

Identity & Access Management Gliding Flight

Paolo Ottolino PMP CISSP–ISSAP CISA CISM OPST ITIL

- 1 General Concepts
- 2 Logical Components
- 3 Implementation Structure
- 4 Governance
- 5 Web App Firewall (WAF)

1. General Concepts

IAM: Opened Features



- **Seamless Integration:** enable business processes, people, and heterogeneous applications to work together seamlessly and securely
 - **Secure Control:** Being able to view and control who has access to what resources: effectively protecting sensitive information
 - **Improved User Experience:** transparent and uninterrupted user's experience in interacting with multiple entities in multiple ways
 - **Cost Reduction:** reduce administrative costs by automating manual processes.
- Integrated and integratable solutions across traditional business boundaries
 - Enabling compliance with legislative mandates and regulatory requirements (Security, Privacy, and Governance)
 - Directory-based identity management
 - Reduce spiraling help desk and other support expenses through capabilities such as automation, self-service, and delegation

1. General Concepts

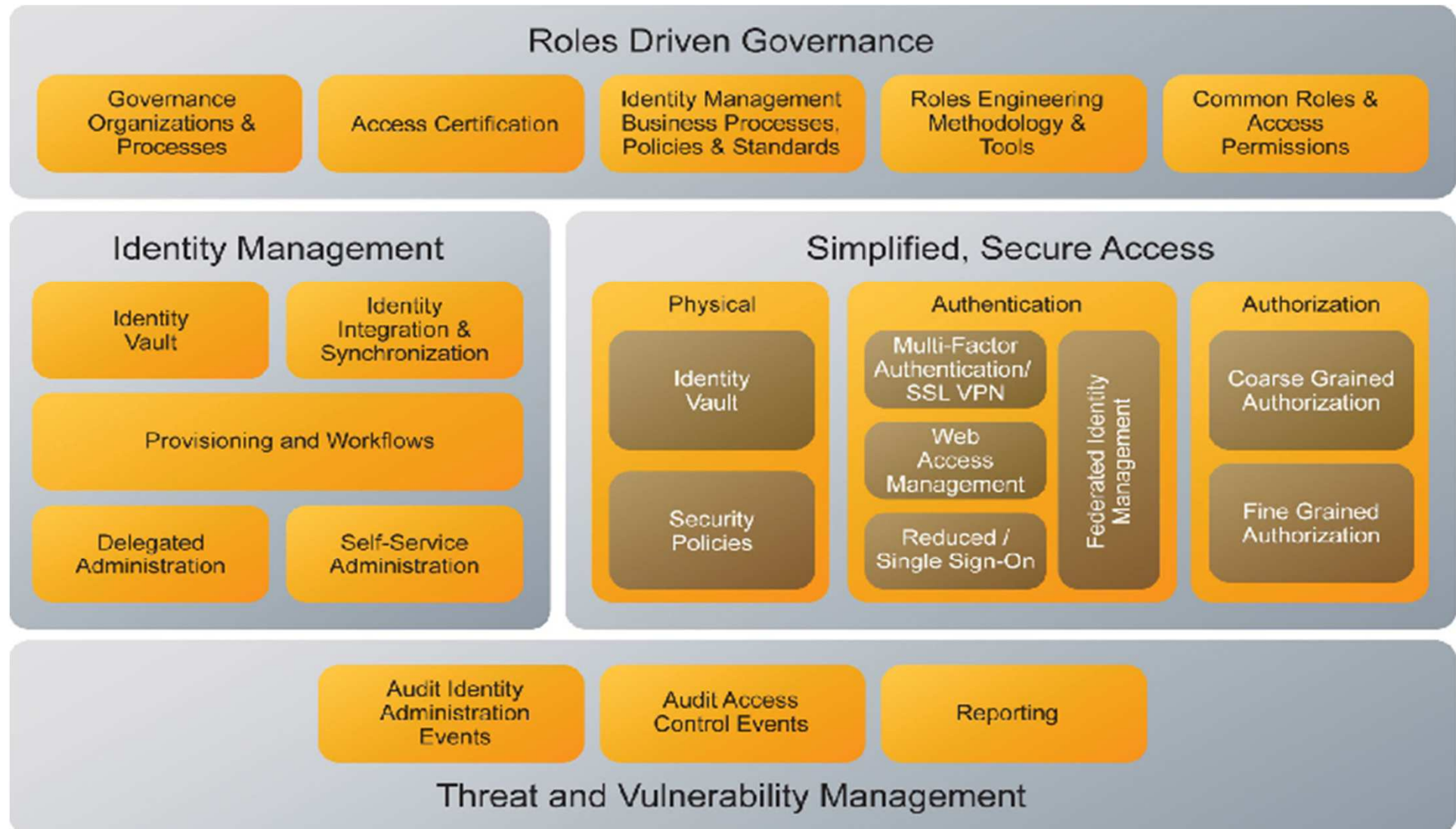
IAM: Expected Benefits



- **Need to Know:** every user can access only the information needed to perform his job
 - **Segregation of Duties:** it is possible to activate different application functions for different roles and tasks
 - **Approval Workflow:** every modification (advancement, special task, leave, etc) to each user's attribute should be put under specific approval
 - **Activity Monitoring:** collecting, analyzing and (eventually) forgiving evidences of (unusual) action performed by Administrators, changing user's attributes values
- Proper Role definition and Access Control performed accordingly
 - Proper Role definition and Access Control to provide compliance
 - System of Validation for every modification, for adhering to official organization change
 - Infrastructure for collecting log from systems and applications, in order to analyze information

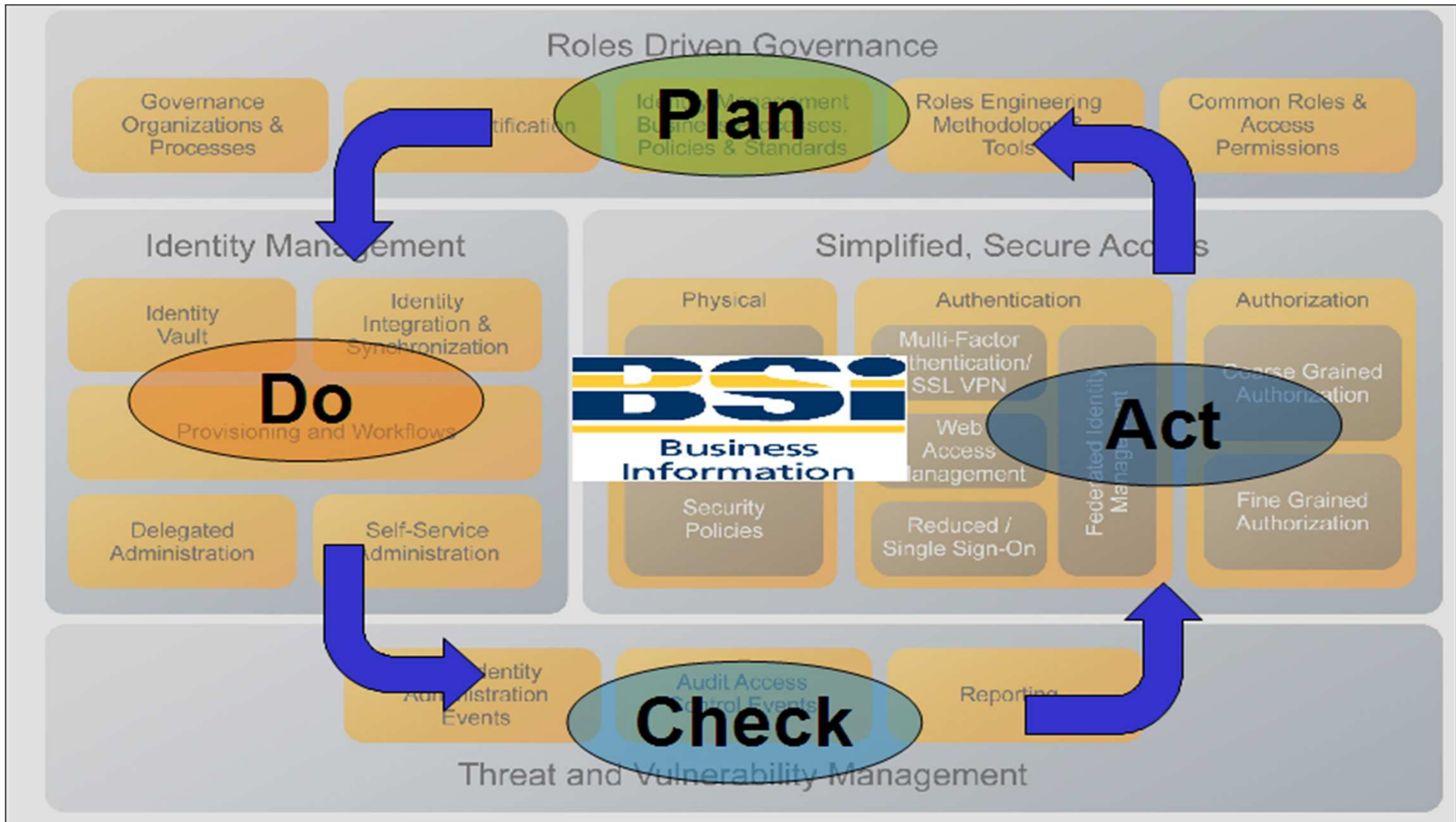
1. General Concepts

IAM Framework



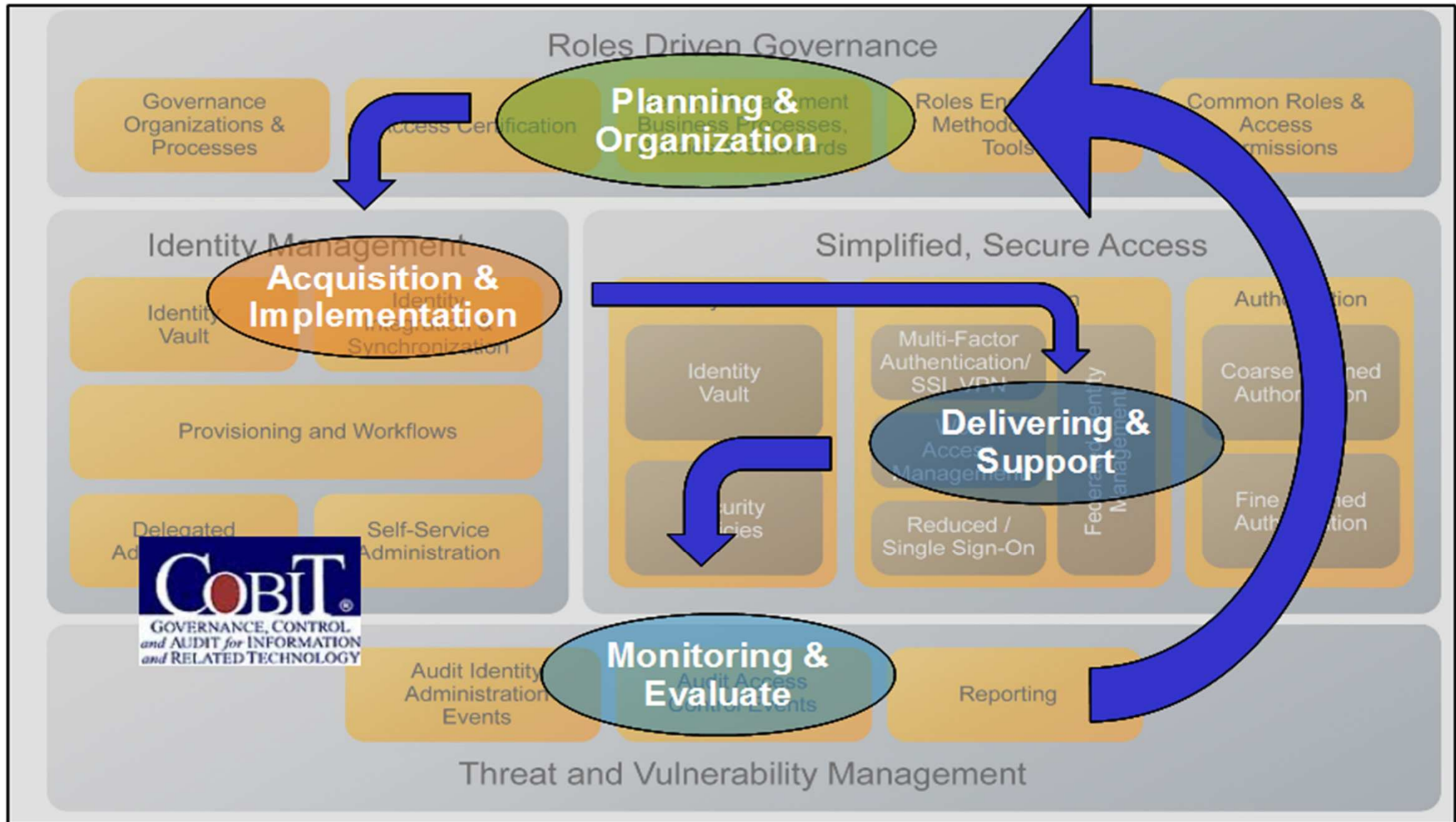
1. General Concepts

IAM Framework vs Deming Cycle (PDCA)



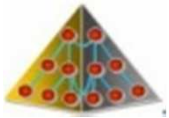
1. General Concepts

IAM Framework vs CobiT 4.1

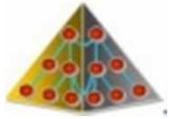


1. General Concepts

Key Features



RBAC: Role-Based Access Control



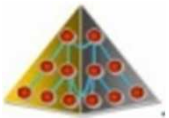
OUA: Orphan User Account



FGE: Fine-Grained Entitlements



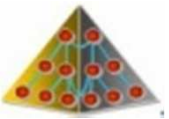
RM: Role Mining



SoD: Segregation of Duties



ACAR: Access Certification Attestation Re-certification



RBA: Risk Based Analysis

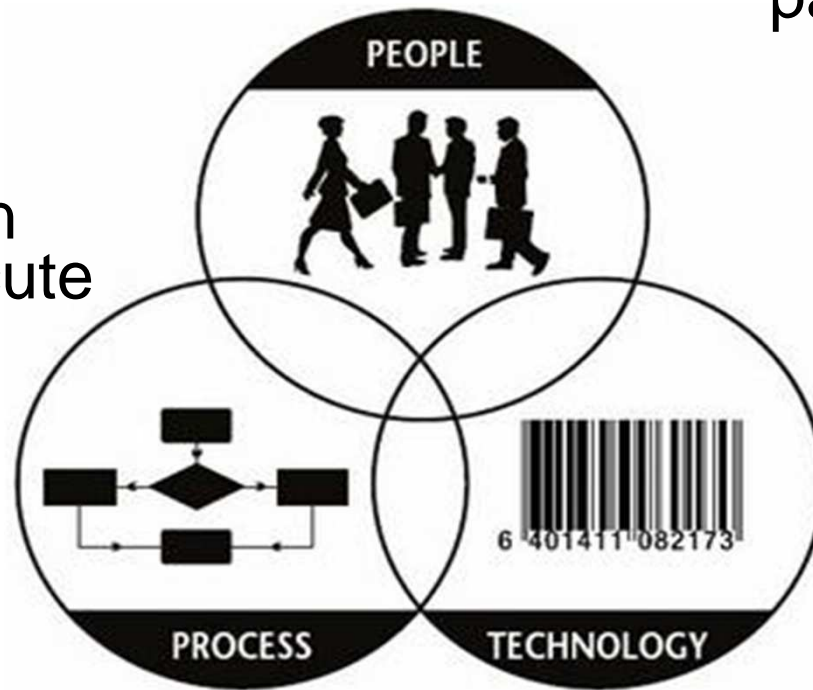
2. Logical Components

IT Elements: People, Process, Technology



People: stakeholders
(employees, customers,
partners, suppliers)

Process: action
performed to execute
business



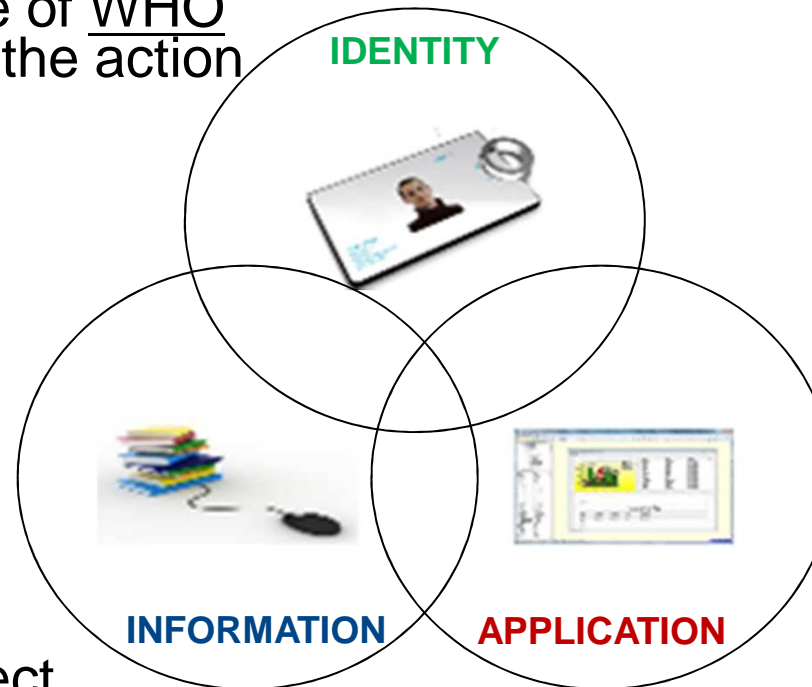
Technology: tools used to
perform processes by people

2. Logical Components

IT Concepts: Identity, Information & Application



Identity: personification into the IT world. Instance of WHO and WHY to perform the action



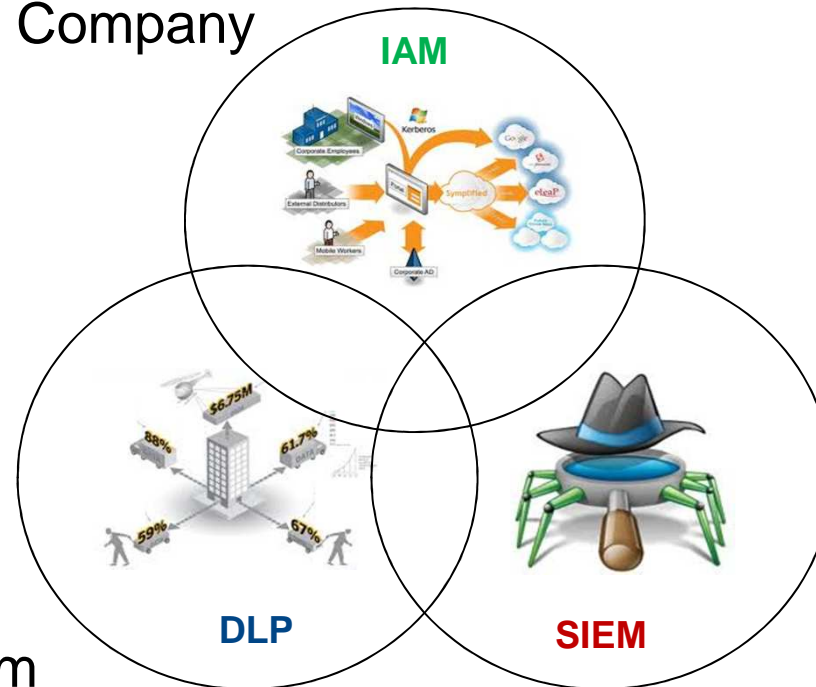
Application: object composing the IT world. Instantiation of WHEN and WHERE to perform the action

Information: object surrounding the IT world. Instance of WHAT and HOW to perform the action

2. Logical Components

IT Sec Infrastructure: IAM, DLP, SIEM

IAM: management of identity, and its attributes, mapped in virtual tree fashion, according to Company hierarchy



SIEM: management of security information (log) and events (coming from application)

DLP: protection from uncontrolled data leakage, performed by information users

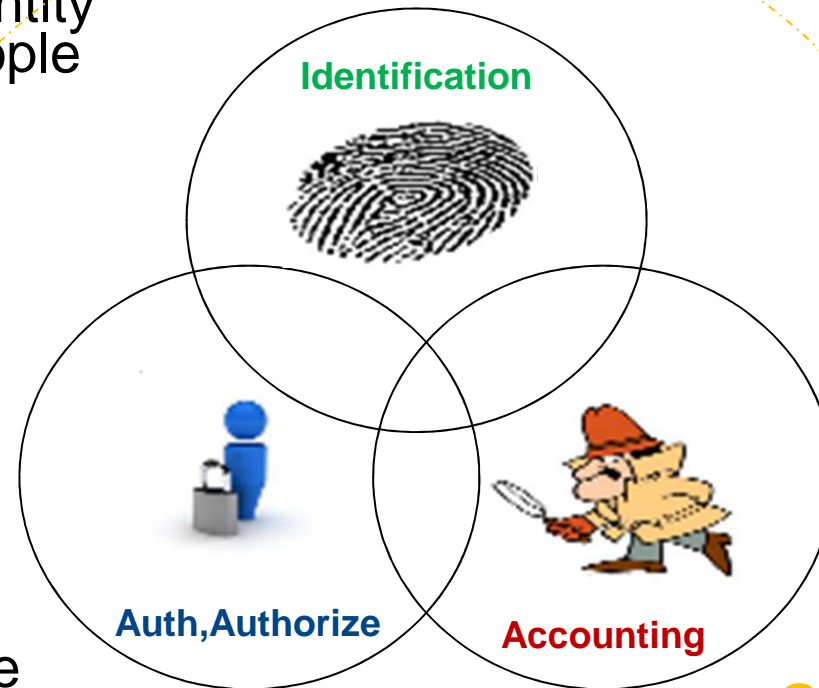
C4: from Military Environment (Computer/Communication Command & Control)

2. Logical Components

IAM Actions: Id, Auth, Authorise, Account + Govern



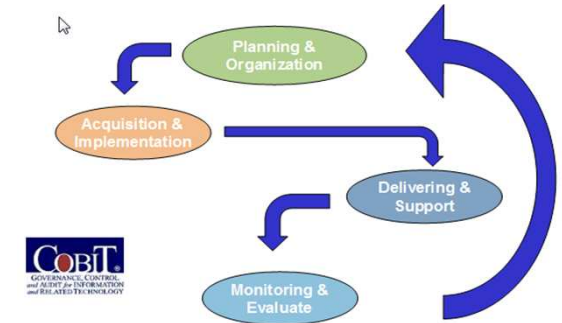
Identification: personification in the IT world. Virtual Identity association to each people



Accounting: monitoring and tracking of accesses and performed operation and accessed data

Auth, Authorize: provide proper access to resources and Information on the basis of Attribute values

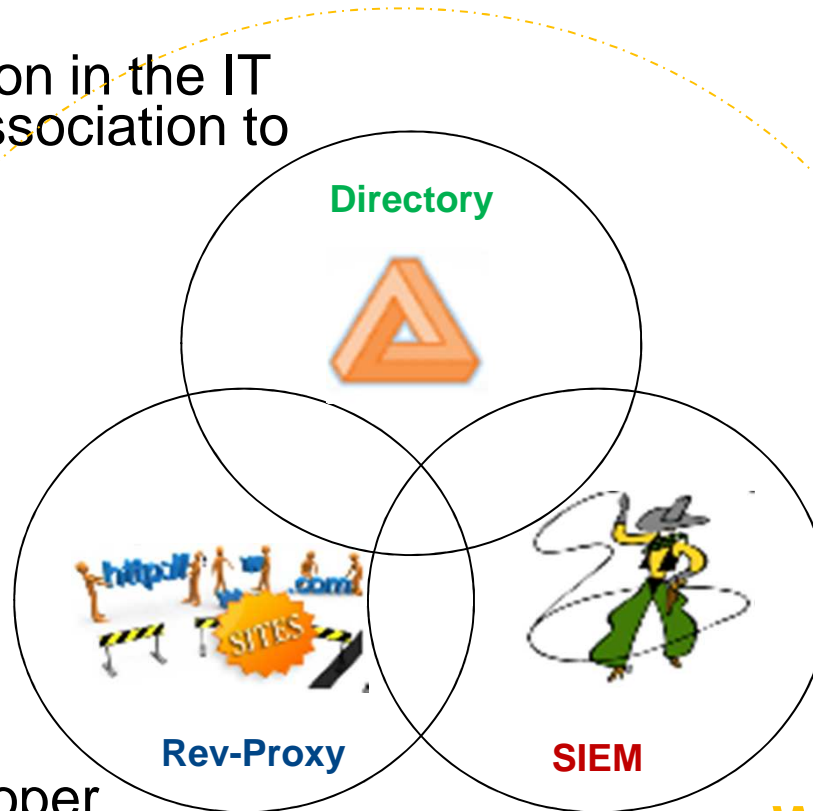
Governance: plan, enforce, control, clean-up and certify identity-related issues



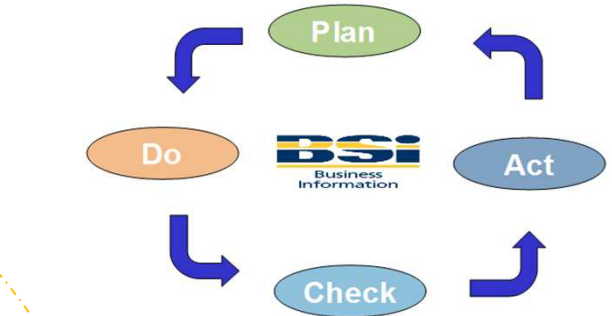
2. Logical Components

IAM Objects: Directory, Rev-Proxy, SIEM

Directory: personification in the IT world. Virtual Identity association to each people



Rev-Proxy: provide proper access to resources and Information on the basis of Attribute values

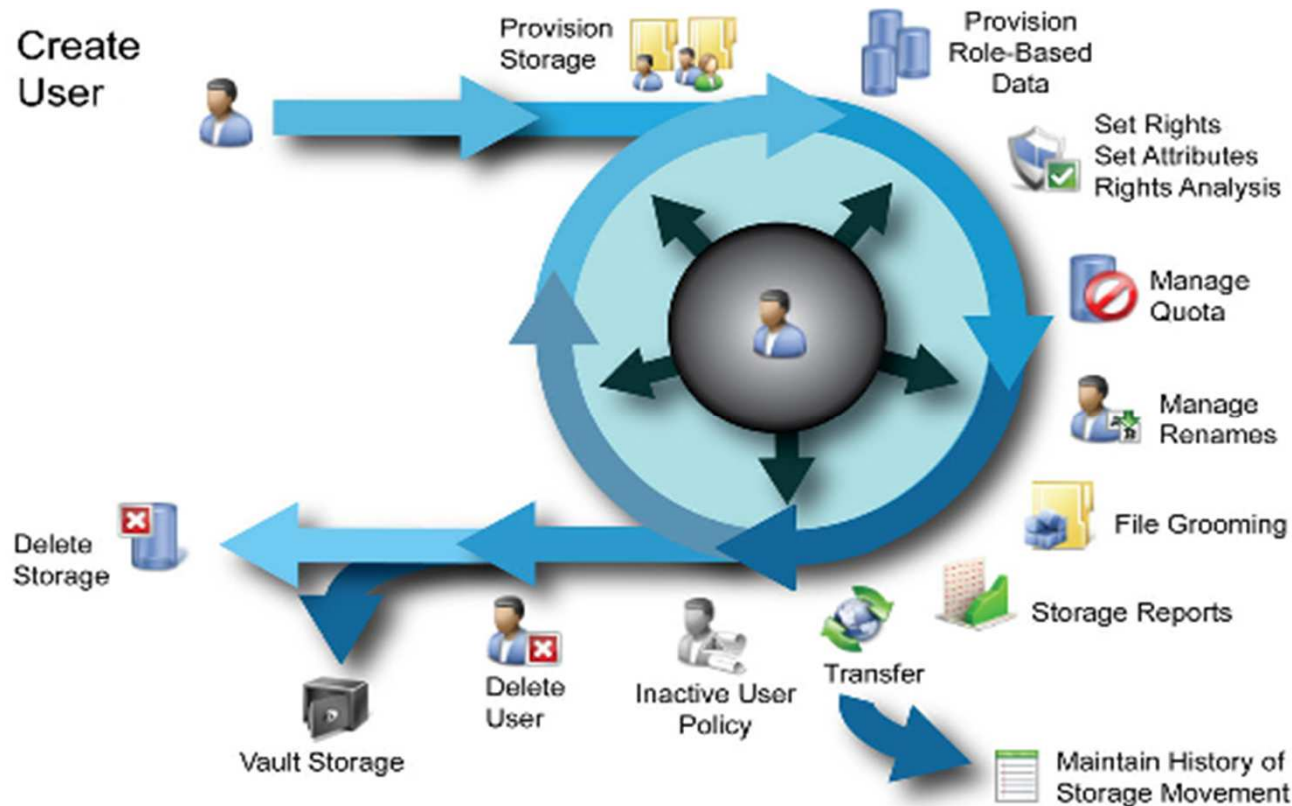


SIEM: monitoring and tracking of accesses and performed operation and accessed data

WKF & Engine: core component for activating all human processes and technical interaction

3. Implementation Structure

Usual Pains in IAM Projects 1/2



Identity Life-Cycle

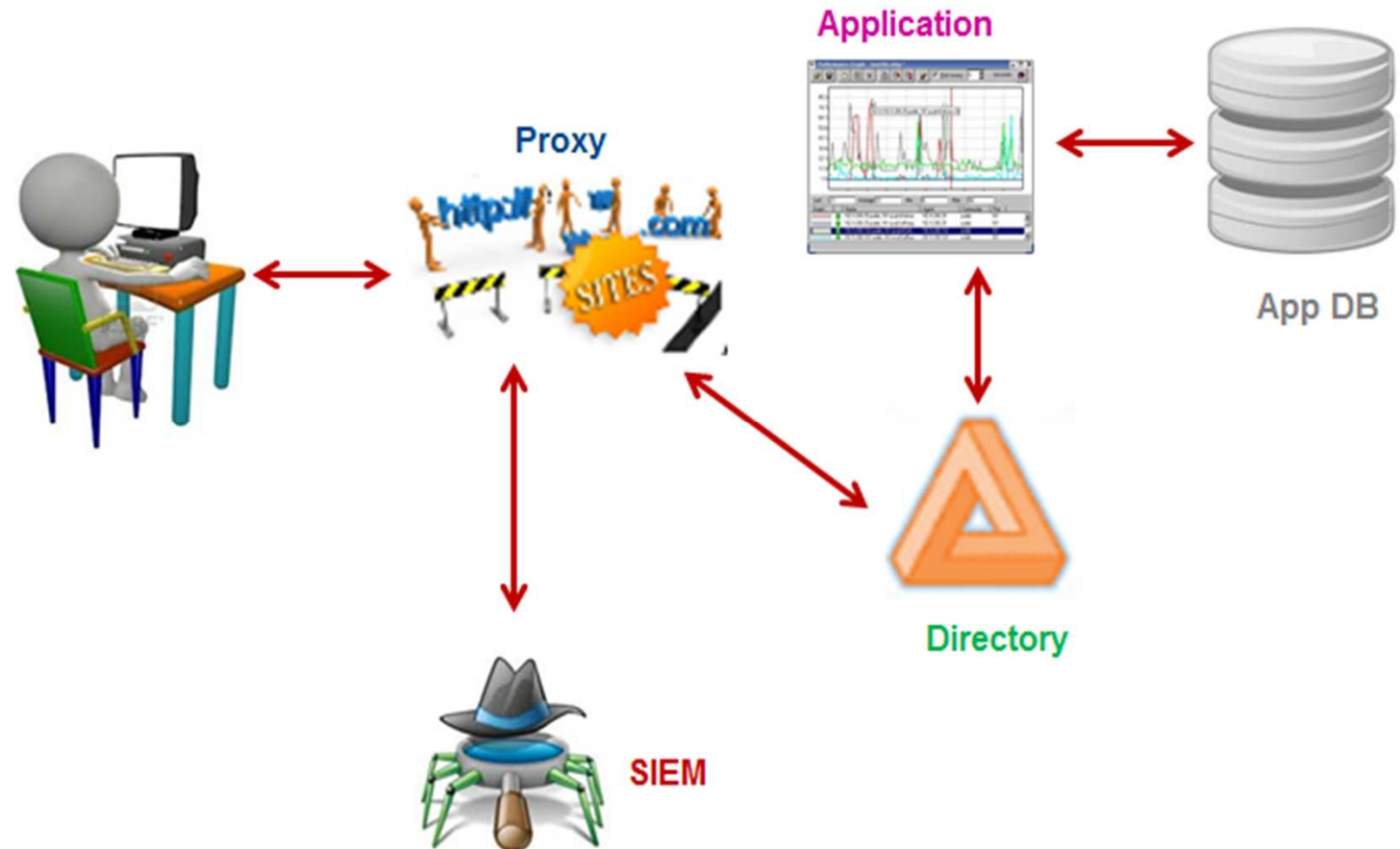
- Unique entry point (SAP HR?)
- Complete Identity Acknowledge
- Approval Workflow (due to initial event)
- App vs Org Chart mapping
- Role Minding

3. Implementation Structure

Usual Pains in IAM Projects 2/2

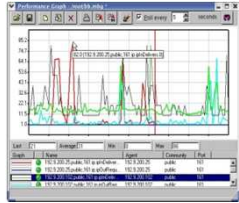
Application

- Identity-ready (attributed-driven access)
- HTTP (no Client/Server)
- Authentication Header
- IBM Legacy integration
- Cloud Architecture
- Federation (accountability delegation)
- Fine-Grained (XACML)



3. Implementation Structure

Key Success Factors: Environment Knowledge



Application Asset Counting

- Owner
- Functionalities
- Organisational Responsibility



User Provisioning, Identity Synchronization, Identity Audit

- Automated Account Provisioning, Key Architecture Considerations
- Identity Synchronization Services, Identity Audit



Password Management

- Pwd Management, SelfService



Access Management and Federation Services

- Access Management, Federation Services



Directory Services

- Directory, LDAP Directory Services, AD Synchronization
- Directory Proxy Services

3. Implementation Structure

Application Asset



Application Characteristics		
App Name	Name of the Application, together with refereces (i.e. IP address o DNS name)	
Organzation	Organization that sponsored the app	
Business Unit	Business Unit (part of the above organization) tha actually manages the app	
Responsible	The name of the person that is in charge for the management (i.e. Change) to the application	
Main Functionality	Short Description, addressing the offered functionalities, allowing to identify the part fo the Org Chart that should access it, the App Roles, etc	

3. Implementation Structure

Identity, Attributes, WorkFlow



Identity		
Approval	Who is in charge for approval of creation, modification, suspension and deletion of accounts	
Id Source	Where each account is stored	
Repository	References to the repository (IP, DNS name), type (i.e. LDAP, DB) and access (i.e. Password, certificate, etc)	
Attributes	User's characteristics, qualities pointed out into the identity description. These could be useful to determine right permissions and access right in specific application	
Roles	User's special characteristics, due to categorization, expressed as belonging sets (roles)	
Naming	Eventual naming convention or mapping between attribute names used in different applications	
Workflow	Current workflows in order to approve identity modification (creation, suspension, etc)	
Compliance Issues	SoD (Segregations of Duties) needed to be compliant to some laws or regulations	

3. Implementation Structure

Dimensioning



Directory		
#Internal Users	Total amount of internal users	
#Partner Users	Amount of users belonging to partners to the current company	
# Occasional	Estimated value of occasional users	
# Admin	Amount of users that own special right (i.e. DBA, OS admin, Network, etc)	
# Total Users	Total amount of users belonging to the different groups	

3. Implementation Structure

Password



Password		
Strength	Collection of password policies enforced on every system, in order to guarante the needed strenghtness	
Disabling	Collection of policies used for disabling users	
Self-Service	Eventual offered services for autonomous password management (change, resume, etc)	

3. Implementation Structure

Application Access, SSO, Logging



Accesso		
System/Platform	System and Platform on which the application is running	
Version	Exact version of System and Platform	
Auth	Kind of Authentication performed (i.e. password, certificate, etc)	
Procedure	Sequence (i.e. 1 factor, 2 factors, etc)	
Security	Kind of implemented security (SSL, Ash, etc)	
SSO	Does the application belong to an infrastructure able to provide SSO?	
Logging	Does the application provide logging capabilities?	
Federation	Required features about federation	
Interface	Which kind of interface (HTTP, LDAP, etc) the application provides	

4. Identity Governance

Correcting the IAM Behaviours

Effectiveness: to be able to soundly
answer to Internal Audit



Efficiency: to provide fast, useful
and complete responses

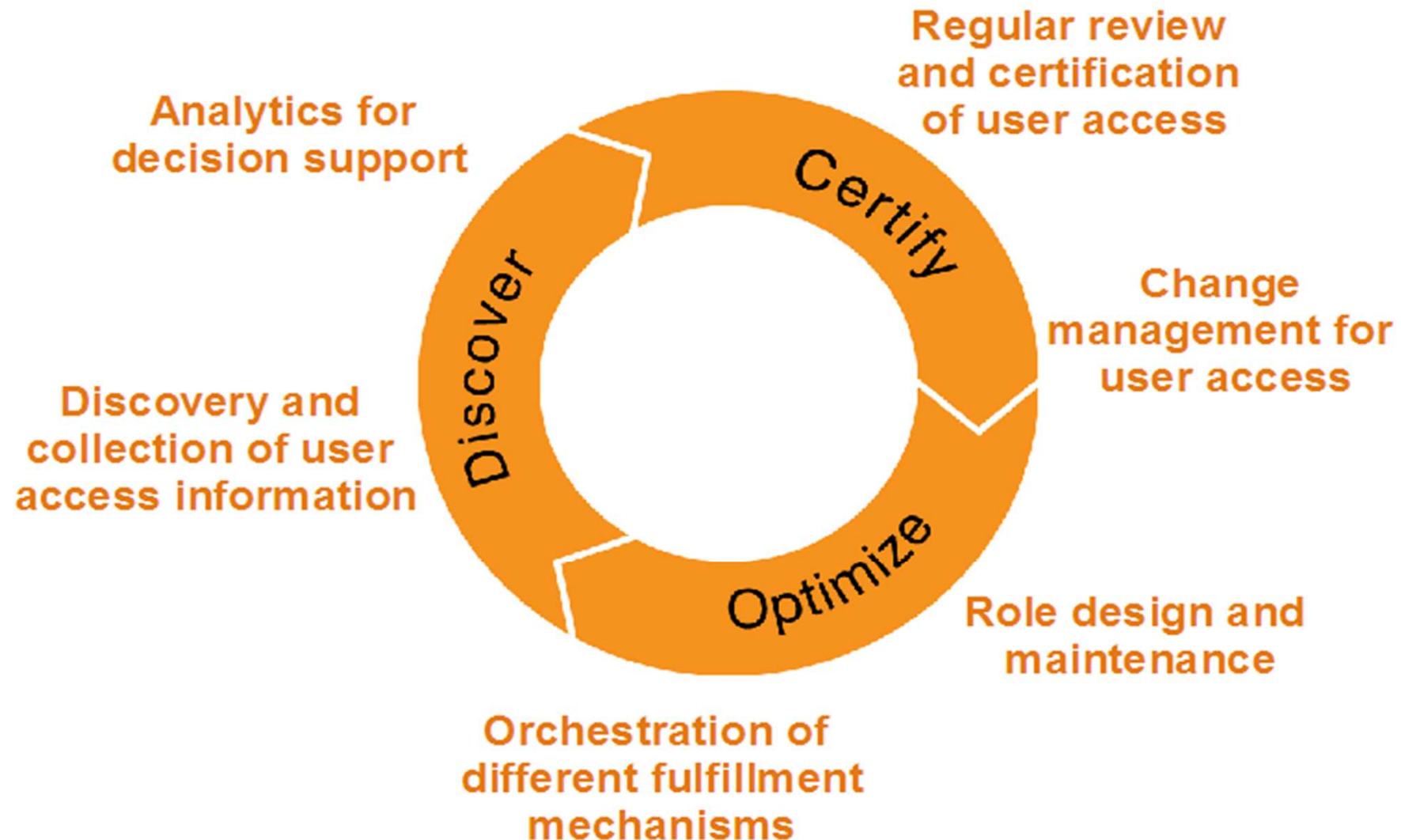


Proactivity: to prevent Auditor enquiry
By proper scheduling



4. Identity Governance
















Dynamic, OnGoing Process



4. Identity Governance

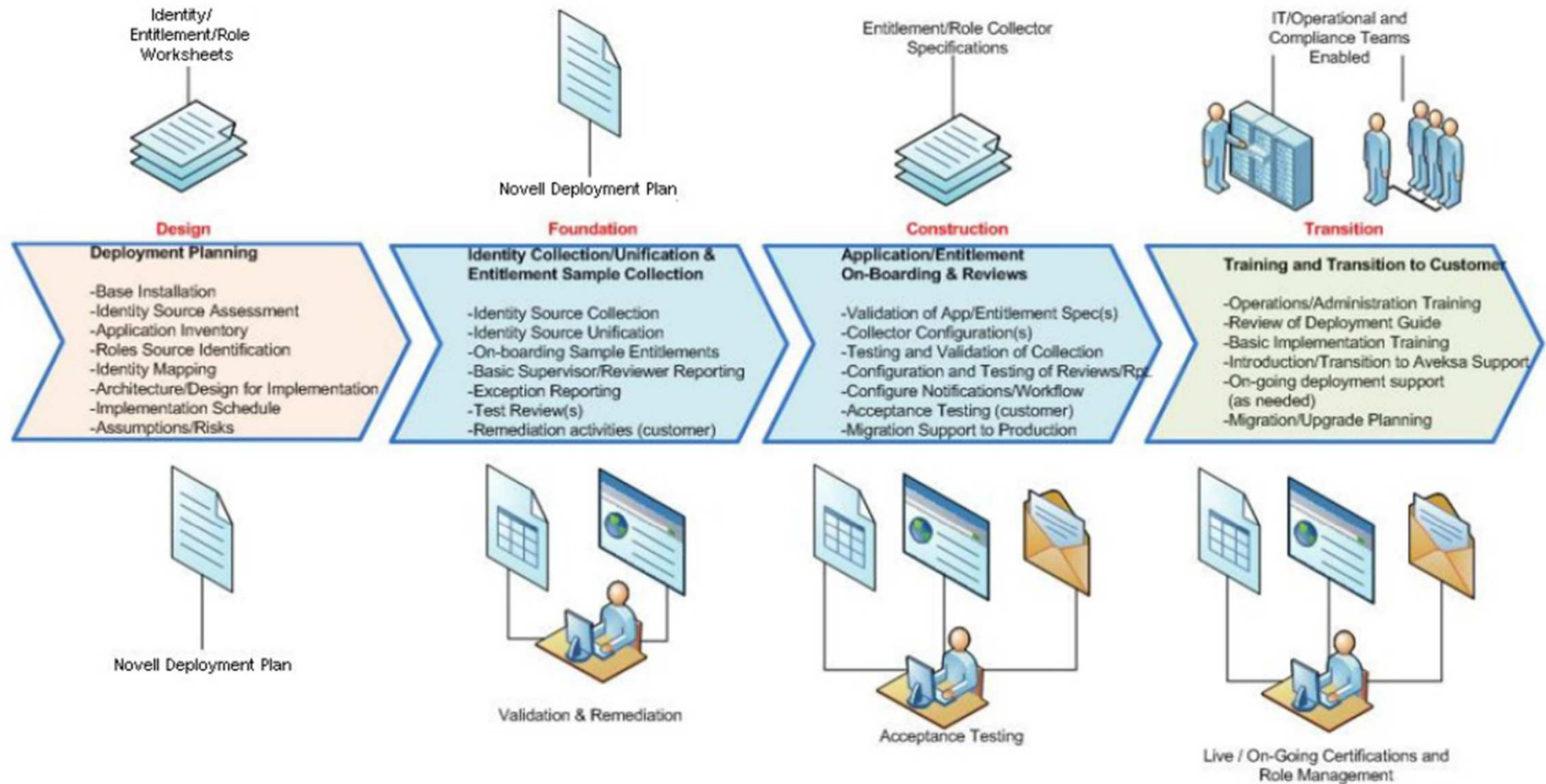
IAM vs Access Governance



	IAM	IAG
Stengthness & Efficiency	Effect: <u>Risk Elusion</u> Mode of Operation: <u>Automatic</u>   	Effect: <u>Risk Mitigation</u> Mode of Operation: <u>Manual</u> 
Costs	Project Duration: <u>High</u> Involved Resources: Many   	Project Duration: <u>Low</u> Involved Resources: Few 
Organizational Impact	Involvement: <u>Direct</u> Change Management: <u>Needed</u>  	Involvement: <u>Indirect</u> Change Management: NOT <u>Needed</u> 
Amplitude of Operation	Application Number: <u>30%</u> (average) 	Application Number: <u>100%</u> (account DB)   

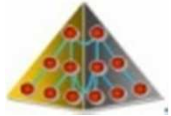
4. Identity Governance

High Level Approach

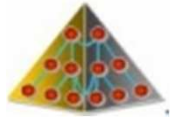


4. Identity Governance

Key Features



RBAC: Role-Based Access Control



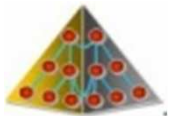
OUA: Orphan User Account



FGE: Fine-Grained Entitlements



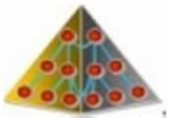
RM: Role Mining



SoD: Segregation of Duties

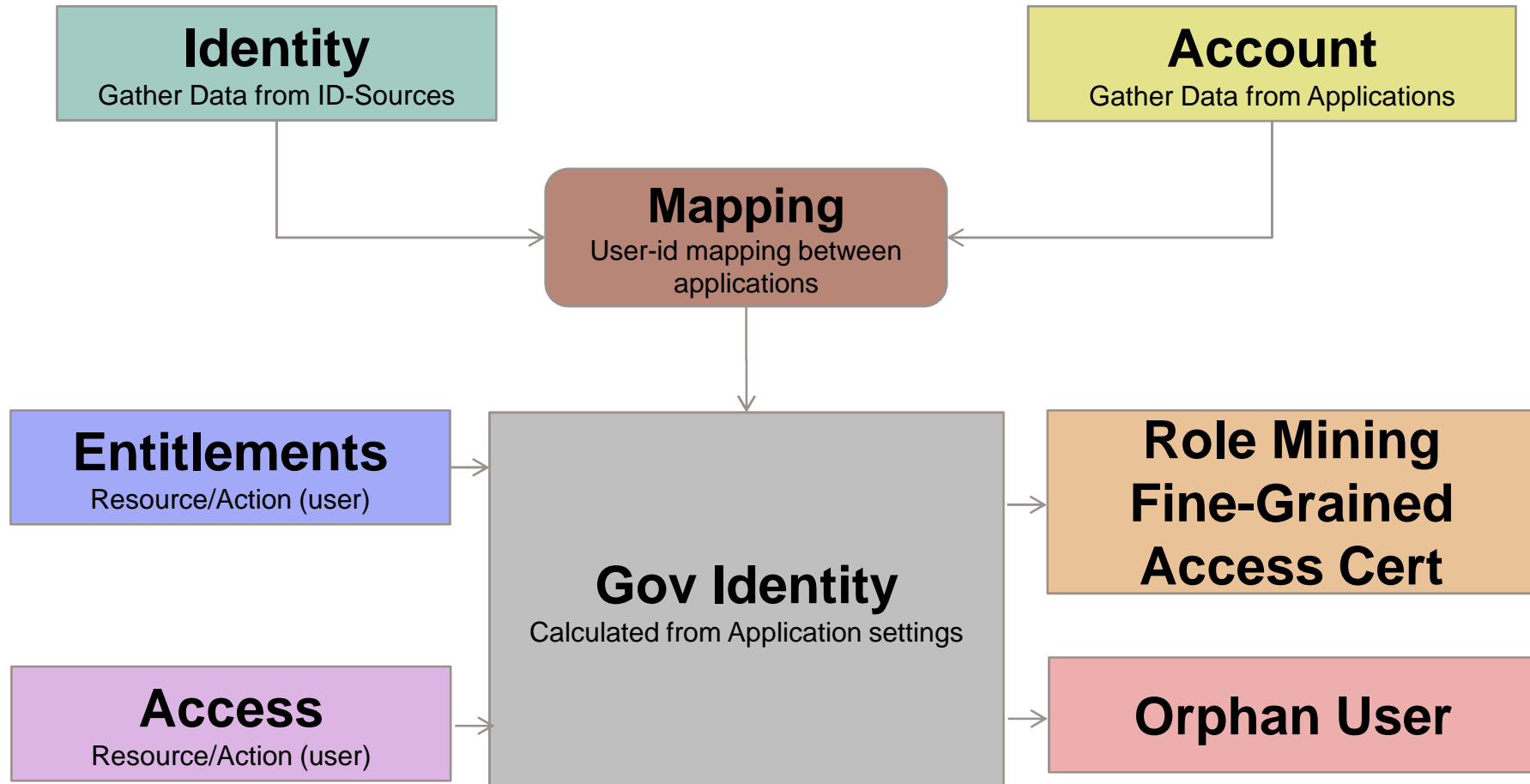


ACAR: Access Certification Attestation Re-certification



RBA: Risk Based Analysis

4. Identity Governance Process



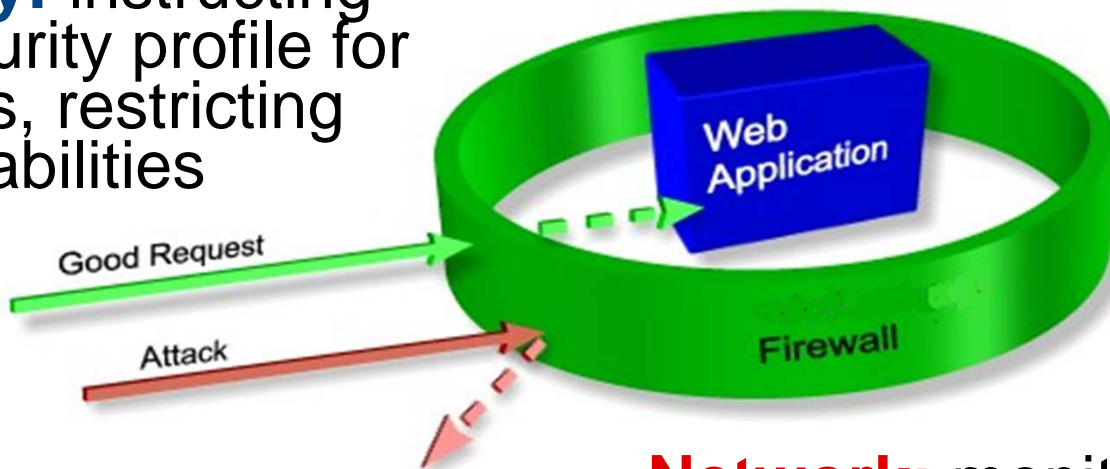
5. Web Application Firewall

IT Sec & Web 2.0: Access, Capability, Network



Access: issuing the correct user to enter the proper application functionality

Capability: instructing proper security profile for programs, restricting capabilities



Network: monitoring, controlling and taking advantage of the proper means to pass information through

AM implies a GW → IT Command & Control

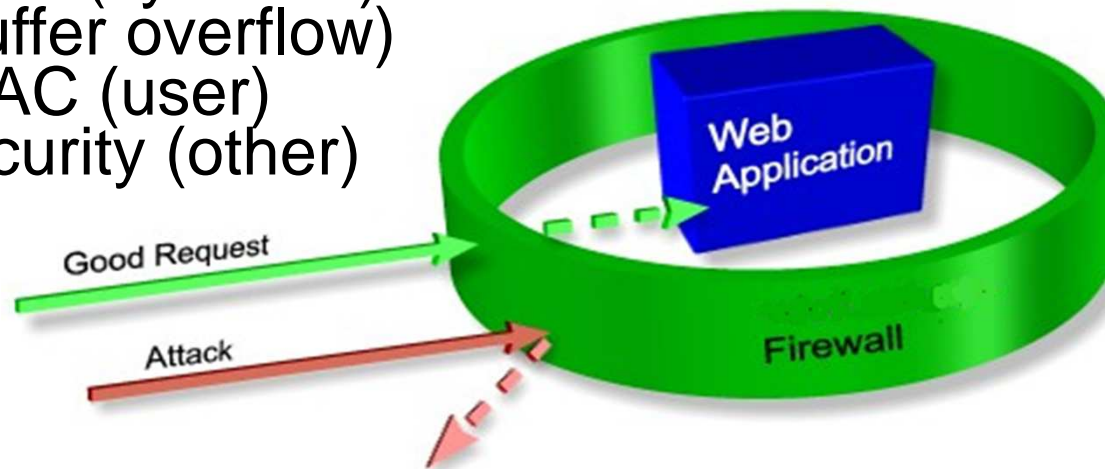
5. Web Application Firewall

IT Sec & Web 2.0: Access, Capability, Network



Capability

- App Armor (apps)
- SysTrace (sys calls)
- PaX (buffer overflow)
- RBAC (user)
- GRSecurity (other)



Access

- Identity Server (directory)
- Access Gateway (enforce)
- iManager (admin)

Network

- Iptables (FW)
- Snort (IPS)
- Load Balancing (BC/DR)

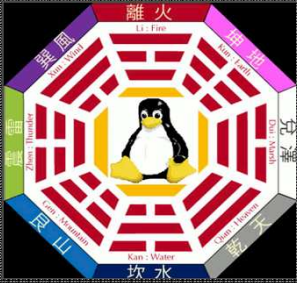
AM implies a GW → IT Command & Control

5. Web Application Firewall

WAPF References: WWW Articles & Manual



	References
OWASP	Open Web Application Security Project:
Open-Source	Open Source Web Security Tools: NAXSI: ArmorLogic: Modsecurity:
Vendor	Barracuda Networks: Imperva: F5 Networks: Bee Ware: TrustWave: Breach Security:



Thank You