Identity Cloud Services: What, Why, and Should We Convert

MOUS 2017

Oracle Top 25

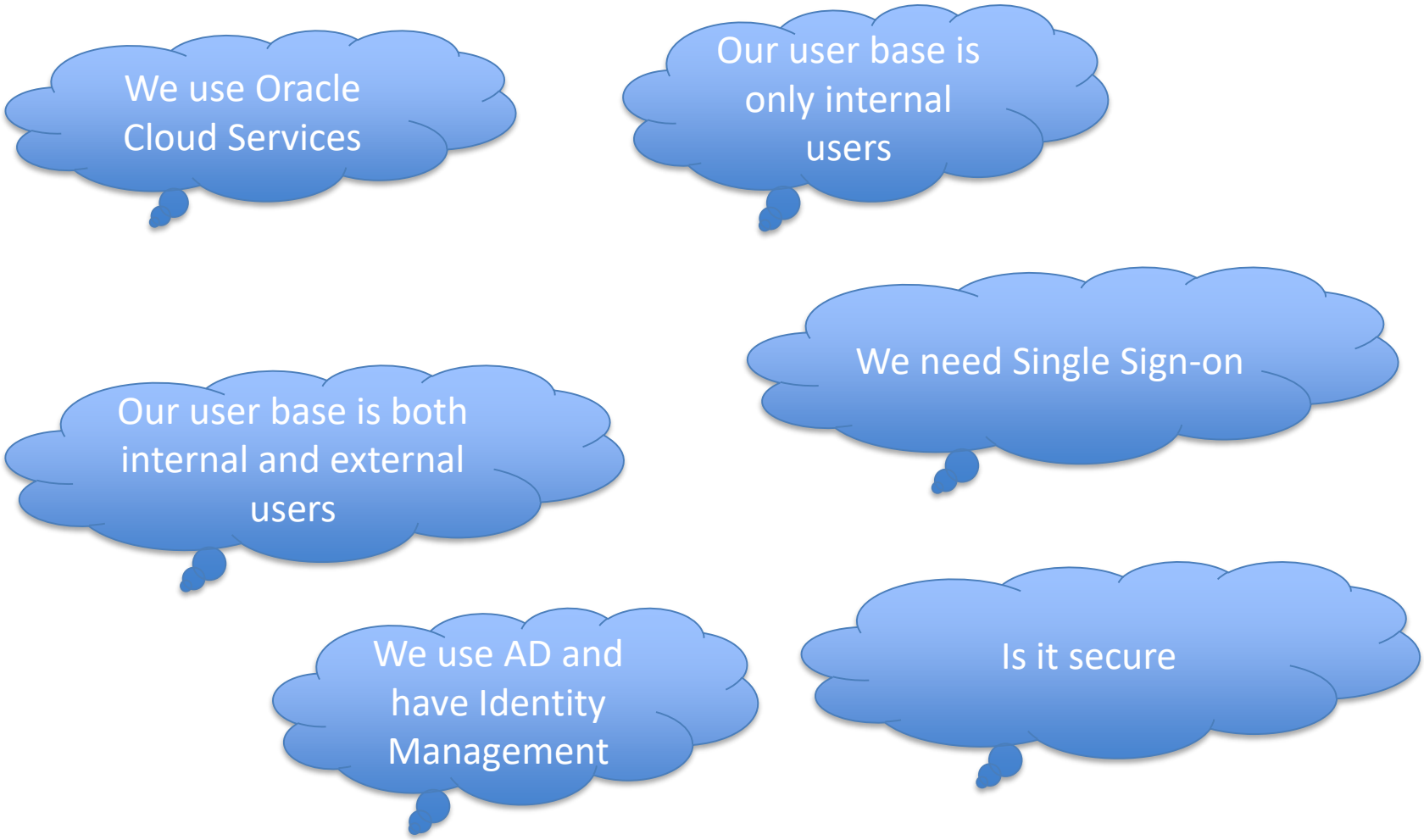
ORACLE Platinum Partner

Managed Services | Consulting Services | Cloud Services | Oracle Resell

Agenda

- Introductions
- Business Concerns
- Background information
- Identity Cloud Services Overview
- Detailed Look
- Architectures
- How it fits
- Should you use it

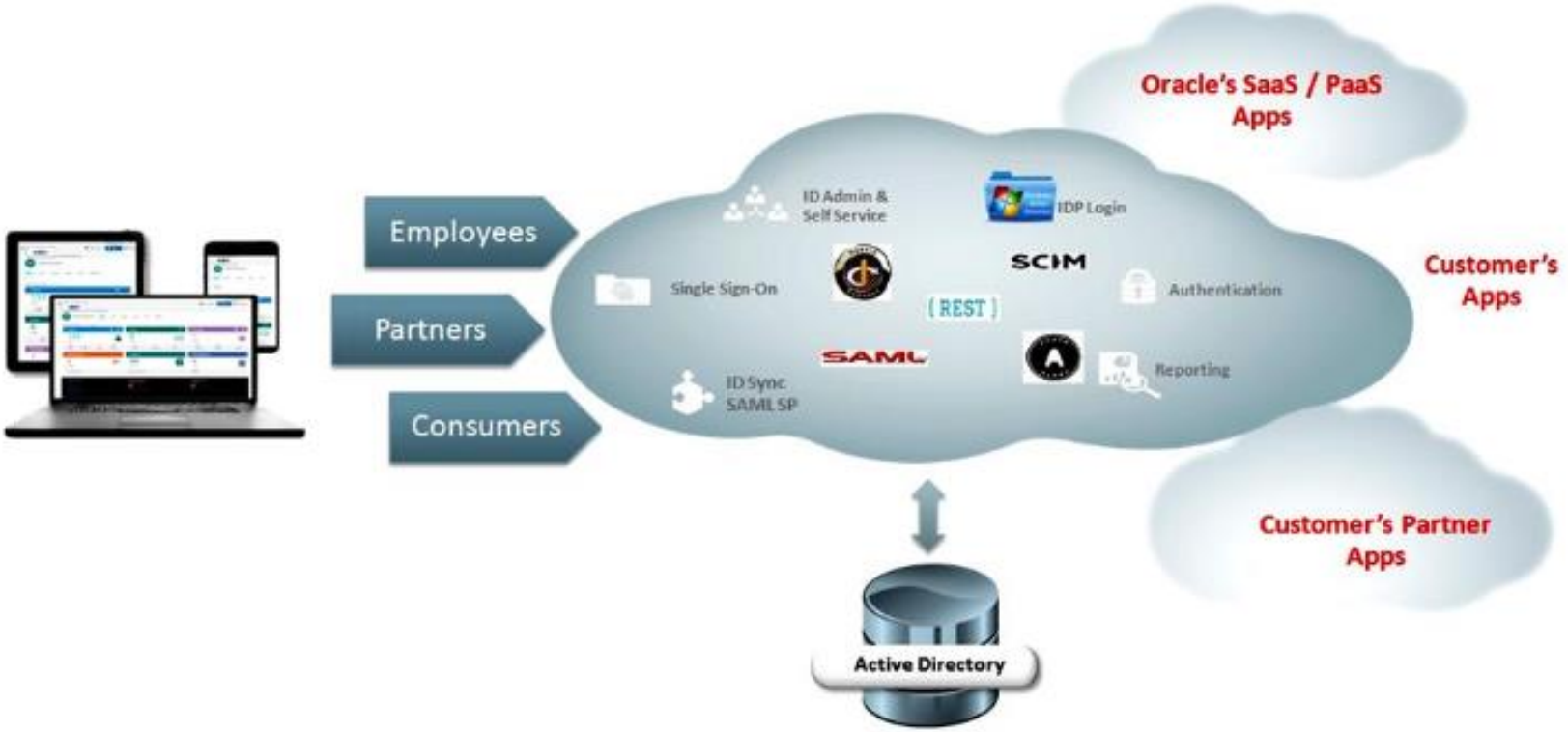
Business Concerns



Background Information

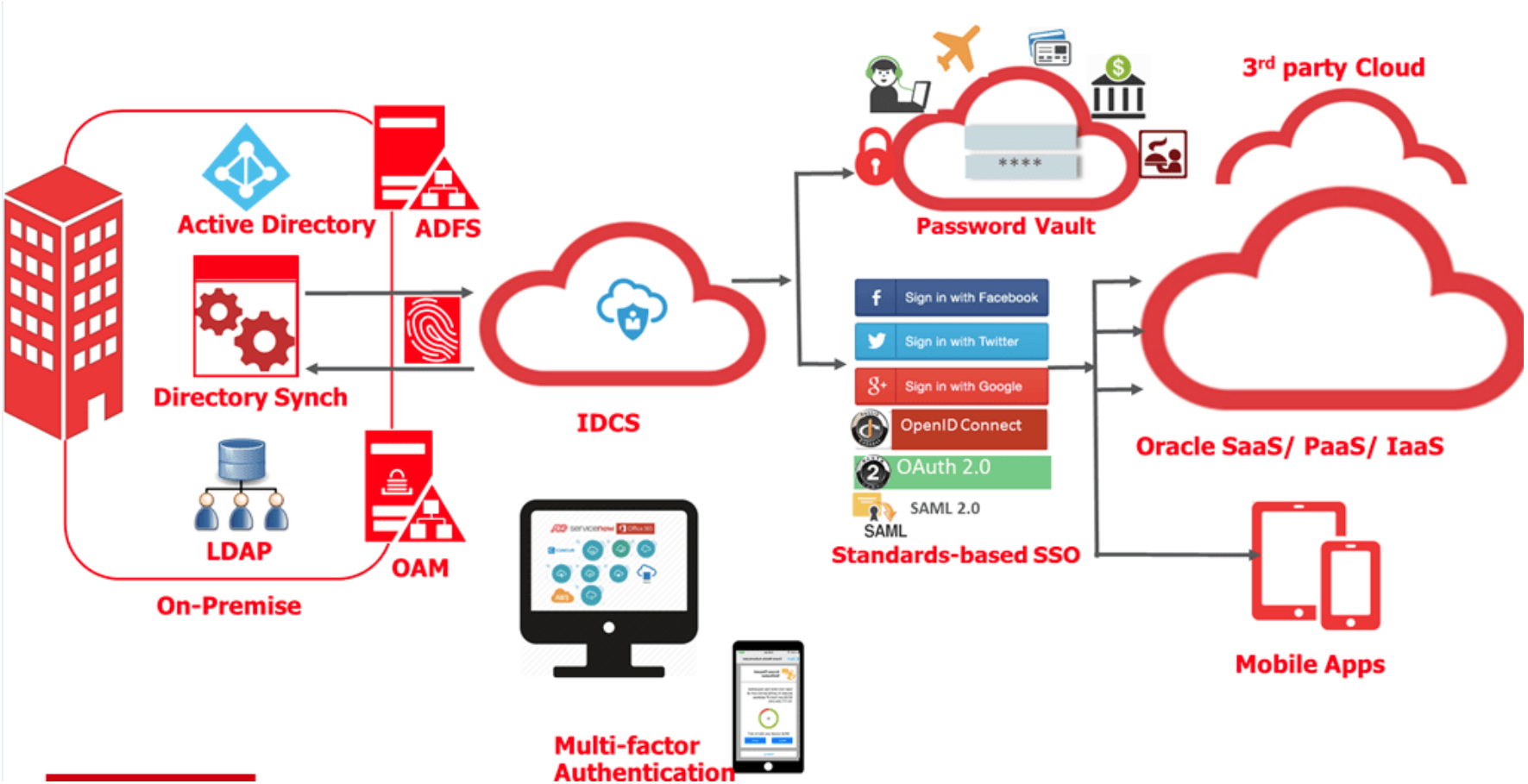
- Software as a Service offerings are gaining popularity
- Necessity for increased security not only on-premises and in the cloud
- Desire for Single Sign-On
- Need to play well with existing identity infrastructure
- Increase identity lifecycle productivity
- Standards based to promote interoperability

Concept


Oracle's SaaS / PaaS Apps
Employees
Partners
Consumers
ID Admin & Self Service
IDP Login
Single Sign-On
SCIM
Authentication
{ REST }
SAML
Reporting
ID Sync SAML SP
Customer's Apps
Customer's Partner Apps
Active Directory

Identity Cloud Services Key Components

- Single Sign-On
  - Cloud based portal to access Software as a Service applications
  - Ability to use on-premises Active Directory identity store
  - Bi-Directional single log-out SAML and OpenID support
  - Out of the box support for Oracle Public Cloud
- OAuth2 Support
  - Tokenized Authentication to access remote resources.
  - Administration interfaces for registering clients and resources
  - Standards based token service can be used by third party services and Oracle Public Cloud
  - Identity Propagation where clients are required to impersonate end users
- Identity Federation
  - Transient Federation, Account Mapping, Account Linking and Attribute Sharing
  - End to End Federation
  - Reduce cost of integration
- Identity Administration
  - Manage Identity Lifecycle across multiple stores
  - On Premises Active Directory and SaaS applications
  - Provide Self Service Capabilities


Active Directory
ADFS
Directory Synch
LDAP
OAM
On-Premise
IDCS
Password Vault
****
3rd party Cloud
Sign in with Facebook
Sign in with Twitter
Sign in with Google
OpenID Connect
OAuth 2.0
SAML 2.0
SAML
Standards-based SSO
Oracle SaaS/ PaaS/ IaaS
Mobile Apps
Multi-factor Authentication

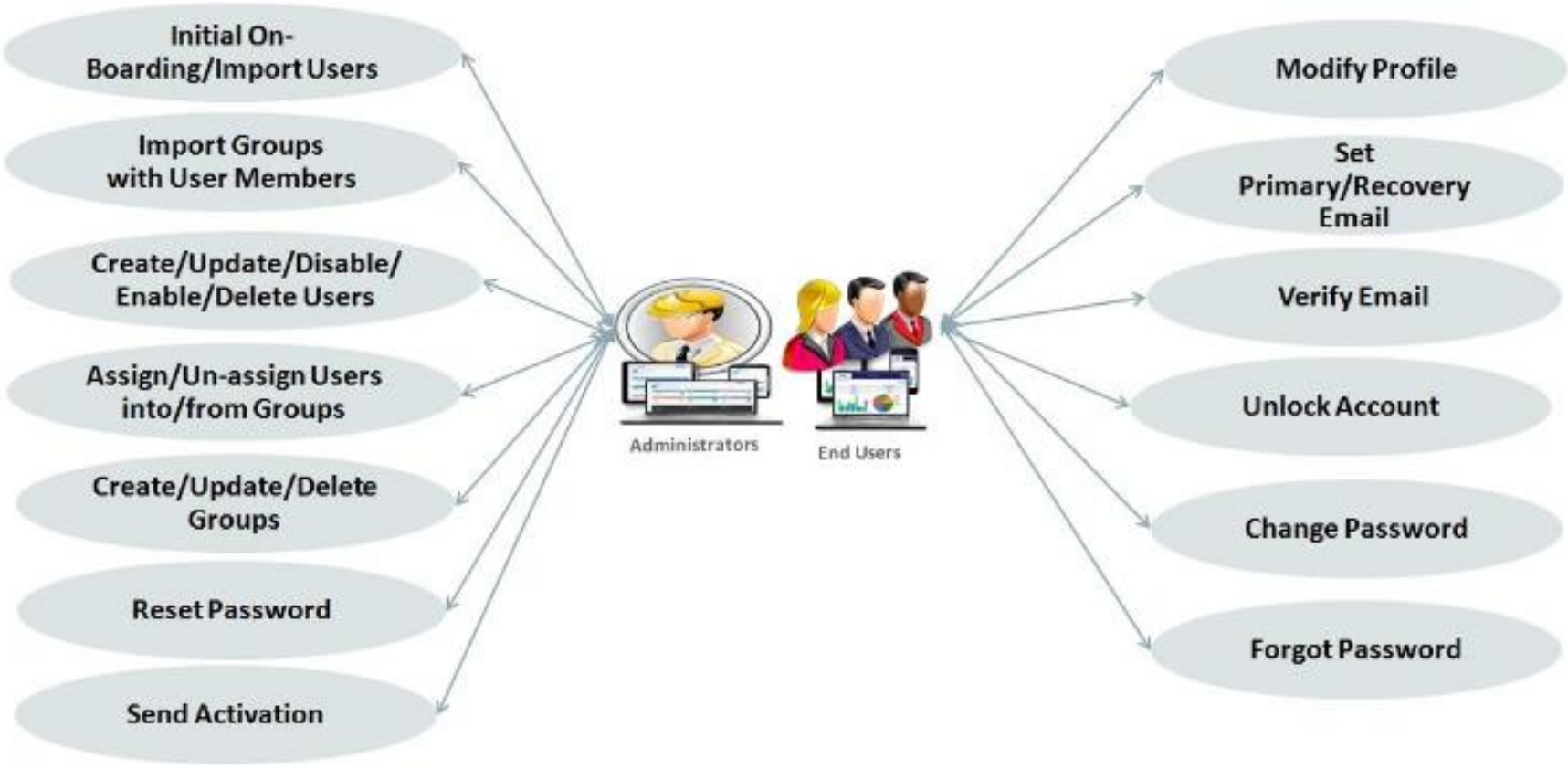
Standards Based Single Sign-On

- Quickly integrate applications
  - In-house applications
  - Oracle Fusion Middleware Applications
  - Third-party applications
- Security Assertion Markup Language (SAML 2.0)
  - Supports Sending and receiving SAML via HTTP-Post or redirect for Single Sign-on
  - Supports Single Logout requests and response via HTTP-Post or redirect
  - Generate and consume SAML 2.0 compliant metadata files
- Cryptographic Support
  - SHA-256 and SHA-1 hash algorithms
  - IDCS Signed Certificate in SAML messages
  - SAML response and Assertion will be singed when acting as an Identity Provider
    - Encrypted using AES-128-CBC, AES-192-CBC, AES-256-CBC or 3DES-CBC
- Multi-factor Authentication
  - Oracle Mobile Authenticator (Key Authenticator)
  - Push authentications
  - Text Messages

Integration With On-Premises

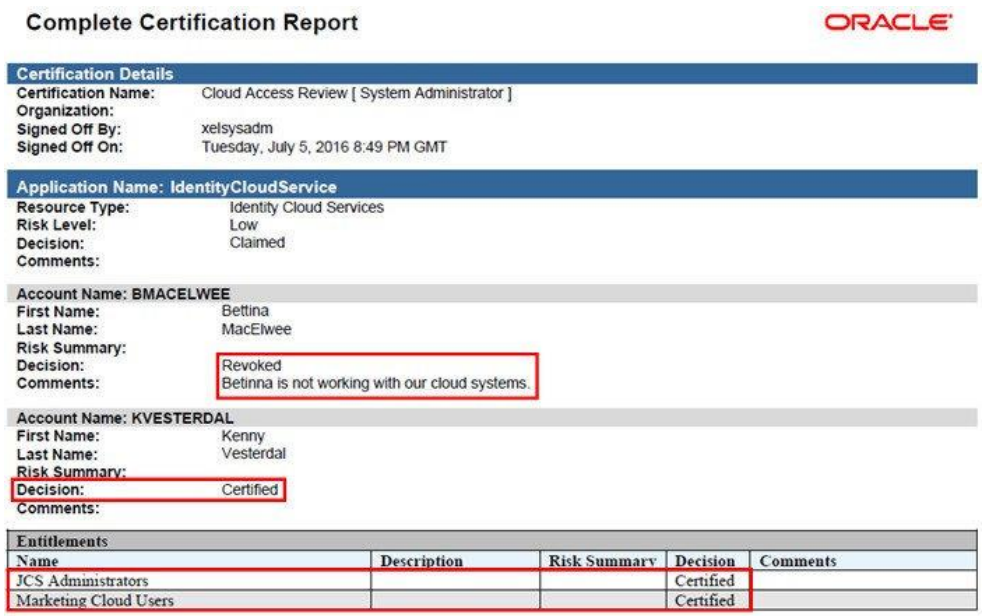
- Leverage enterprise identity systems such as Active Directory
  - Communication Bridge for linking IDCS with Active Directory
- Leverage On-Premises Oracle Access Manager
  - Utilize OAM as an Identity Provider for IDCS
- Integrate with Identity Governance
- System for Cross-domain Identity Management (SCIM)
  - Provides ability to plug applications into the user provisioning process
- Identity Manager Connector
  - Reconcile users and roles automatically
- API support
  - Enable developers to rapidly integrate IDCS services

Identity Management



Identity Governance

- Compliance
  - IDCS Connector for OIG
  - Manage identity lifecycle
  - Remediation for IDCS protected resources
  - Definable audit policies
  - Account Activity reports



Complete Certification Report ORACLE

Certification Details

Certification Name:	Cloud Access Review [System Administrator]
Organization:	
Signed Off By:	xelsysadm
Signed Off On:	Tuesday, July 5, 2016 8:49 PM GMT

Application Name: IdentityCloudService

Resource Type:	Identity Cloud Services
Risk Level:	Low
Decision:	Claimed
Comments:	

Account Name: BMACELWEE

First Name:	Bettina
Last Name:	MacElwee
Risk Summary:	
Decision:	Revoked
Comments:	Betinna is not working with our cloud systems.

Account Name: KVESTERDAL

First Name:	Kenny
Last Name:	Vesterdal
Risk Summary:	
Decision:	Certified
Comments:	

Entitlements

Name	Description	Risk Summary	Decision	Comments
JCS Administrators			Certified	
Marketing Cloud Users			Certified	

Governance

- Continuous Monitoring
  - Monitor user activities
  - Reporting
  - Integrate with existing tools

EBS

- Previously EBS required OID/OUD and Access Manager to be integrated to use external identities.
- Recent announcement indicates that IDCS / EBS integration will be supported without the need to Oracle Access Manager
-

Conclusion

- Enable your developers to concentrate on application functionality instead of how to integrate security
- Support internal employees and external customers
- Provide users with an intuitive self service environment
- Lower costs of maintaining On-Premises hardware
- Maintain compliance with existing security regulations
- Manage both local and external user populations
- Monitor and report
- Not an LDAP directory

Questions?