RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: IDY-F02

How to Implement an Identity & Access Management (IAM) Program Driven by Access Analytics

Vishu Mandalika

Director, Information Security
CVS Health

Goals of an IAM Transformation Program

- Enable business processes at a high velocity and low cost.
- Manage security risk for the enterprise effectively.
- Maintain full compliance with the IAM regulatory requirements.

Key Drivers of an IAM Transformation Program

People

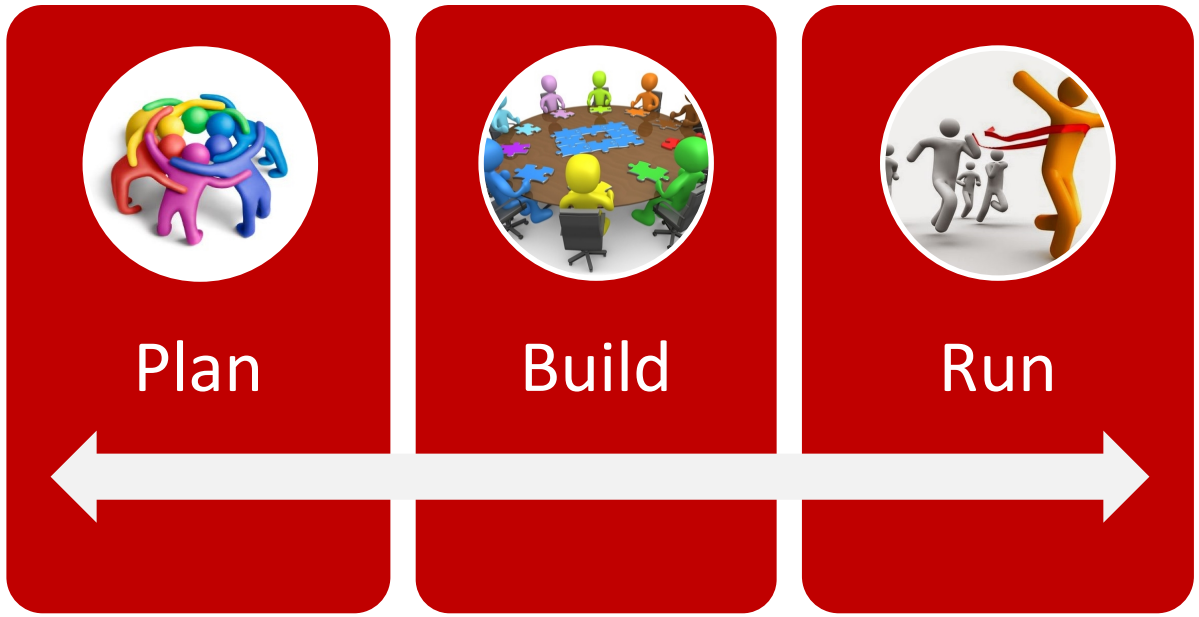
Process

Technology

Guiding Principles

- Deliver a delightful user experience with IAM services
- Apply best available technology, products and methods to meet business objectives
- Design IAM services/solutions to be as simple as possible
- Support business agility by rapidly delivering incremental improvement to IAM products and services
- Move to/adopt Analytical Model Driven Security for IAM

Organizational Model



RSAConference2020

Key Strategy for IAM Products/Services

Identity Data Store & Identity Data Services

- A single view of the Workforce Identity is critical for IAM success.
- Digital identity is NOT an account. Recognize the fact that identity is not the same as an account, and stop using provisioning tools as your identity store or for identity data services to downstream applications.
- An identity data store that provides an aggregated view of person and non-person identities with a rich data services layer supports simplicity, delightful experience, cost effectiveness, compliance and risk management.

Access Analytics & Entitlement Data Warehouse

- Aggregate the user access data from enterprise platforms (AD, Databases, OS platforms etc.,) and applications to provide a single ‘pane of glass’ view.
- Build a centralized entitlement data warehouse through aggregation. Provide tools and services to manage the entitlement meta-data such as the description, risk rating, privileged flag etc.,
- Key to accelerate improvements in all other IAM tools/services.

Access Provisioning

- Automation first. Consider manual provisioning only when there is a clear requirement and a viable financial model for doing so.
- Retire provisioning systems which don’t provide enough business value, but don’t be bogged down by the idea that there should only be one provisioning tool.
- Use recommendations from Access Analytics to “sense” the access a workforce member needs and provision it without requiring the person to request for it. Supports simplicity, delightful experience and cost effectiveness.

Access Review & Recertification

- Stop treating access reviews as a compliance-driven activity, and approach them as a security mitigation exercise to derive the most benefit.
- Aggressively pursue simplicity principle and identify opportunities to simplify the user experience including reducing the scope of the access reviews as much as possible.
- Use risk-driven and event-based access reviews as much as possible to get the most out of this exercise.

Access Policy Management

- Identify a unifying approach/strategy for Access Control Policy Management such as RBAC/ABAC.
- There can be multiple tools and services to support this function, but there will need to be one overall approach/methodology to reduce confusion and improve customer experience.

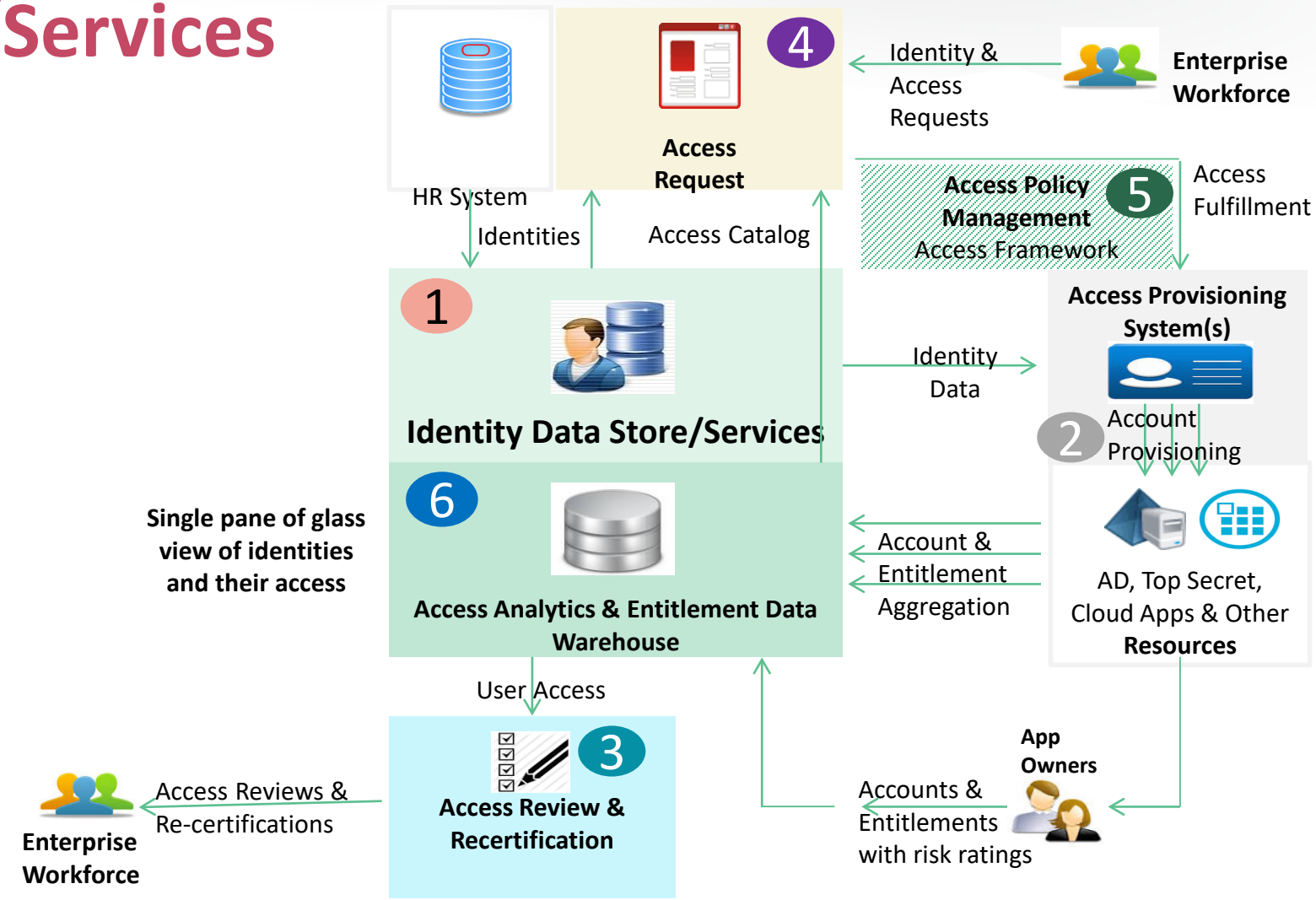
Access Request

- Utilize analytics to make the access request process as simple as possible and reduce request errors supporting a delightful user experience.
- Integrate with automated access provisioning tools and services for faster provisioning.
- Build workflows to support access recommendation services using data analytics.

Behavior Analytics

- Behavior analytics works best on the foundation of a comprehensive view of identities, accounts, and activity.
- Key to Analytical Model Driven Security.

Key IAM Products/Services

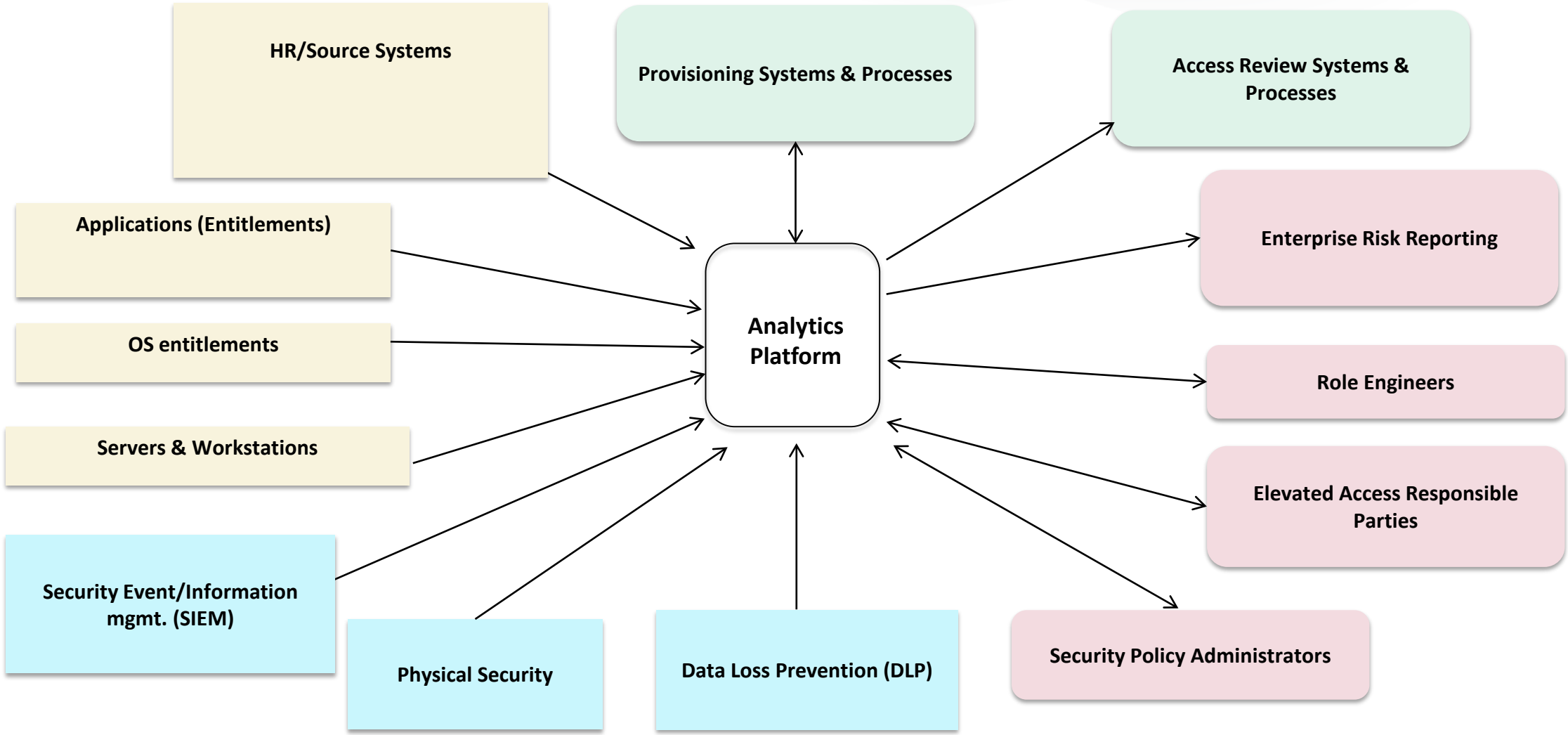


RSAConference2020

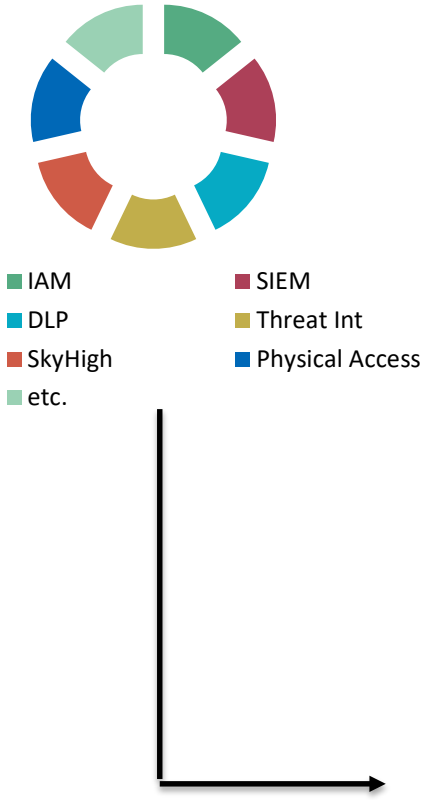
Analytical Model Driven Security

Analytics Platform

A Single Pane of Glass View of the Enterprise-wide Access



Analytical Model Driven Security



Collect Enterprise Risk Intelligence based on all available data

- Historical behavior pattern analysis
- Peer group analysis
- Geographic location
- Policies & known exceptions (e.g. SOD policies)

Individual Risk Scores

- Similar to a credit score
- Individualized to each user
- Adjust dynamically based on user behavior

Behavioral based risk scores are the foundation of model driven security.

How do Analytical Models Work?

- Apply machine learning to create a baseline of normal behavior for every identity
- Build analytical models using the data: behavioral, rules based, or external
  - If a model is triggered, a case is created and investigation occurs
  - The weighted value of the model is applied in a calculation to determine a risk score

Example: Retrieving Vaulted Password

User attempts to check out a vaulted password

Risk score is evaluated

Approved

Denied/Call HelpDesk

Example: Fine Grain Policy Control

User gives two-week notice

The risk to the enterprise has changed.
This user is now considered HIGH risk.

Monitor the user more closely

Change the lens

This allows us to switch lenses and look at the employees from a different point of view based on the risk profile.

RSAConference2020

Key Takeaways

Apply What You Have Learned Today

- Next week you should:
  - Start working on documenting the current state of your existing IAM program
- In the first three months following this presentation you should:
  - Define your IAM strategy clearly. Move away from compliance-driven IAM in favor of analytics & risk-driven IAM
  - Define the key services/products you need to implement to transform your IAM program
- Within six months you should:
  - Kick off and drive the implementation of an Analytical Model Driven IAM Transformation program