

## Identity – Governance and Lifecycle

The "Who", "Why" and "What" rationale and how it different from authentication and SSO

# Why do we need to manage it – The Identity

Do we have some risk in not properly addressing Identity?



#### IDENTITY RISK CHANGING DYNAMICS



Islands of Identity; No Visibility



BYOD, Mobile, Always-on Access



Need to Balance Security with **User Convenience** 



Access for Any User, Anywhere, on Any Device



Increasing Regulatory and Compliance Scrutiny



Proliferating On-Premises & Cloud Apps & Data



Password Protection **Getting Harder** 



Privileged Access; Crown Jewels



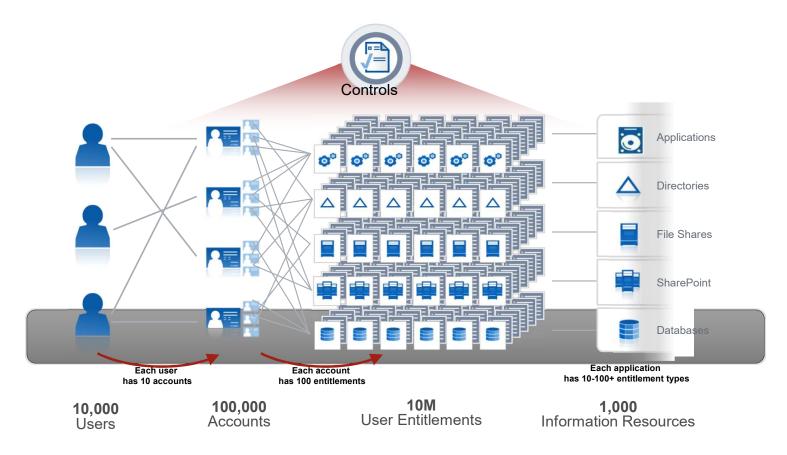
Lacking Business Reviews; Rubber Stamp



Expanding populations; 3 party access



#### Scale of the Problem





## **Seemingly Simple Questions**



Who has access to what, and how did they receive it?



Which applications are users accessing? Is there appropriate security and control of how they authenticate? Where do these applications run?



How confident are you that people are granted only appropriate access to application and data resources?



How well can you measure your compliance with internal and external security guidelines?

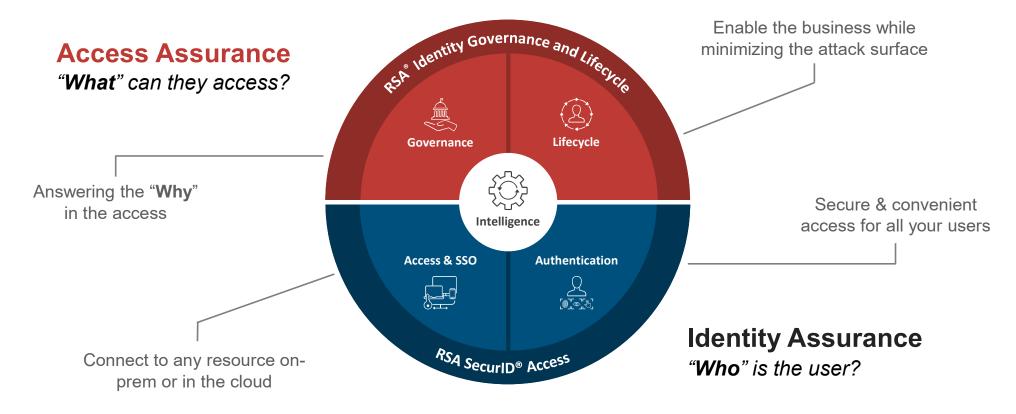


How much time and effort do you spend provisioning user access?



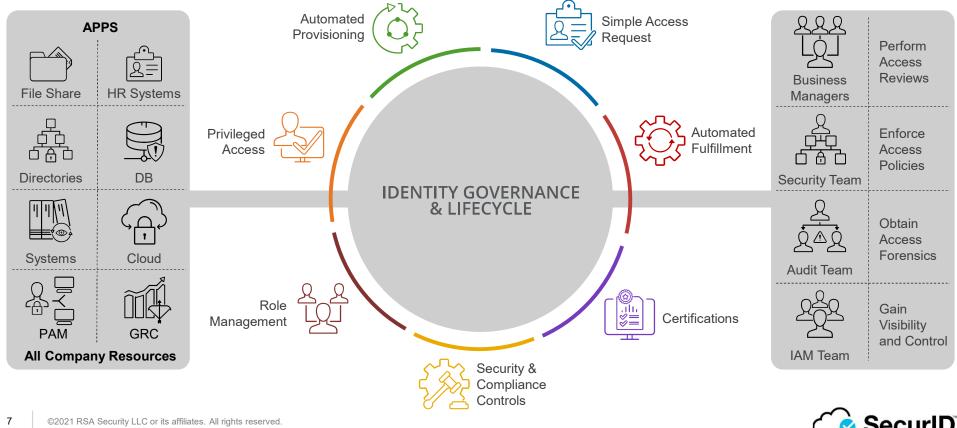
#### **IDENTITY INSIGHTS: THE WHO WHAT & WHY OF ACCESS**

ACCELERATE BUSINESS WHILE MITIGATING IDENTITY RISK

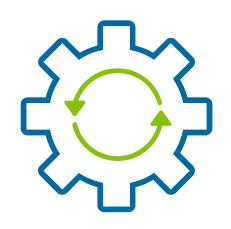




## DISCOVERY SURFACING INFORMATION & AUTOMATION



## Then Implement a risk-driven strategy to manage



#### Enable risk and context-driven governance

Understand business impact of application risk, privileged identities, shared accounts

#### Discover outliers, inappropriate access

Act on unauthorized change detection, out-of-role entitlements, segregation of duties, orphan accounts

#### Surface meaningful information for decisions

Reduce fatigue by organizing activities by risk, priority and context

#### Automate processes

Process orchestration for JML, Rules, Birthright Access

CONFIDENTIAL



## Understanding & address the Critical identity Risk Factors

CONFIDENTIAL

- Orphaned accounts
- Privileged access
- **Outliers** 
  - Unauthorized changes
- Changes as a result of movement

- High risk applications
- Unstructured data
- Un-reviewed items
- Shared and service accounts
- Toxic combinations Segregation of Duties & policy violations



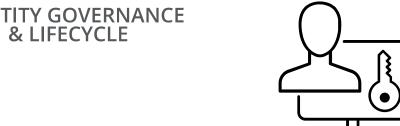
# Enable risk and context-driven governance with RSA® Identity Governance & Lifecycle









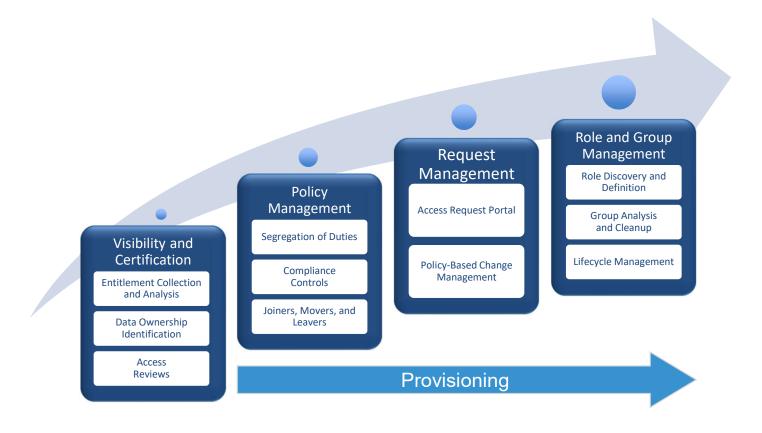


**Data Access Governance** 



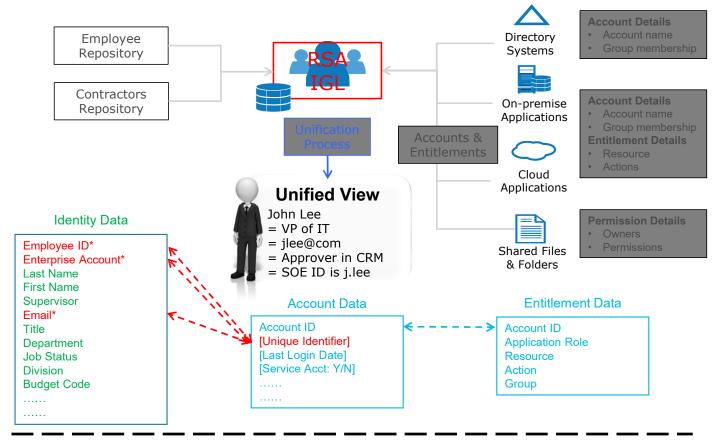


## How do we get there?





#### Visibility



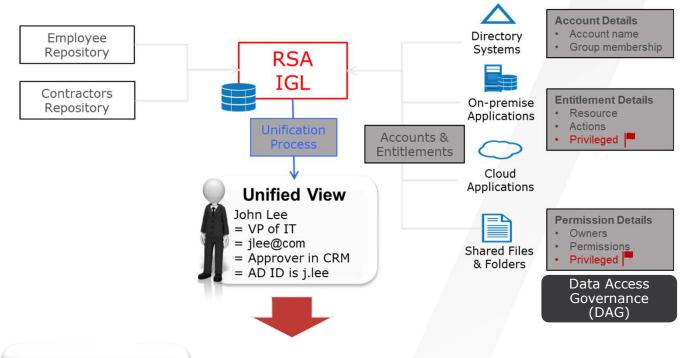
#### **External Data**

- · Business Descriptions
- Values for Custom Attributes
- Orphan Mappings

CONFIDENTIAL



## Policy & Certification

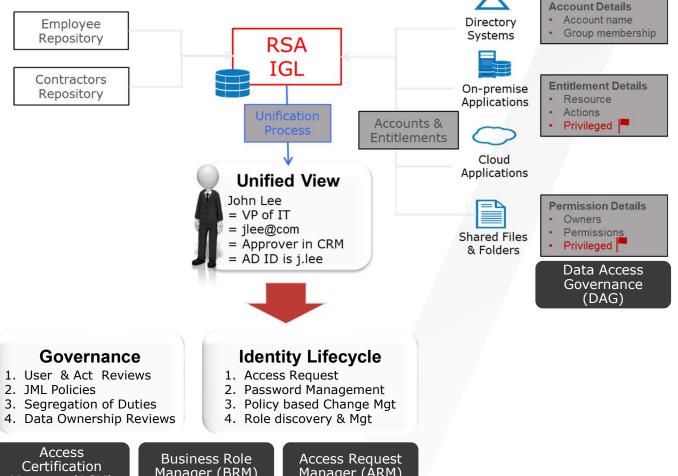


#### Governance

- 1. User & Act Reviews
- 2. JML Policies
- 3. Segregation of Duties
- 4. Data Ownership Reviews

Access Certification Manager (ACM)

#### Role and Request Management

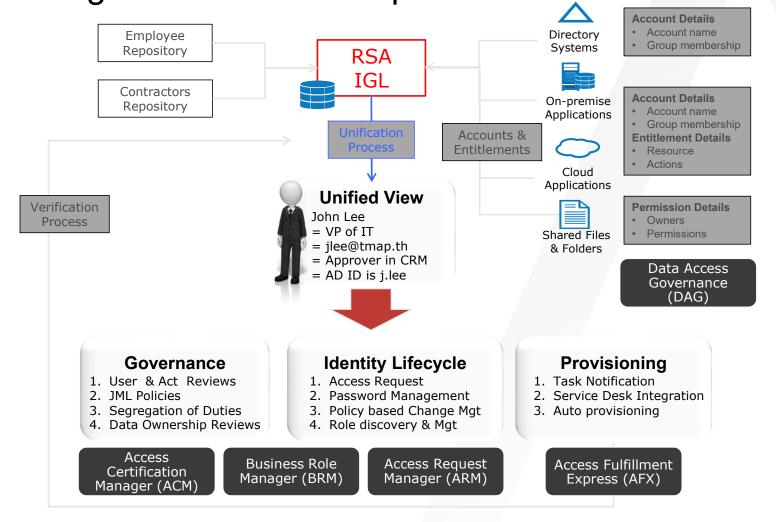


Manager (ACM)

Manager (BRM)

Manager (ARM)

Provisioning and Closed – Loop Validation



**RSA** 

# WHY DO WE NEED THE STAGGERED APPROACH

#### THE APPROACH LEADS TO

Architectural Superiority

- Intelligent Enterprise Data Model for IAM\*
- Scalability and Performance\*
- Separation of business logic and Integration logic

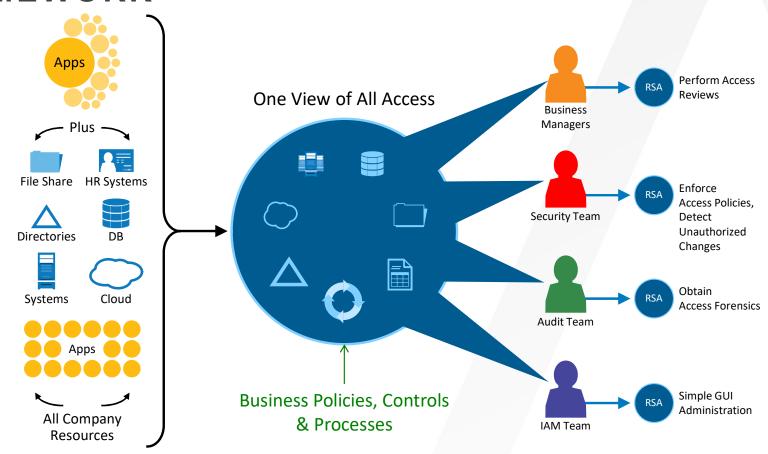
Lowest TCO and Fastest Time-To-Value

- Configuration vs. Customization
- Business-Logic Driven not IT-provisioning Driven
- Unified management of on-premise and cloud

Completeness of Solution

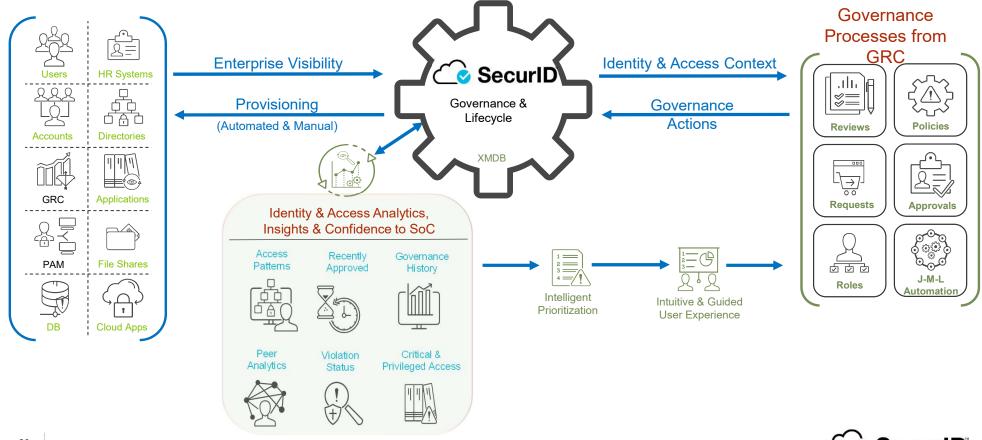
- Integrated IAM Platform for Governance, Provisioning, and SSO
- All Apps, Data, Users, and Devices
- Manage Complete Business Identity Lifecycle
- Security Integration Model SIEM, Data Access Governance

# BUSINESS DRIVEN IDENTITY GOVERNANCE FRAMEWORK



### Closing the Access Risk Gap

#### THROUGH AUTOMATION, VISIBILITY AND IDENTITY ANALYTICS







## SecurID®

Governance & Lifecycle

- Multiple options to meet customer requirements and infrastructure
- Ground-to-Cloud models

#### **DEPLOY YOUR WAY**



ON PREM



HYBRID



CLOUD



HOSTED/MANAGED

- H/W Appliance
- S/W Only
- S/W Bundle
- Virtualized Application
- Docker Container
- On Premise/Cloud blended deployment
- AWS Deployment
- Azure Deployment
- RSA Direct
- Strategic Partners:
  - Capgemini
  - HCL



#### FLEXIBLE DEPLOYMENT OPTIONS FOR ANY ENVIRONMENT



#### SOLUTION COVERAGE BY RSA FOR RBI

#### Collection Methodology

Custom Schema for collected applications

Diversity of collection mechanism

Ability to collect application metadata

Collection of fine-

Data Validation and rules processing

Normalization of dentity & entitlement

OOB Supported
Applications for

#### Reviews & Certification

Reviews of accounts, groups entitlements &

Dynamic Change /event based Certification

> Change Management / Remediation

Detailed review certification reports

Diversity of Basis of certification

End-to-end Traceability for Audit

#### Access request & Workflows

Self service with restricted visibility

Rule Based Acces request

Workflow based
Exception
Management

Graphical Workflow configuration

Reassignment & escalation capabilities

Automated SLA Management

Multiple changes with single workflow

#### Business Policies

Ability to create compliance policy based on regulatory requirements

Automatically scan and detect policy violations

Notify violations during the request process based on

Compliance based reports

Criticality integration with Risk management tools

Ability to provide automated reports for metrics

Multiple options for addressing policy violations

#### Password Management

Reset passwords in one or more system simultaneously

Ability to set a max threshold for unsuccessful logins

Challenge/Response for both enrollments as well as for self-

Allow specification of password strength requirements

Secure viewing of new passwords generated

Allow users to reset their passwords external to the system

New users to receive their usernames and passwords external to the system

#### Unstructured Data

Streamline compliance policies both in data and application entitlements

Normalize collected Data

Gain Unified view of application and data entitlements

Allow access request to data resources

Organize classifications of data within sources

Establish ownershi across data resources

Collect data from unstructured sources

#### Provisioning

Closed loop provisioning architecture.

Diversity of collection mechanism

Should allow automated J/M processes that match existing user entitlements

Should support terminations and leaves of absence

Ability to send a group of changes

All provisioning activities recorded for audit purposes with full audit trail

Manage the complete user account lifecycle

#### Use Cases & Integrations

Complete Access

Complete Vendor
Access Lifecycle

Business roles simulation and standardization

Integration With SIEM Systems

Integration With GRC Systems

Integration with DLP Systems



