



# Identity Risk l'importanza di un approccio integrato per la gestione e mitigazione dei rischi

Pasquale Russo - Senior System Engineer, RSA

Luciano Veronese - Advisory Sales Consultant RSA

# AGENDA

- The Identity Risk
- RSA Archer GRC Suite
- RSA SecurID® Suite
- Conclusion

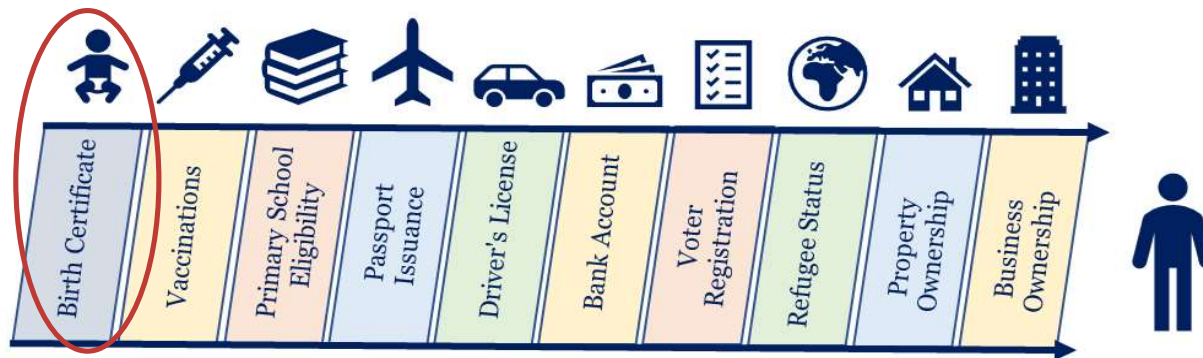
# The Identity Risk

©2020 RSA Security LLC or its affiliates.  
All rights reserved.

**RSA**

# The scenario

Today, Digital Identities are used everywhere and associated to everyone and everything

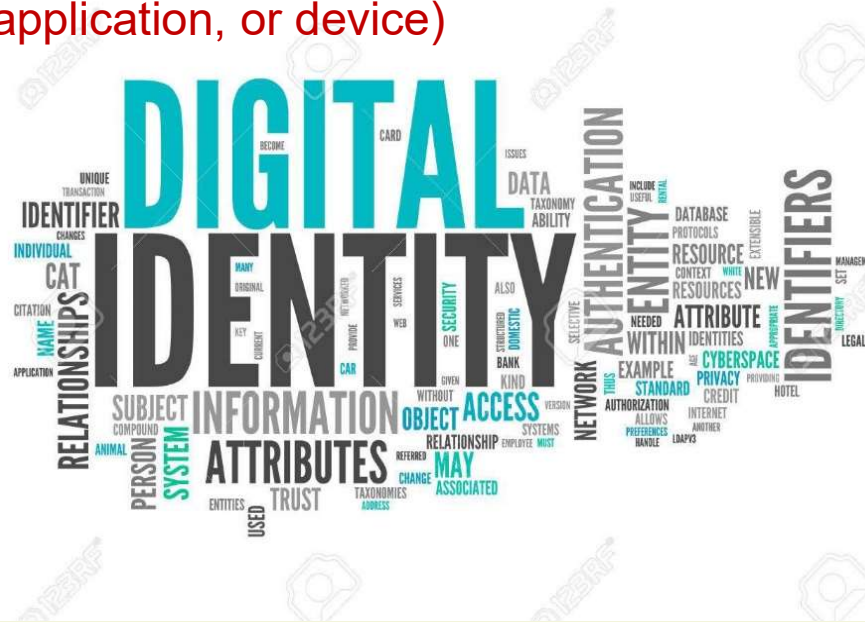


*The more they are used, the more they become a complex and interconnected ecosystem of relationships!*

# What do we mean by “digital identity”?

Information on an entity used by computer systems to represent an external agent (person, organization, application, or device)

ISO/IEC 24760-1 defines identity as "set of attributes related to an entity".



Information contained in a digital identity **allows for assessment and authentication** of a user interacting with a business system on the web to access digital services

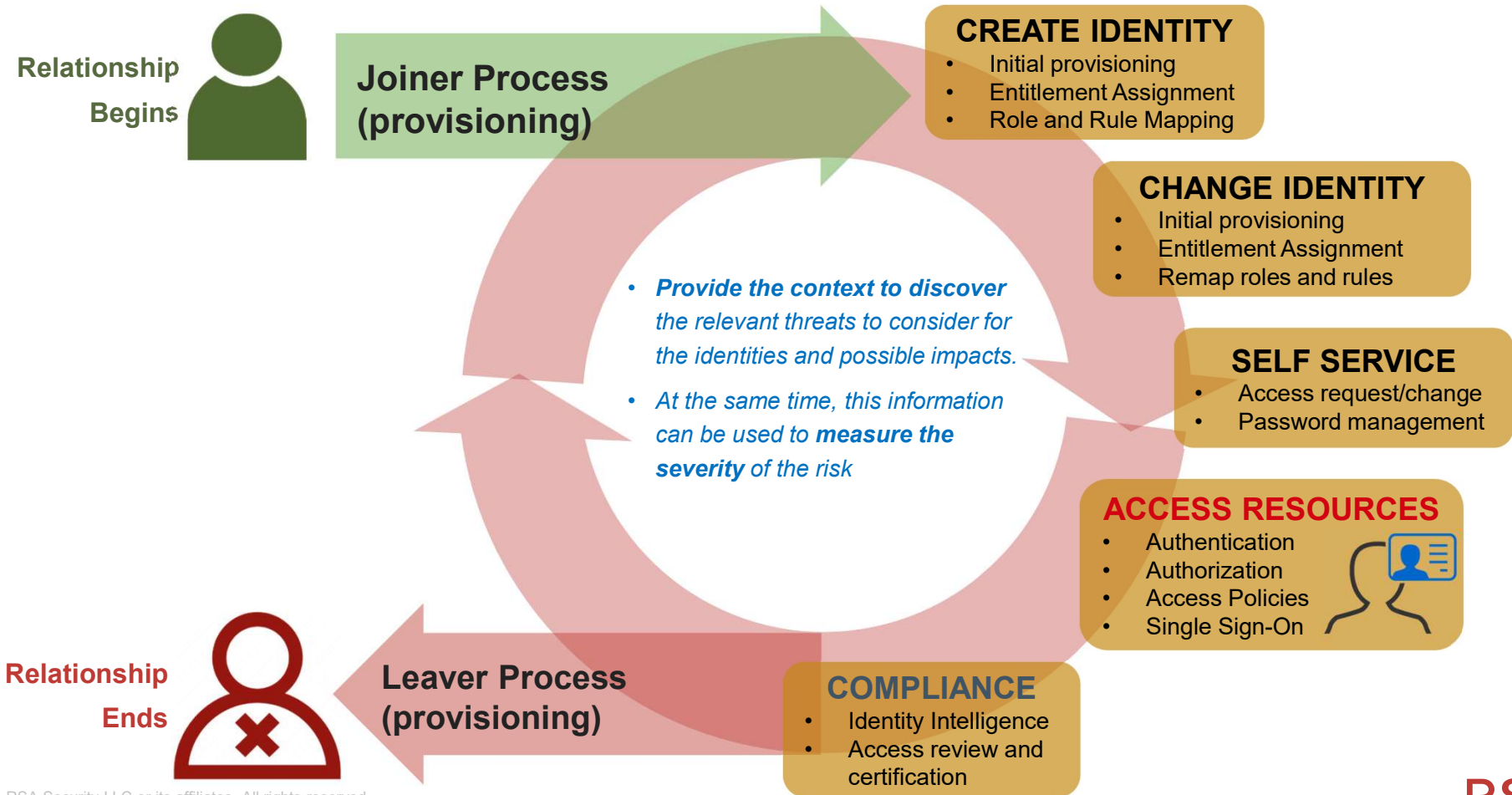
For organizations, Digital Identities are huge assets, as they allow external agents to access the critical digital services of the organization!

➤ As such, identities are a **key target** for some (**threat**) communities of agents



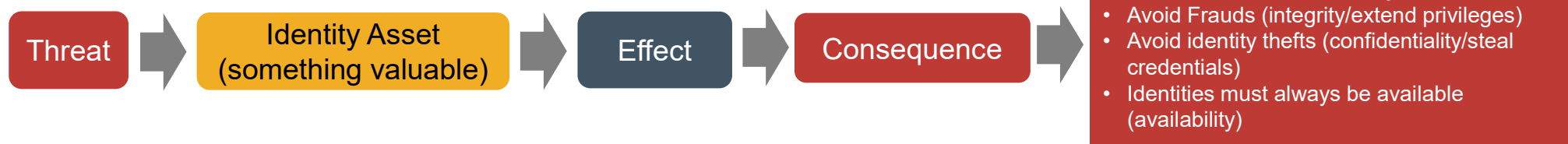
# How are digital identities used?

## The Identity lifecycle



# Risks in using identities

In general, the **concept of risk** is about something that happens (event) over an asset, causing an effect and leading to a consequence that can impact the business objectives:



**Example:** a cyber criminal community (threat) causes a data breach (effect) of personal information (asset) leading to a fine (consequence) that impact the company market share (business impact)

A **shared definition of "identity risk"** does not currently exist, but similarly to other risk categories, some definitions are possible:

- The risk associated to the usage of digital identities (very high level...)
- The effect of misuse(\*) of identity information in using a digital service
- Unwanted outcome (CIA impact) that stems from an unexpected use of identity information

(\*) "misuse" means "unwanted" or "unexpected" and this can be about both a malicious or unintentional behavior.

# Identities in organizations

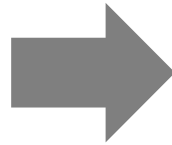
- Every organization can be split into the technology (security) domain and business domain
  - Technology domain typically manages the identities
  - Business domain typically consumes the identities
- This implies that to address Identity Risk we need to consider both technology and business contexts





# Mitigating Identity Risk...

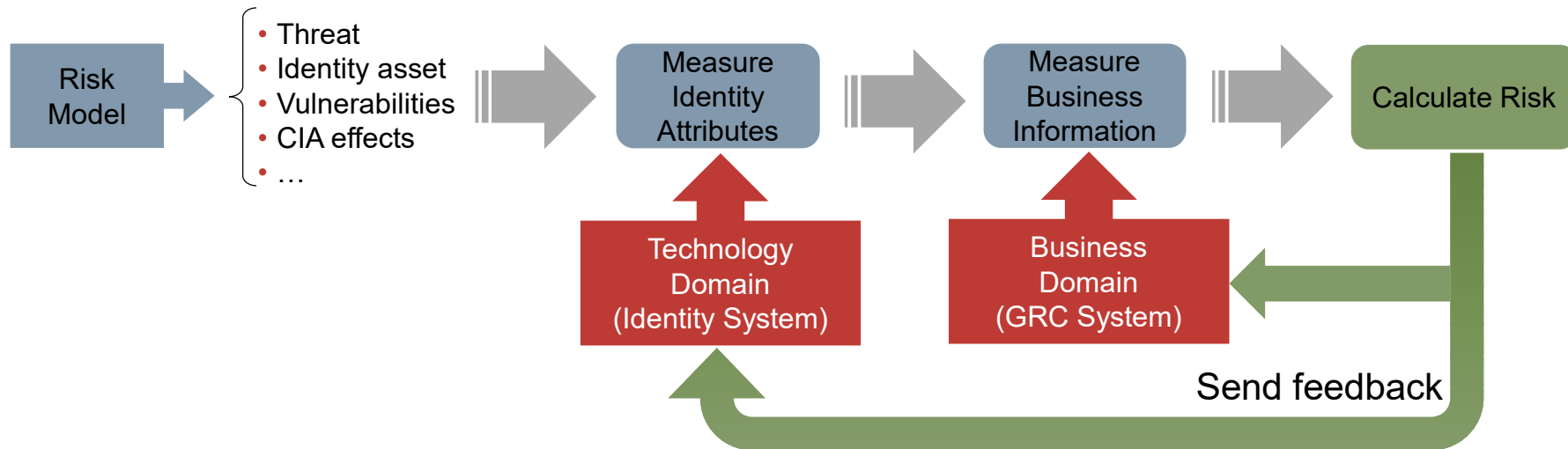
GOAL:  
Minimize  
Identity Risk



- **ASSESS** Identity Risks
  - Identify most relevant scenarios (potential risks)
  - Measure them using a model
  - Compare against thresholds
- Take **ACTIONS** to reduce risks

**What if all of this could be achieved automatically?**

# Mitigating Identity Risk... leveraging on automation!

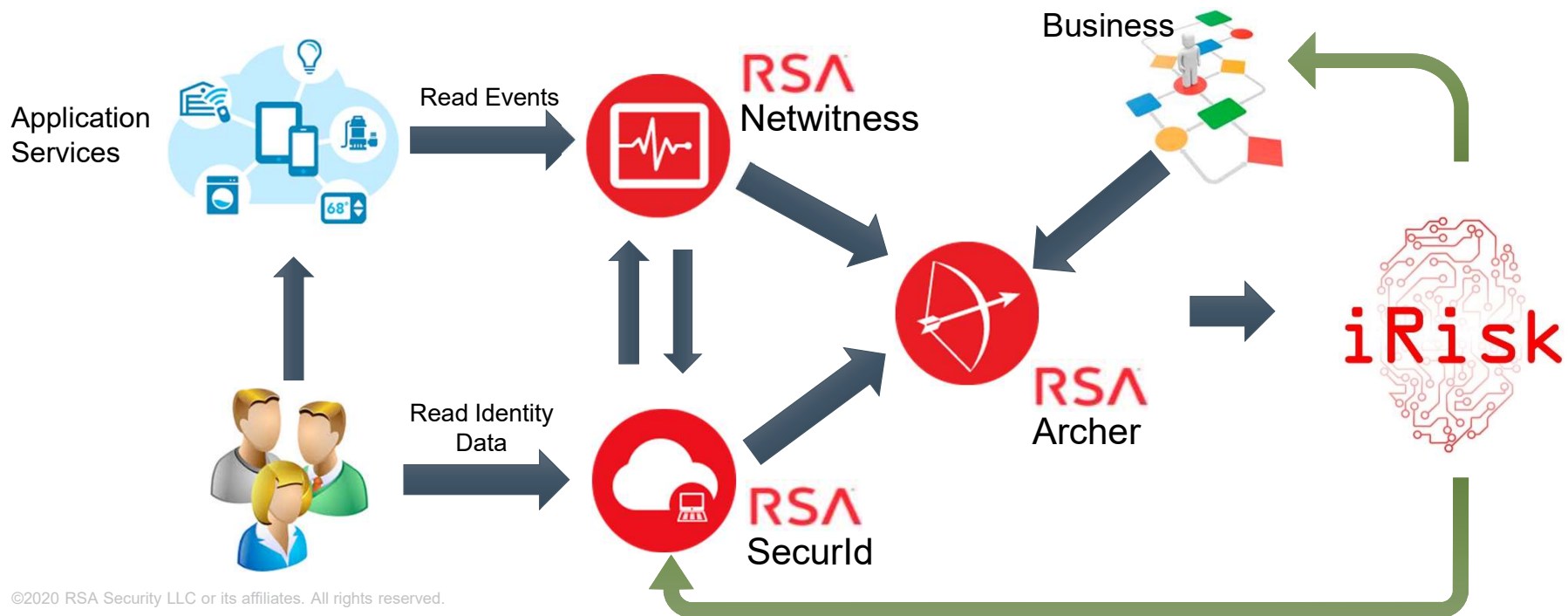


# Integration is key

Identity (e.g. policy violations) and business (e.g. process criticality) attributes can be gathered from an IAM and GRC system respectively

- Typically these systems are organized as silos
- To achieve our objectives, integration is key: this is what you can achieve with the RSA products

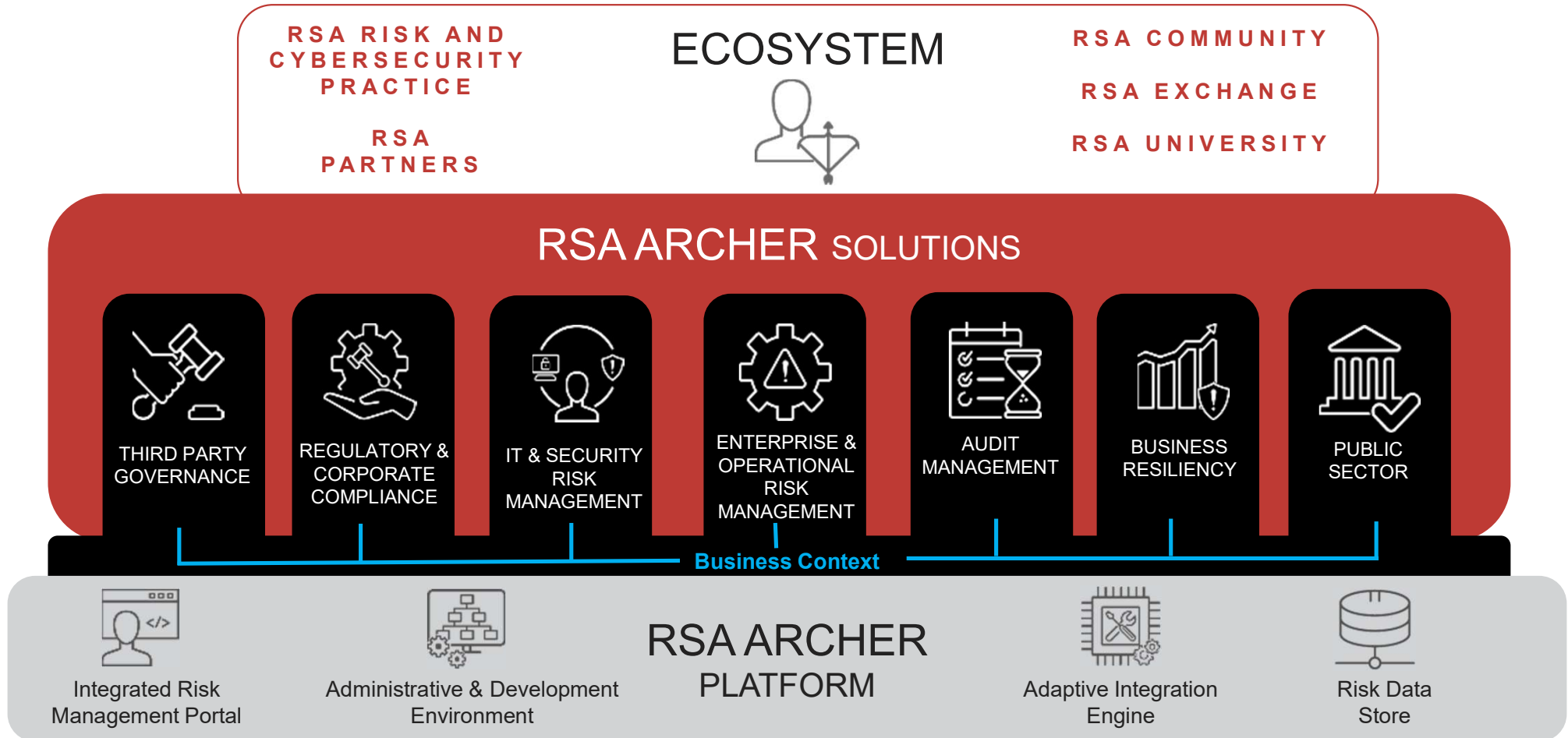
## **RSA SecurId and RSA Archer GRC Suite**



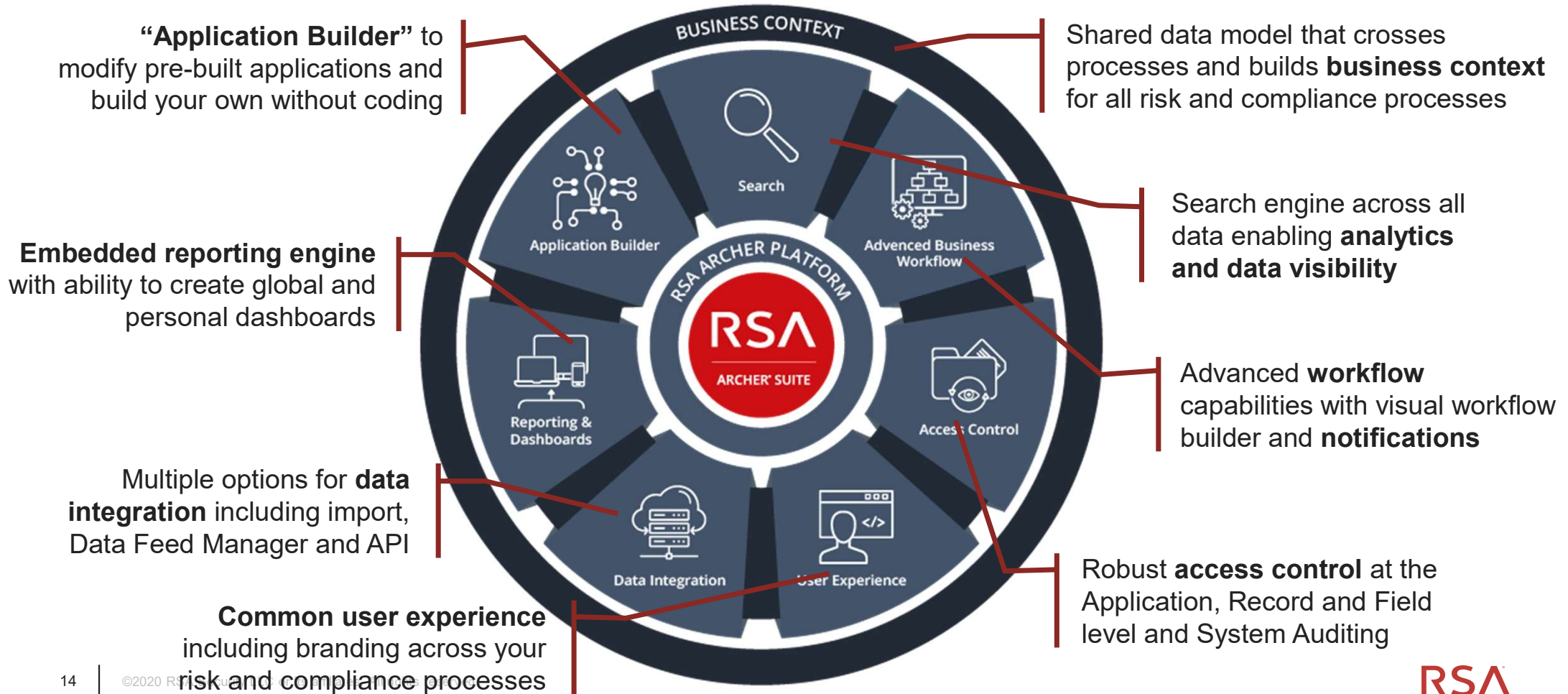
# RSA Archer<sup>®</sup> Suite

A leader in the Governance Risk and Compliance solutions

# Introducing The RSA Archer Suite



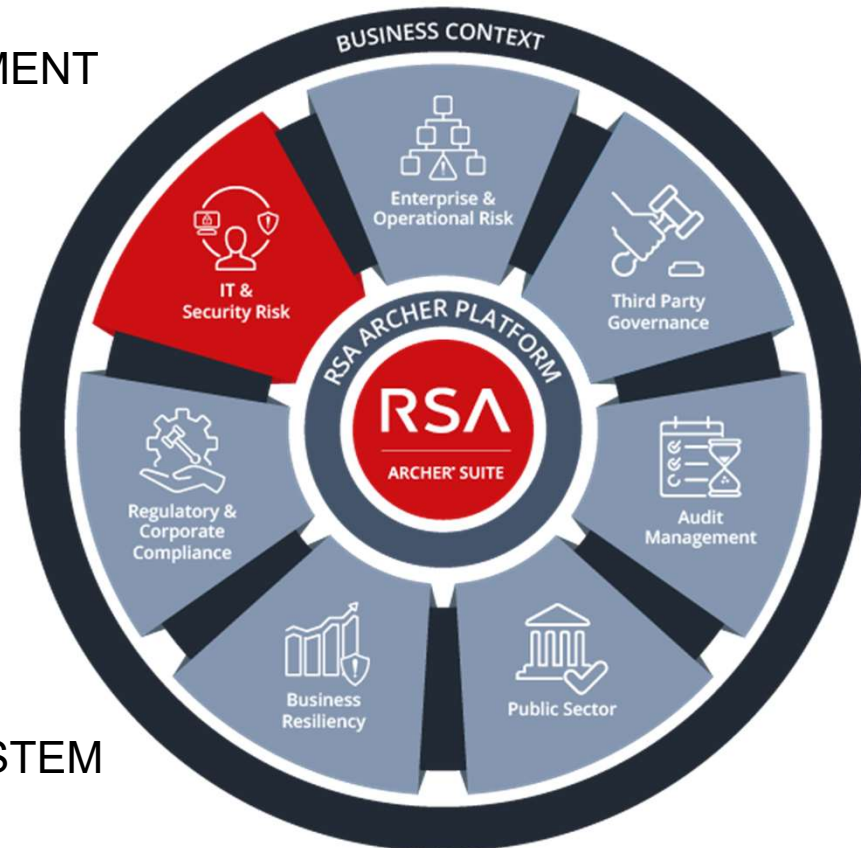
# Key Features of the RSA Archer Platform





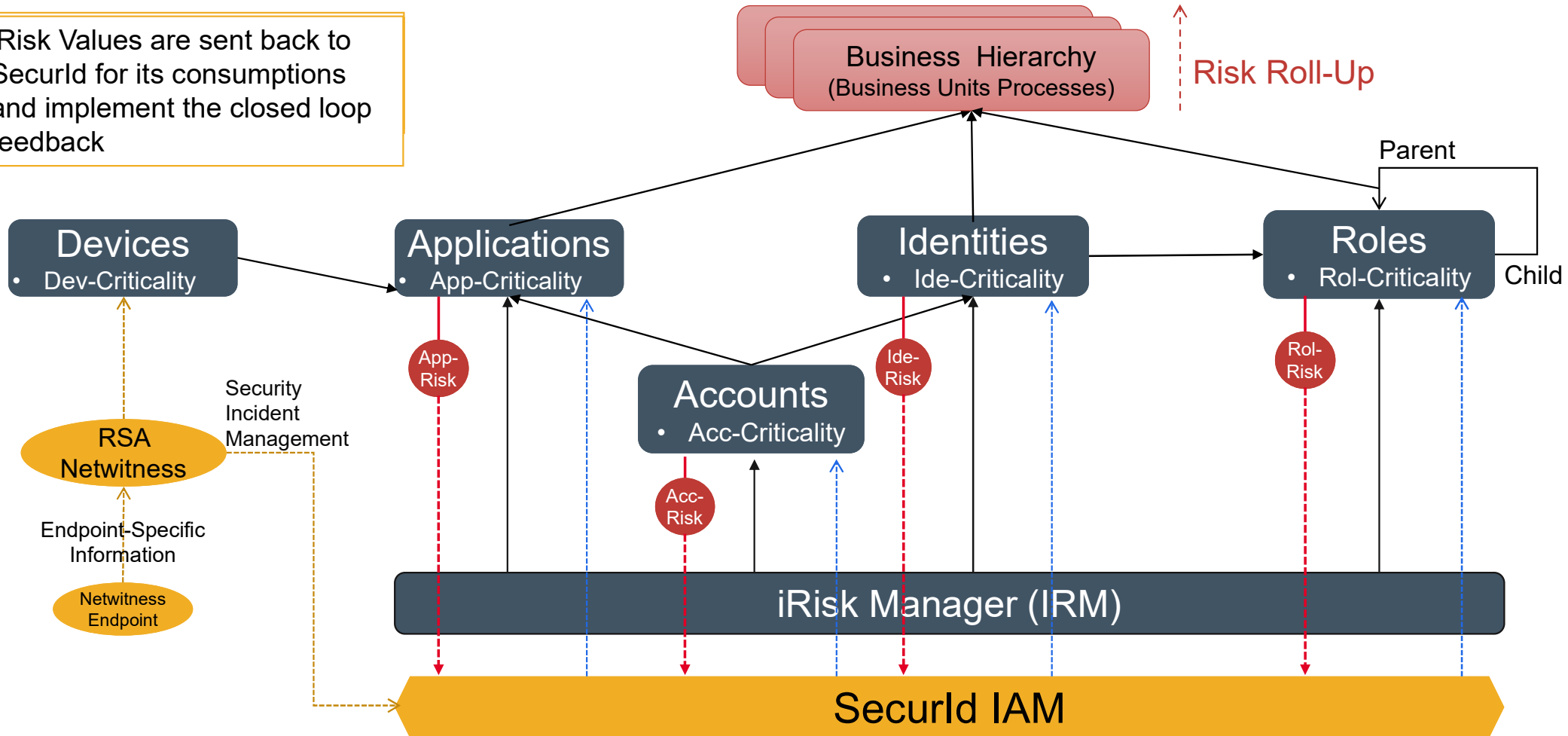
# Modular and Progressive Approach: Archer Use Cases

- IT & SECURITY POLICY PROGRAM MANAGEMENT
- IT RISK MANAGEMENT
- IT SECURITY VULNERABILITIES PROGRAM
- CYBER INCIDENT & BREACH RESPONSE
- CYBER RISK QUANTIFICATION
- IT CONTROLS ASSURANCE
- IT REGULATORY MANAGEMENT
- PCI MANAGEMENT
- INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)




# Modular and Progressive Approach: Archer Use Cases

iRisk Values are sent back to SecurId for its consumptions and implement the closed loop feedback



# Identity Risk Management Dashboard

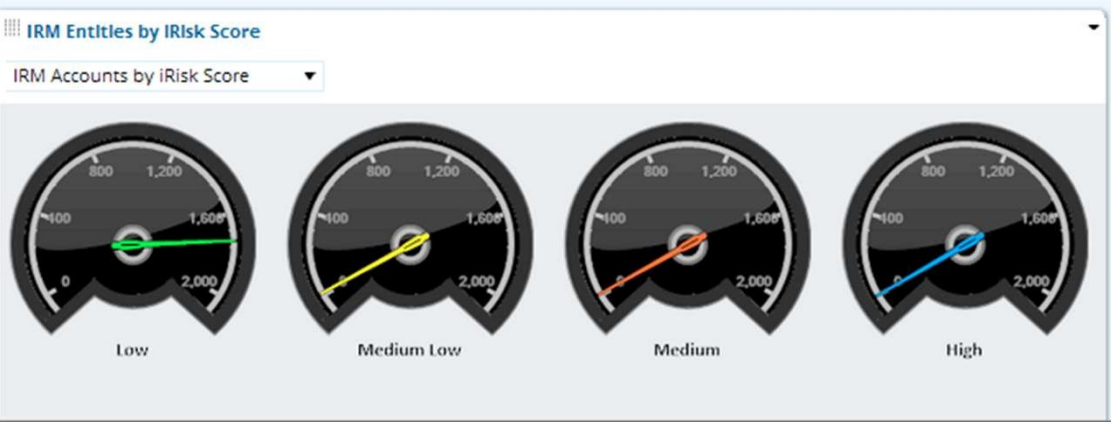
IRM



**Welcome to the Archer iRisk Management Solution**  
*Calculate and merge the identity risk into the business risk*

IRisk Scores and Indicators Summary

System Name	Account iRisk Score	Account iRisk Indicator	Application iRisk Score	Application iRisk Indicator	Identity iRisk Score	Identity iRisk Indicator	Role iRisk Score	Role iRisk Indicator
Risk Manager								



IRM Heat Maps

IRM-Account Risk Heat Map

Acc-Risk Score	High	Medium High	Medium	Medium Low	Low
High					1
Medium High					3
Medium		5			1
Medium Low		11	1		1
Low		1728	1		2
Not Evaluated					
(No Selection)					

# RSA SecurID® Suite

Modernize Secure Access

©2020 RSA Security LLC or its affiliates.  
All rights reserved.

**RSA**



# RSA SecurID SUITE

RSA SecurID Suite enables organizations of all sizes to **mitigate identity risk** and maintain compliance without impeding user productivity. It ensures users have appropriate access and confirms they are who they say they are with a **modern, convenient user experience**

RSA SecurID Suite provides unified visibility and control across organizations' many islands of identity.



**RSA**  
Identity Governance  
&  
Lifecycle



**RSA**  
SecurID

# RSA

## Permissions Before and after Covid

- User Creation
- Badge: activation
- Access to the Corporate
- Asset Supply
- Access to the applications:
  - Profiling
  - Policy
  - etc..

- Badge: deactivation
- VPN access request
- Out-of-Office / Sickness
- Request access to specific applications (never been accessed)
- Remote Worker Profile
- Change Office Address to home

RSA



# Adopting **RSA** as Identity Solution



**RSA**

Identity Governance  
&  
Lifecycle

- GOVERNANCE OF THE IDENTITIES
- ACCESS TO WHAT I NEED
- DIFFERENT IDENTITIES
- RISK MITIGATION

**GIVE TO THE USERS A FACE**

**You Can't  
protect  
what you  
don't know  
you've got**

**RSA**



## VISIBILITY AND GOVERNANCE

WHO CAN ACCESS?

WHO CAN DO

HAS AN ACCOUNT BEEN REMOVED?

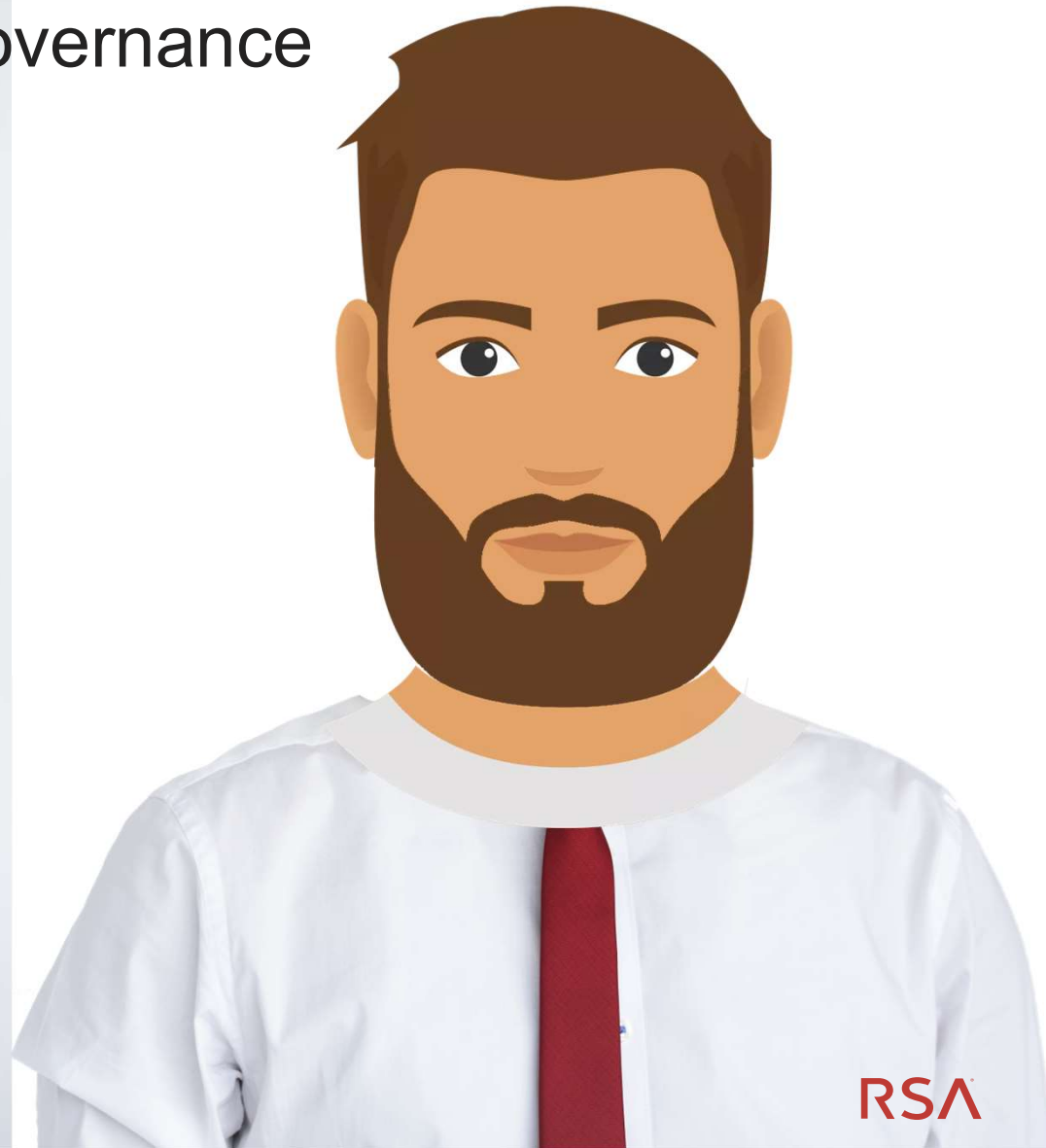
DO WHAT?

ARE WE IN COMPLIANCE?

# A phased approach: Identity Governance

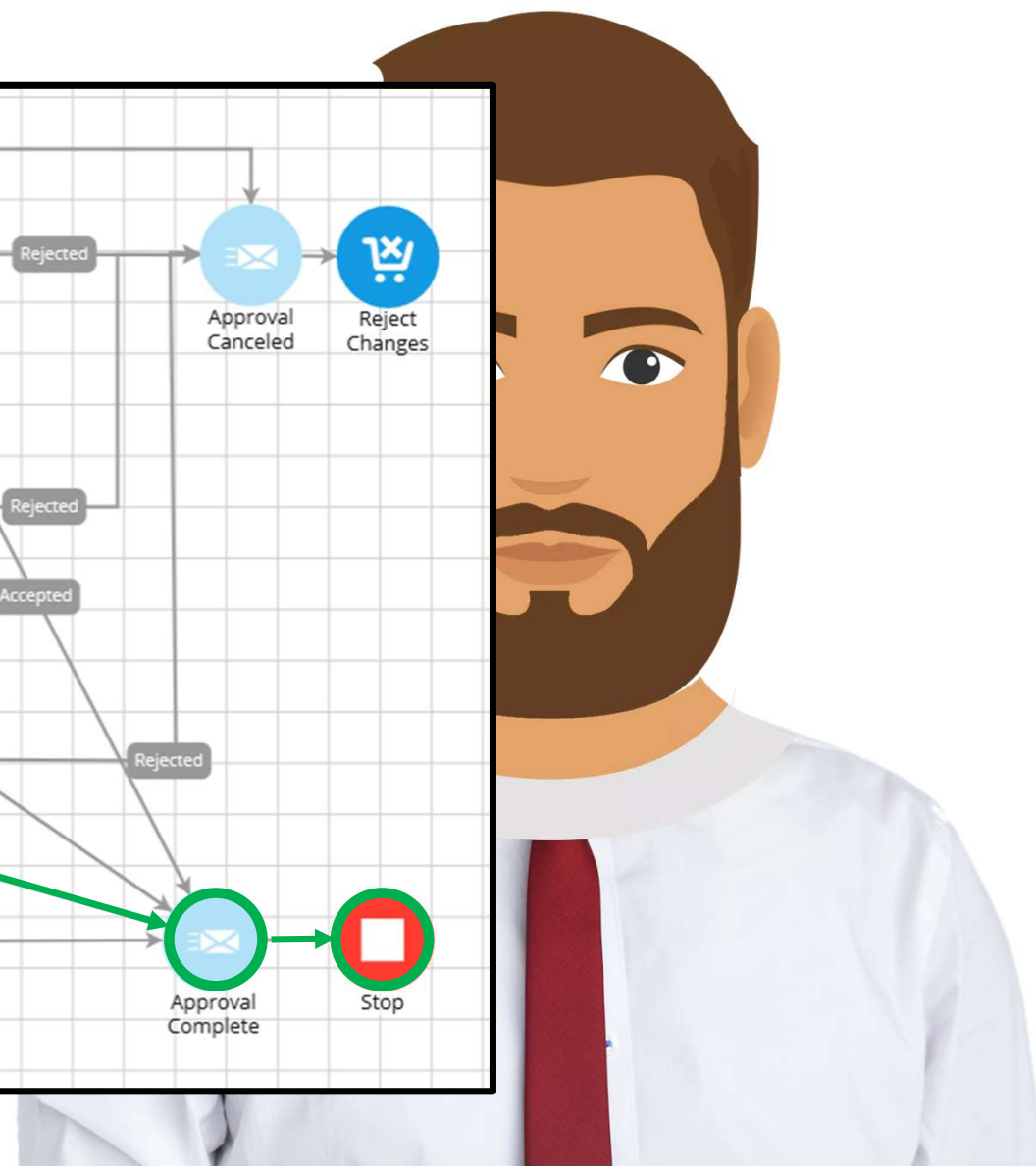
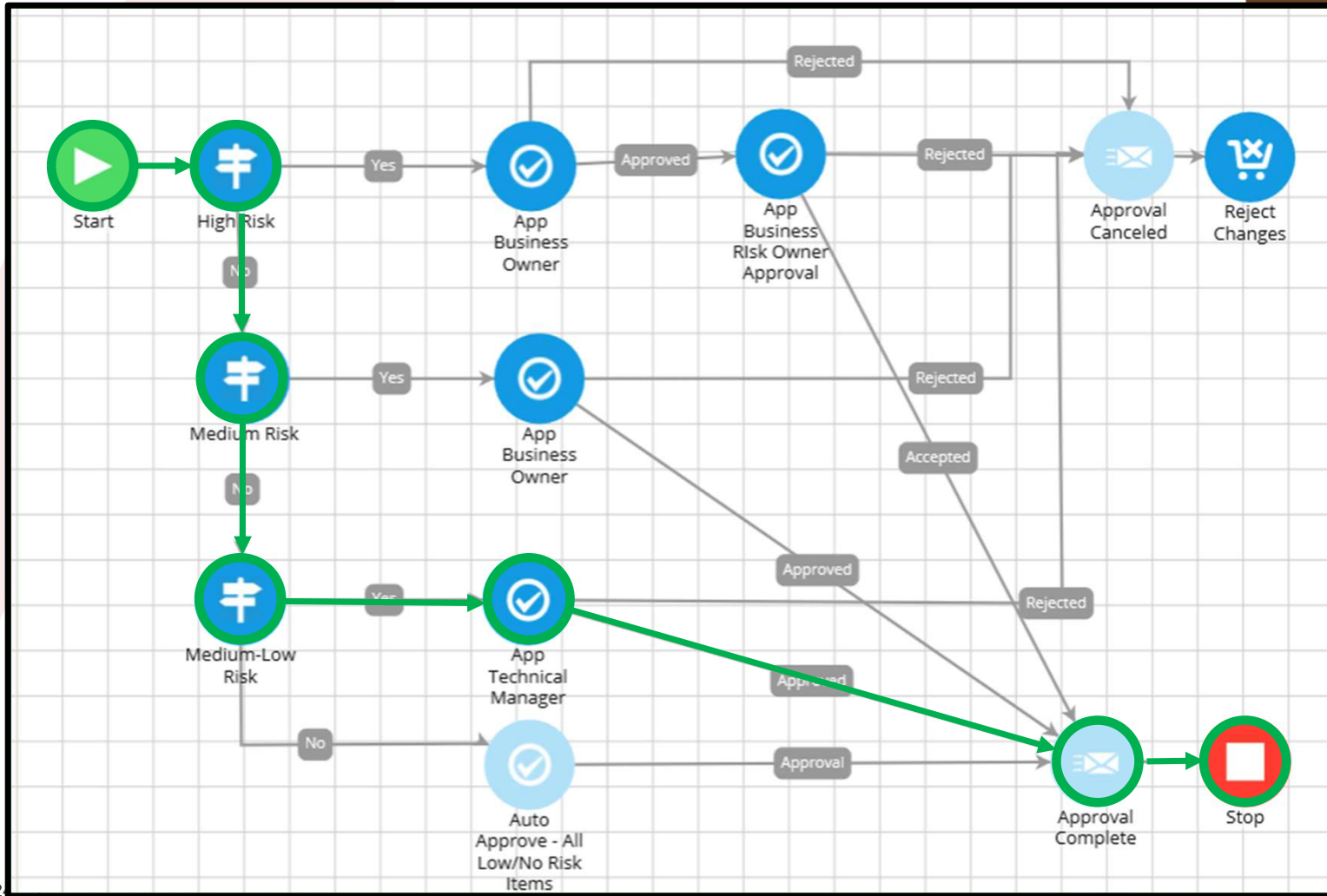


**RSA**  
Identity  
Governance  
&  
Lyfecycle



**RSA**

# Workflow: handle the RISK



# Adopting **RSA** as Strong Authentication

## Modern MFA Methods

Easy & convenient

- Push
- Mobile OTP
- Biometrics
- Text Msg
- Voice Call
- HW Token
- SW Token
- FIDO
- Proximity
- Wearables

## Risk-based Authentication

Access in context

MACHINE LEARNING

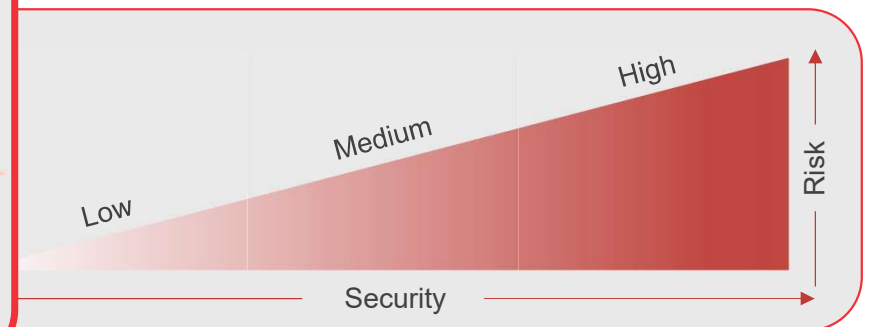
RISK

PASS RISKY DENY

Role Device Location Behavior App

**RSA**  
READY

Microsoft SONICWALL® CITRIX®  
 CYBERARK® salesforce CISCO  
 amazon web services paloalto NETWORKS servicenow  
 Many others... workday. vmware®



## Pervasive MFA

Certified and supported

## Assurance Levels

Challenge according to the level of risk

# Granular policies to manage **any situation**

## Identity Confidence

Rule Set Name  
Allow All Authenticated Users

Target Population

Apply to ?  
All Users Selected Users

Access Details

Access ?  
Allowed Denied

Authentication Details

Additional Authentication ?  
Required Conditional Not Required

Matching conditions determine the action to take. Conditions are evaluated in the order listed. Drag and drop to reorder the conditions. *No matching condition* is always last.

Condition	Action	Assurance Level
Identity Confidence is high	Allow Access	
Identity Confidence is low	Authenticate	Medium
No matching condition	Deny Access	

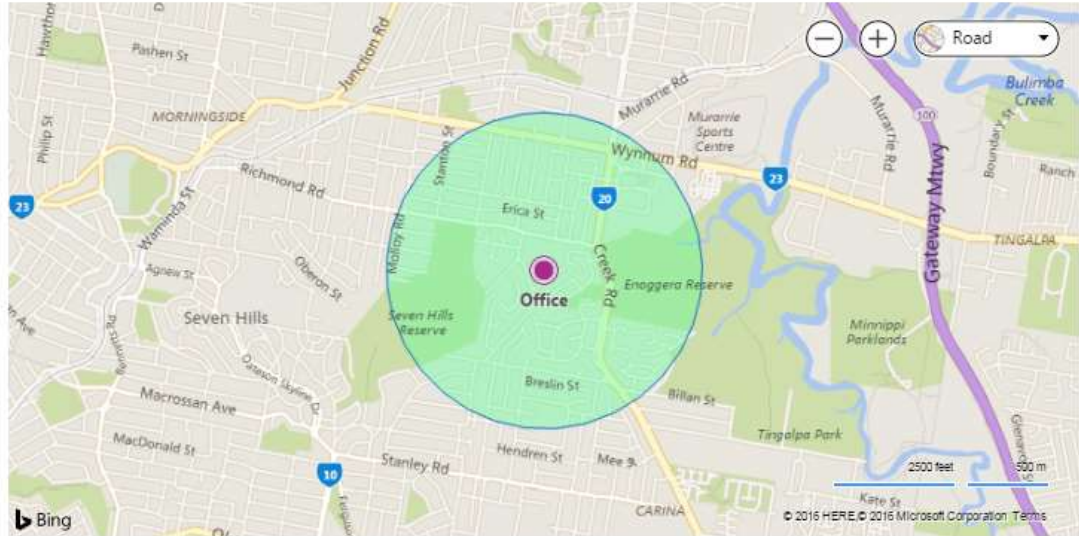
ADD

## Trusted Location

Trusted Location Name ?  
Office

Address ?  
5 Beardsley Pl, Brisbane, Queensland, Australia

Radius ?  
1 Kilometers





# User Attribute-based authentication

DEPARTMENT

LOCATION

TITLE

LAST LOGIN

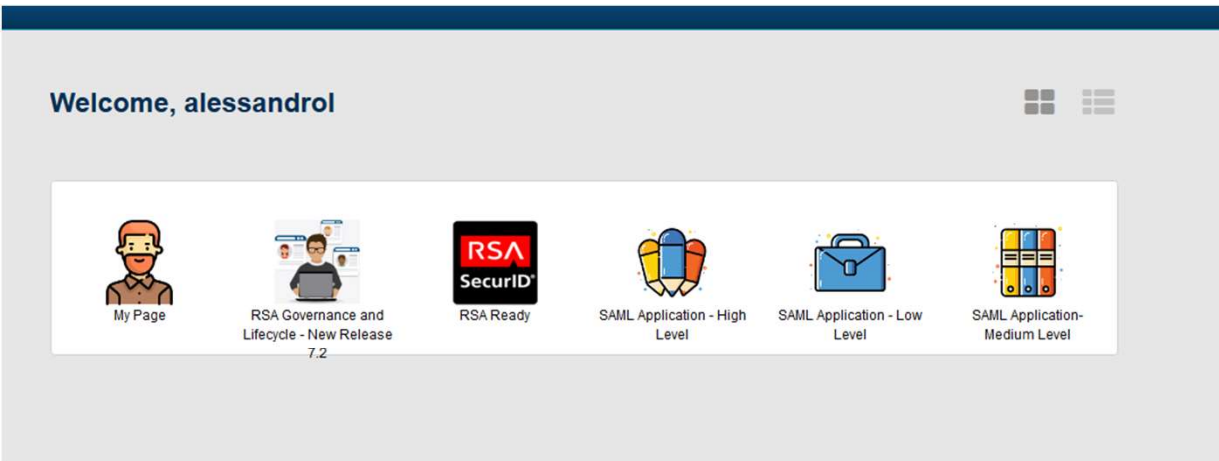
SUPERVISOR

ENROLLED?



RSA

# SSO Portal and Users Enrollment: **An Easy Way!**



RSA SECURID<sup>®</sup> ACCESS My Page

Sign Out

RSA SECURID<sup>®</sup> ACCESS My Page

Sign Ou

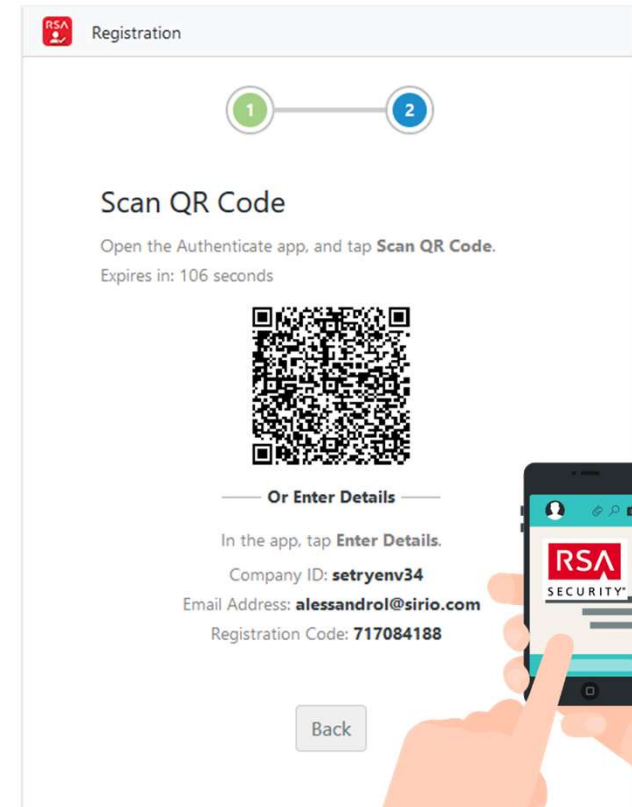
Welcome, Alessandro

Registered Authenticators

 iPhone di Pasquale	IOS 13.4.1	Registered: 2020-04-30	
 alessandrol's Security key 1	Security key	Registered: 2020-04-30	

Select an authenticator

Get Started



Alert: increase the Identity Assurance



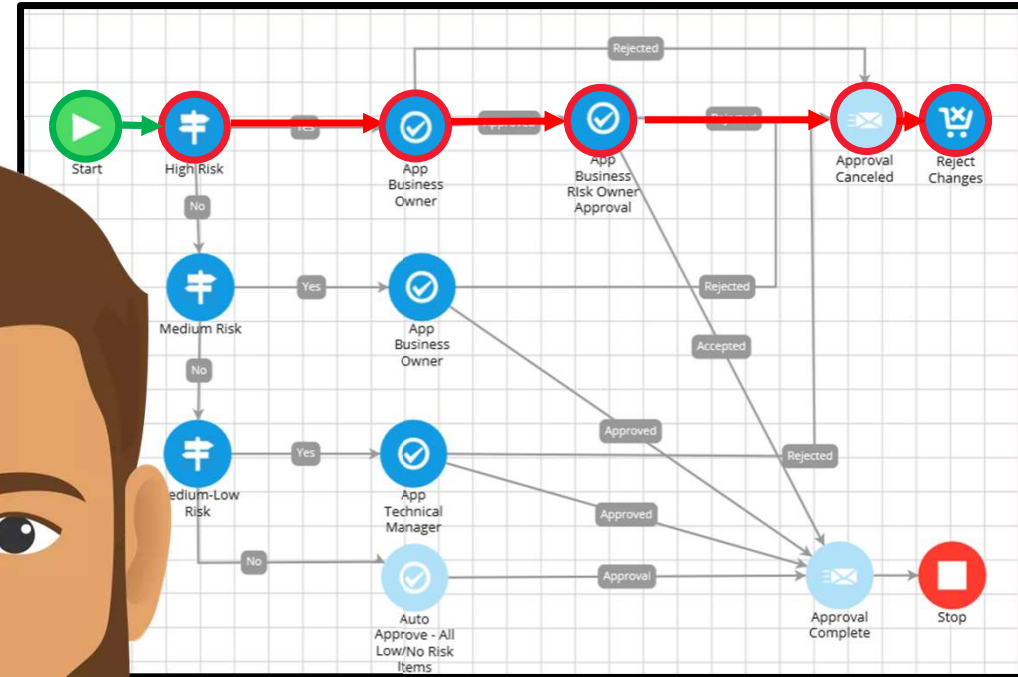
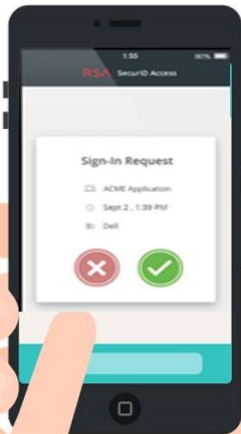
**ALERT!**



# An immediate reaction to an Identity Risk



**EMERGENCY  
TOKEN CODE**



# Orphan Accounts

A BACKDOOR TO YOUR ENTERPRISE

**70%** of enterprises fail to discover the privileged access accounts in their environment. ●

● never tried to find privileged accounts in their environment **40%**

**55%** fails or forgets to revoke permissions after a privileged user has been removed: **orphan account** ●





# Make it easy: Business descriptions!

Search:  🔍 ✕ +

<input type="checkbox"/>	Entitlement Name	Resource	Entitlement Collector	Entitlement Raw Name
<input type="checkbox"/>	RSPFPAR : Display profile parameter	RSPFPAR	SAP Entitlement Collector	RSPFPAR : Display profile parameter
<input type="checkbox"/>	RSPFPAR_AUTH : All authorizations	RSPFPAR_AUTH	SAP Entitlement Collector	RSPFPAR_AUTH : All authorizations



5	ApplicationRole	SAP	TRUE	SAP_ASAP_AUTHORENUMGEBUNG	Working in the ASAP Authoring Environment
7	ApplicationRole	SAP	TRUE	SAP_ASAP_AUTORENUMGEBUNG	Profile for ASAP Authoring Environment
8	ApplicationRole	SAP	TRUE	SAP_ASR_ADIMINISTRATOR	HR Administrative Services : Administrator
9	ApplicationRole	SAP	TRUE	SAP_ASR_EMPLOYEE	HR Administrative Services : Employee
0	ApplicationRole	SAP	TRUE	SAP_ASR_MANAGER	HR Administrative Services : Manager
1	ApplicationRole	SAP	TRUE	SAP_AUDITOR	AIS - Audit Information System
2	ApplicationRole	SAP	TRUE	SAP_AUDITOR_A	AIS - Central Authorizations
3	ApplicationRole	SAP	TRUE	SAP_AUDITOR_ADMIN	AIS - Administration
4	ApplicationRole	SAP	TRUE	SAP_AUDITOR_ADMIN_A	AIS - Administration (Authorizations)
5	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_A	AIS - Authorizations for SAP Applications (Except HR)
6	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_CFM	Business Audit, Treasury (Transactions)
7	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_CFM_A	Business Audit, Treasury (Authorization)
8	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_CO	AIS - Internal Activity Allocation
9	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_CO_A	AIS - Internal Activity Allocation (Authorizations)
0	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_EC_CS	AIS - Consolidation
1	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_EC_CS_A	AIS - Consolidation (Authorizations)
2	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_EC_PCA	AIS - Profit Center Accounting
3	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_EXPORT_DATA	AIS - Data Export
4	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_FI_AA	AIS - Tangible Assets
5	ApplicationRole	SAP	TRUE	SAP_AUDITOR_BA_FI_APMD_A	AIS - Accounts Payable - Master Data (Authorizations)

# Quarterly review with escalation

The screenshot displays the RSA Archer interface for a 'Payroll User Access Review-1'. The left sidebar shows various filters under 'DISPLAY VIEWS' and 'ANALYSIS & GUIDANCE'. The main area shows a list of items with columns for State, Categories, Name, Business Source, and Entitlement Name. An 'Edit Escalation' dialog box is open, showing configuration for an escalation workflow.

**DISPLAY VIEWS**

- Grouped By User
- View of Contractors Only

**ANALYSIS & GUIDANCE** [Clear Selec...](#)

**Critical**

- Violations - 0
- Exceptional Access - 0
- Expiring Soon - 0
- Previously Revoked - 0
- Critical Application Access - 0
- Privileged Application Access - 0

**General**

- Never Reviewed - 1
- Uncommon Access - 0
- Common Access - 0 [Keep](#)
- Recently Approved - 0 [Keep](#)
- Unchanged Items - 0 [Keep](#)
- Pending Revoke - 0

**HOME > MY REVIEWS > PAYROLL USER ACCESS REVIEW-1**

Payroll User Access Review-1 (Display View : Grouped By User)

For each entitlement, click the Keep button to continue granting access to the user. To set an expiration date for this grant, use the drop-down arrow to choose an expiration date. To repeal the user's access. To hide these instructions, use the toggle on the bottom right.

Take Action Showing: All (6)

State	Categories	Name	Business Source	Entitlement Name
		Greer, Terry		
		Greer, Terry		
		Lee, Harry		
		Mendez, Timothy		
		Mendez, Timothy		
		Mendez, Timothy		

Items 1 - 6 of 6

**Edit Escalation**

A workflow will run on the configured trigger date below. Based on the type of workflow selected, the workflow will apply to each reviewer with un-reviewed items when the escalation is triggered or to the entire review.

Trigger Date: 3 days after the review start date

Workflow: Reviewer Email Reminder

Reviewer: reviewers."Reviewed Percent"=0

OK Cancel ? Help

# Out-of-Office and Delegation

Home My Tasks Users Resources Requests Reviews

Return to: Home Users

User: Peterson, Dan

General Access Violations/Exceptions Requests Privileges

Set Out of Office

Default Out Of Office Form

Specify the date the Out of Office will begin and the date the user will return to office. An optional comment can also be included with the request.

Start Date\*: 03/20/2017

Return Date\*: 03/24/2017

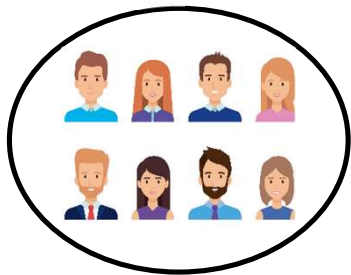
Comment: I will be out of the office on PTO, please take care of my assigned reviews and approvals during this time. Thank you.

Select Delegate: Bond, Donald

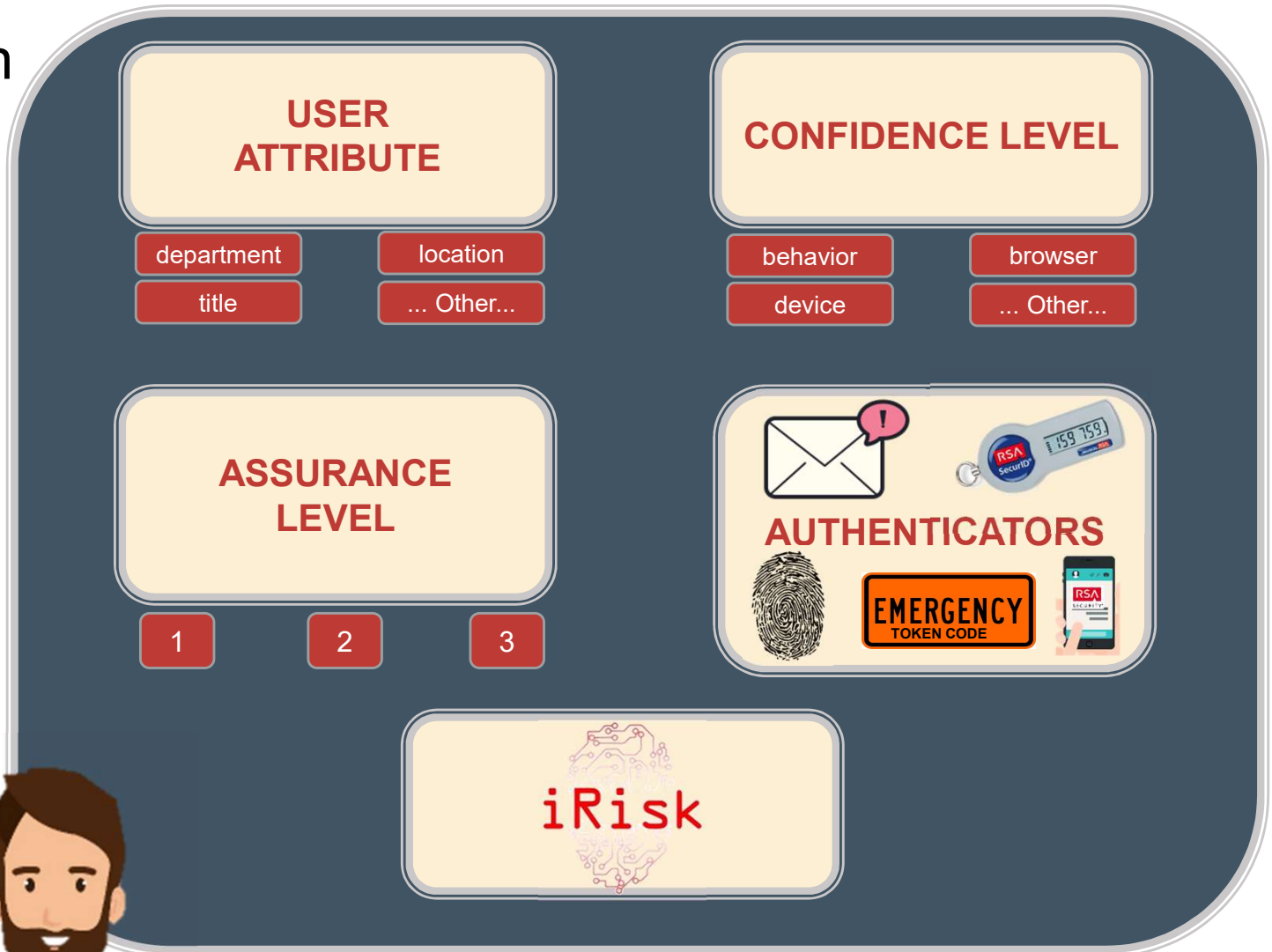
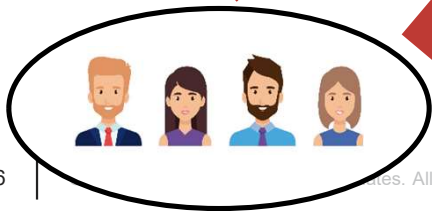
- Assigned tasks (Approvals, Activities, Reviews, Remediation) can be delegated
- Tasks are always visible to the delegate, delegator and user
- Detailed history of the requests and delegations



# Access to an application



**FILTER**  
Search Criteria /  
Lookup users



**RSA**

# Benefits RSA SecurID® Suite



**RSA**

BUSINESS-DRIVEN SECURITY™

- VISIBILITY
- GOVERNANCE
- SECURITY
- CONVENIENCE
- COMPLIANCE
- AUTOMATION

# Conclusion

- **Digital identity is pervasive** and still the **main trigger** of most cyber attacks
- **Identity risk is a major component** within the operational risks, and it's characterized by a **very high volatility**
- This risk can be measured considering both **technology and business factors**
- To effectively address and mitigate this risk, **speed is a key factor!**
- This requires both **automation** and **integration** across the products that manage the identity and governance information
- The **RSA SecurId Suite** and **RSA Archer Suite** allows you to achieve this goal!



# Thank You

©2020 RSA Security LLC or its affiliates.  
All rights reserved.

**RSA**



**RSA<sup>®</sup>**