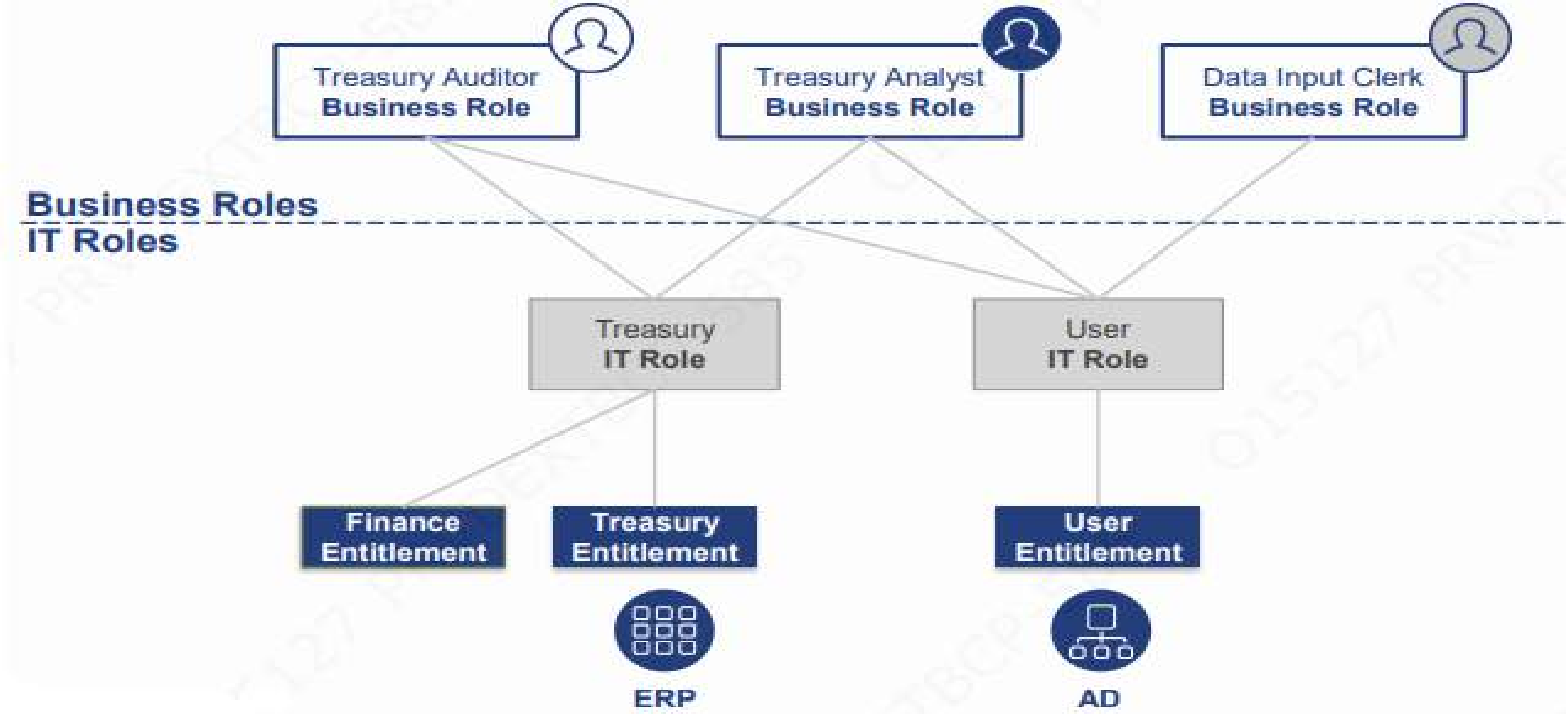
Role-Based Access Control (RBAC)

Access to resources is decided based on user's role

Identity Life Cycle Management



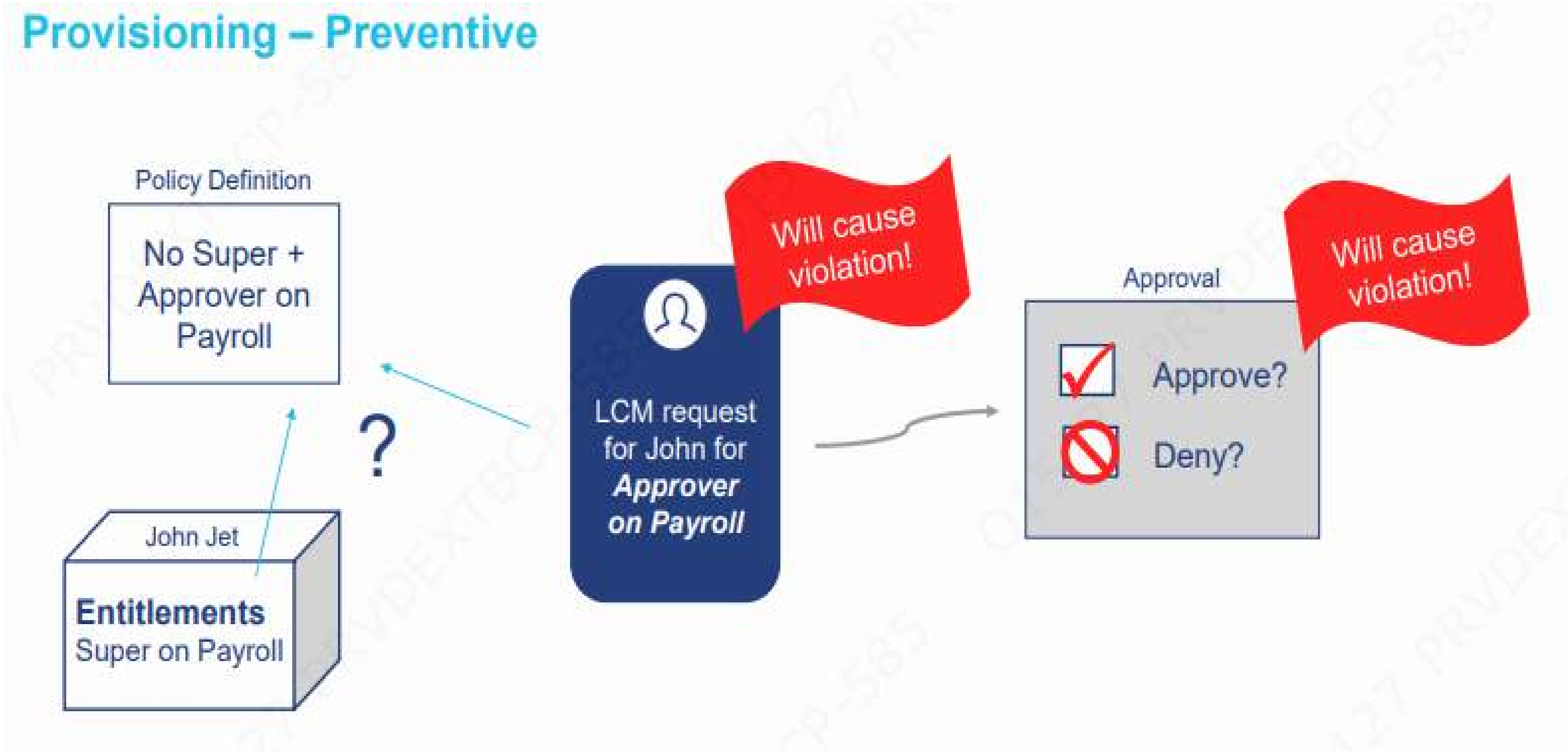
Role Based Access Control



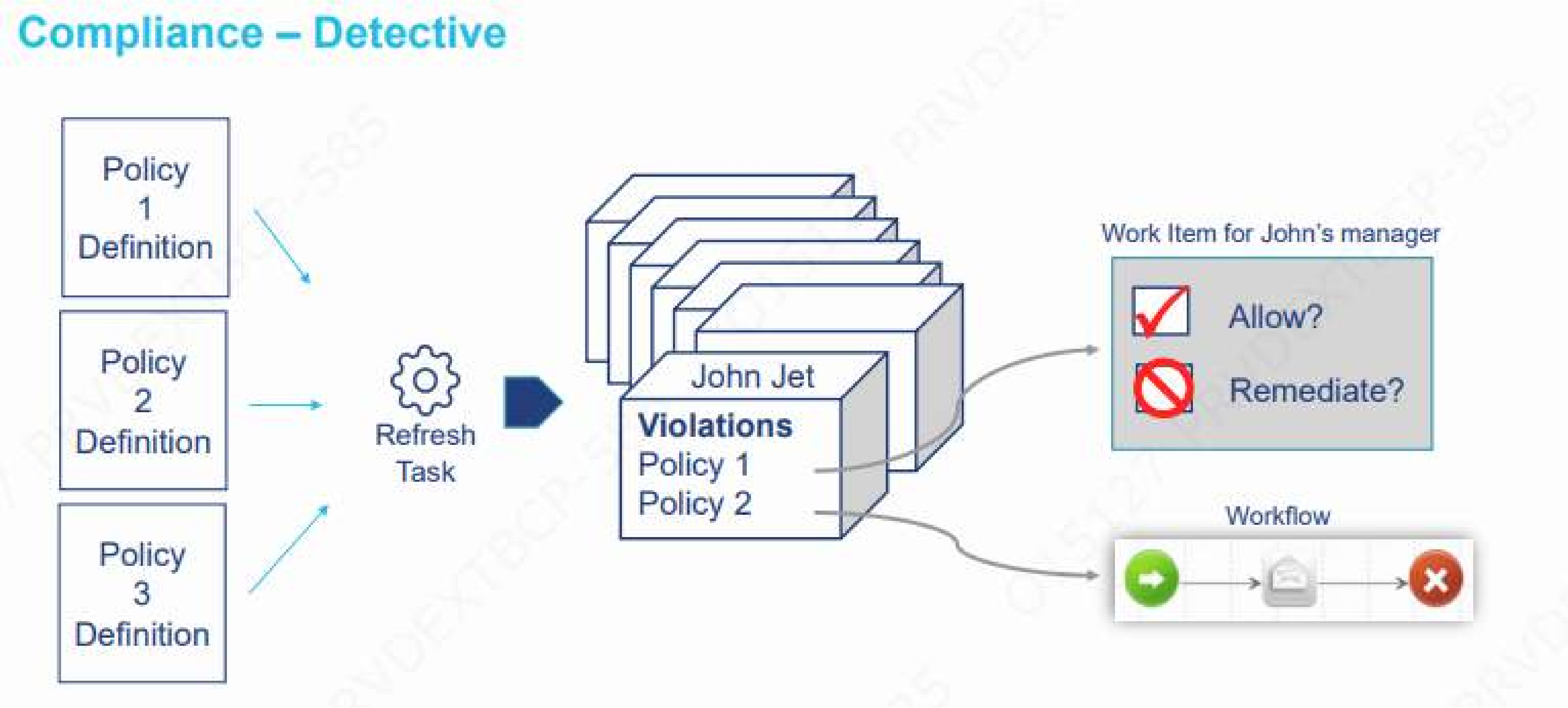
Segregation of Duties (SOD)

Internal control ensures that no one user / role can complete transaction within any business processes end to end without proper checks and balances to avoid error or fraud

Compliance – SOD Preventive Policy



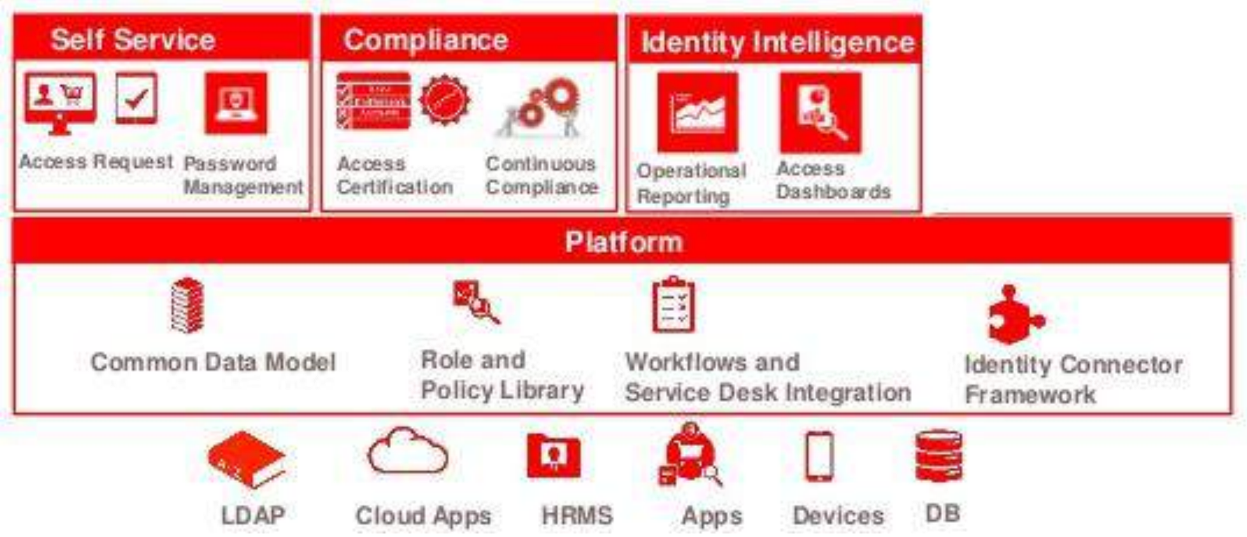
Compliance – SOD Detective Policy



Access Recertification Process

The recertification process enables organizations to answer key questions such as:

- *Who has access to what?*
- *When was access granted and used?*
- *Who has excessive access privileges?*
- *Is access still valid and in-line with company policy?*



Self Service

Access Request

Password Management

Compliance

Access Certification

Continuous Compliance

Identity Intelligence

Operational Reporting

Access Dashboards

Platform

Common Data Model

Role and Policy Library

Workflows and Service Desk Integration

Identity Connector Framework

LDAP

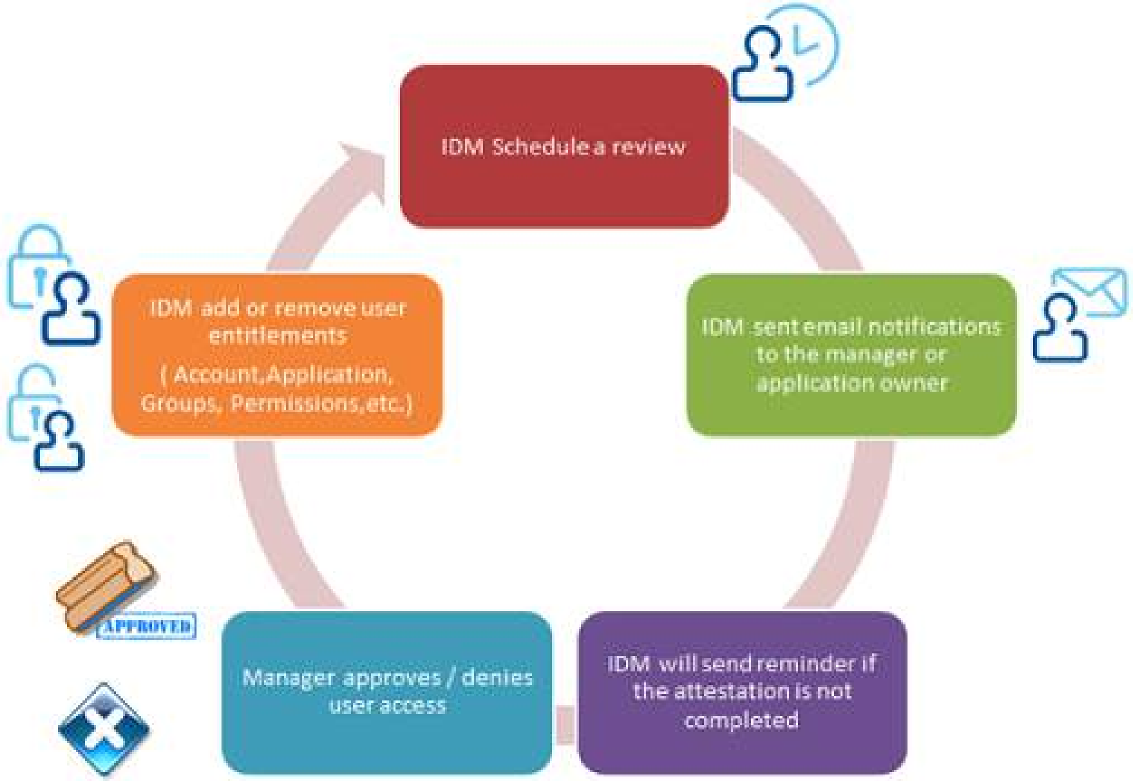
Cloud Apps

HRMS

Apps

Devices

DB



IDM Schedule a review

IDM sent email notifications to the manager or application owner

IDM will send reminder if the attestation is not completed

Manager approves / denies user access

IDM add or remove user entitlements

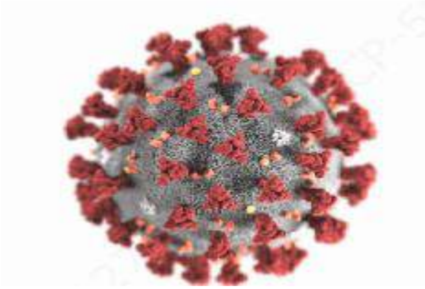
(Account,Application, Groups, Permissions,etc.)

Common Identity Risks

Orphan Accounts

Entitlement Creep

Shared Generic Accounts



Rouge Accounts

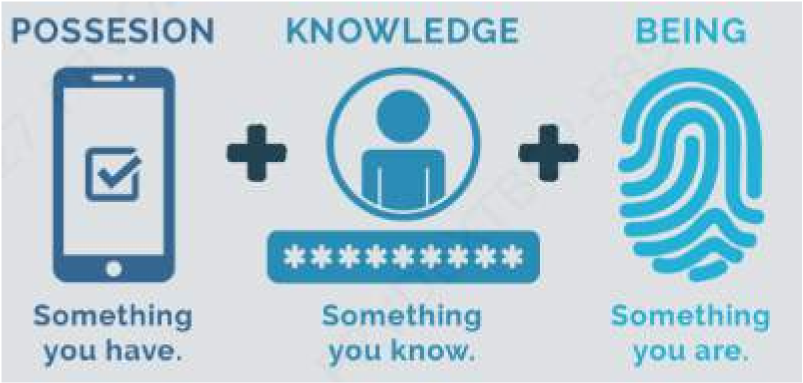
Very easy & Very Complex password policy

Segregation-of-Duty Policy

Contractors or Temporary Workers Identity management

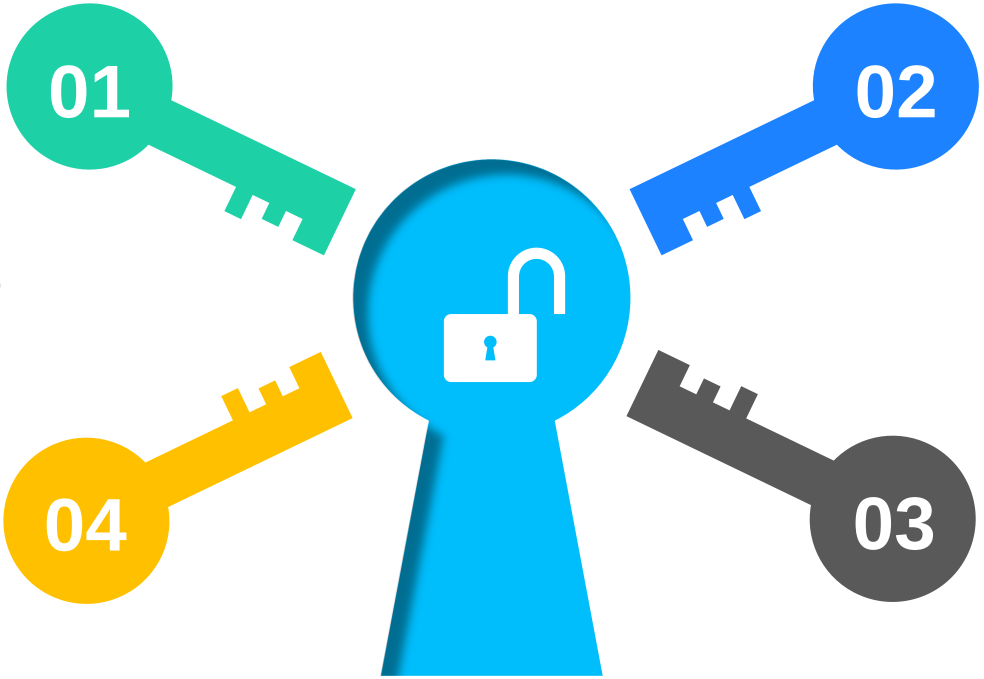
IAM Best Practices

IAM programs must support shifting investments from on-premises to off-premises capabilities and support more agility in multicloud and hybrid environments.



- ✓ Automate Onboarding and offboarding
- ✓ 4 Eye Principle
- ✓ Least Privilege Principle
- ✓ SOD Enforcement
- ✓ Role Management
- ✓ Centralized User Repository
- ✓ RBAC
- ✓ Risk Based Identity Management
- ✓ Multi Factor Authentication (MFA)
- ✓ Federation
- ✓ SSO
- ✓ Session Management
- ✓ Routine Review and Removal of Orphan Accounts
- ✓ Segregation between risky identity and less risky identities.

Modern Identity Decisions



Application and DevOps Teams

Who is responsible to design, develop, test and implement technical solution for business operations.

Security Team

Who is responsible for computer and network security and support business operations securely

Infrastructure and Operations Team

Who is responsible to configure, monitor and administrating the IT infrastructure for business operations

IAM Team

Who is responsible to define, enforce identity access management methodologies in line with Policy and procedures.

Modern Identity Decisions

Covid Pandemic & IAM

Technology Choice – Teleworking options and Impacts

- ✓ VPNs, virtual desktop infrastructure (VDI), desktop as a service (DaaS), etc.,.
- ✓ However, these technologies cannot provide requisite IAM controls and must be complemented by authentication and/or access management tools.
- ✓ Remote access increases the attack surface — everything is on the internet! — and organizations must implement additional mitigating controls to contain this risk.

57%

Enhanced work-from-home related infrastructure.

47%

Increased use of cloud-based applications.

45%

Increased attention to endpoint security.

37%

Streamlined on-boarding and transitioning of users, devices and services

29%

Alignment between IAM and business continuity management.

28%

High level of Data Security concerns.

13%

Robust integration amongst workforce and/or non-human resources

Key Factors for IAM Planning

Increasing importance of strong authentication and safely enabling remote access.

Continued movement away from private data centers to cloud-hosted technology and IAM services.

Requirement to provide more digital services via more channels with even better user experience.

Need for more integrated and automated approaches to governance and monitoring to cope with growing IAM complexity and cyber threats.

Growing importance of managing identities, not only for people, also containers, agents, keys, secrets & smart things

Hybrid cloud and multi-cloud will continue to transform infrastructure IAM best practices.

Need to standardize IAM support for an ever-widening set of technologies with zero trust, where users must explicitly be granted access to each application

Involvement of IAM in Security Initiatives and decisions

IAM – Focused Areas

IAM Demands….

Predictive Identity Analysis (AI) - AI Driven Identity governance

Access controls can be enforced based on user behavioral analysis with AI.

Identity Proofing & Threat Intelligence

Identity proofing can be achieved using advanced analytics and threat profiling .

Policy driven compliance and Regulation Automation

LCM automation helps regulatory compliance and safeguard assets adequately.

THANK YOU

Senthilkumar
Information Security Professional