DARKRA White Paper
JANUARY 2016

Oracle Identity & Access Management

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for DARKRA's products remains at the sole discretion of DARKRA.

Contents

Background on this White Paper

Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials.

The **purpose of this white paper** is to offer a broad overview of DARKRA success stories on implementing Oracle Identity & Access Management tool across served industries. Moreover, provide set of business challenges faced by our clients and how DARKRA data solutions team overcome those with hands-on expertise on Identity & Access Management with best results beyond client expectations.

Executive Summary

DARKRA is the leading independent Oracle Consulting & Oracle Solution provider.

Our services are customized to the best possible level ensuring absolutely no compromise with regard to deployment of skilled personnel, following of standards and implementation of industry best practices.
Our services encompass all the aspects of Oracle Applications / Database software that includes Implementation, Development, Upkeep, Maintenance and Administration.
We help clients to rapidly reengineer themselves and be flexible enough to change with the current volatile environment. We guide our customers in the transition phases and present them with diverse growth opportunities for expanding into unique and uncharted territories.
Having established a sizeable offshore development center, with clients across Globe. It is our intention to broaden our horizon serving our clients.
Our dedicated and committed team of qualified techno-functional consultants is well versed with emerging technologies and enable us to harness the latest technologies for boosting business capabilities. Our talented pool of project management personnel have helped us thus so far overcome every challenge as we strive to reach greater heights.

Highlighters

- **Offshore Development Center (ODC) in** INDIA and a registered office in UAE
- Presence in Australia via local partners
- Oracle Gold Partner, Red Hat Partner and Amazon Cloud Consulting partner

Key Achievement

- 20+ certifications for Oracle Database and Oracle E-Business Suite
- 10+ Oracle Identity and Access Management Consultants
- 50+ Oracle consultants
- Carried out multiple Oracle Identity & access management projects in UAE & Australia
- 20+ Oracle customers
- A team of engineers fully certified on Oracle systems such as Database, E-Business Suite, Red Hat Linux, Identity Management.

Introduction to Identity & Access Management Overview

Identity and access management is the entire aspect of maintaining a person's complete set of information, spanning multiple identities and establishing the relationship among these various identities with the goal of improving data consistency, data accuracy, and data systems security in an efficient manner. Identity and access management helps extend business services, improve efficiency and effectiveness, and allow for better governance and accountability. Identity management is critical to ensure compliance with industry regulations, including the SarbanesOxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Basel II. Another benefit is significant reductions in audit compliance costs; an organization's security and compliance efforts are dependent on understanding who has access to what resources and efficiently and effectively managing those relationships. In turn, this contributes to improved business results.

According to Oracle, Oracle Identity Manager is an enterprise identity management system that manages users' access right and privileges, throughout the provisioning life cycle, within enterprise IT resources. It helps to answer the critical compliance questions of who has access to which applications and data.

Oracle Identity Manager's architecture can handle complex IT and business requirements without requiring changes to existing infrastructure, policies, or procedures. This architecture abstracts core-provisioning functions into discrete layers. Changes to workflow, policy, data flow, or integration technology are isolated within the respective functional layers, thus minimizing application-wide impact. All configurations are done via OIM's user interface. The product does not rely on any scripting language for setup, configuration, or process modeling.

Technologies that compose an IAM stack include Web single sign-on (WSSO) and federated single sign-on (FSSO); host/enterprise SSO; user provisioning/deprovisioning, including granular authorization and policy rights; risk and entitlement management; identity federation; advanced authentication software, such as PKI and digital rights management; and traditional hardware tokens and smart cards.

DARKRA research shows that 85% of IAM purchases are driven by regulatory compliance demands.

DARKRA's model is to collaborate with our clients and provide subject matter expertise and knowledge transfer throughout our deployment to empower our clients to perform further expansion of the overall Identity Management framework without the need of consultants.

The Oracle Identity Management platform delivers scalable solutions for identity governance, access management and directory services.

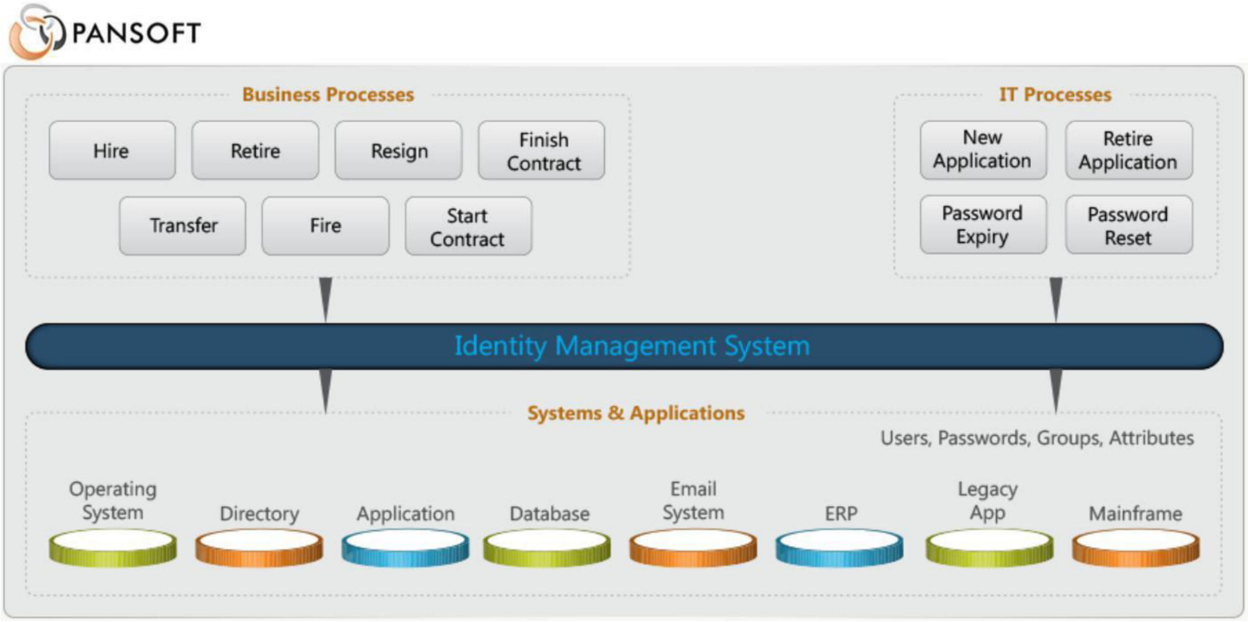

Figure1: Oracle Identity Management IT framework

Oracle's strategy for identity and access management provides the following key benefits:

- Consolidate or virtualized multiple, complex identity environments to a single enterprise identity source
- Automate linkage of employee records with user accounts
- Establish enterprise roles for automation, compliance and business continuity
- Eliminate rogue and orphaned accounts
- Deploy self-registration and self-service to reduce helpdesk cost and improve level of servicing

Oracle Identity & Access Management's Key Services

Oracle Identity & Access Management provides a comprehensive set of services as shown in Figure2 below: Identity administration; access management; directory services; identity and access governance; platform security; operational manageability.

- Access Control
  - ✓ Single Sign-On
  - ✓ Identity Federation
  - ✓ Web Access Control
  - ✓ Web Services Security
- Identity Administration
  - ✓ User Role Management
  - ✓ User Provisioning
- Identity Infrastructure
  - ✓ Virtual Directory
  - ✓ Directory

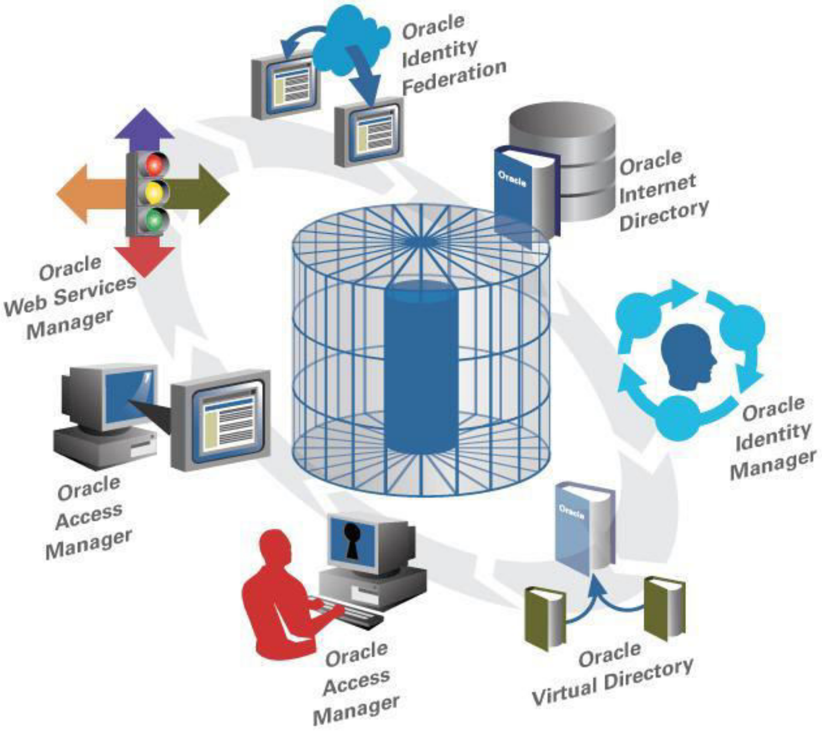

Figure2: Oracle identity management services

Instead of cobbling together a heterogeneous environment from diverse, separate products, each service (for example user on boarding) works with other identity services through standard interfaces to provide a complete, homogeneous environment.

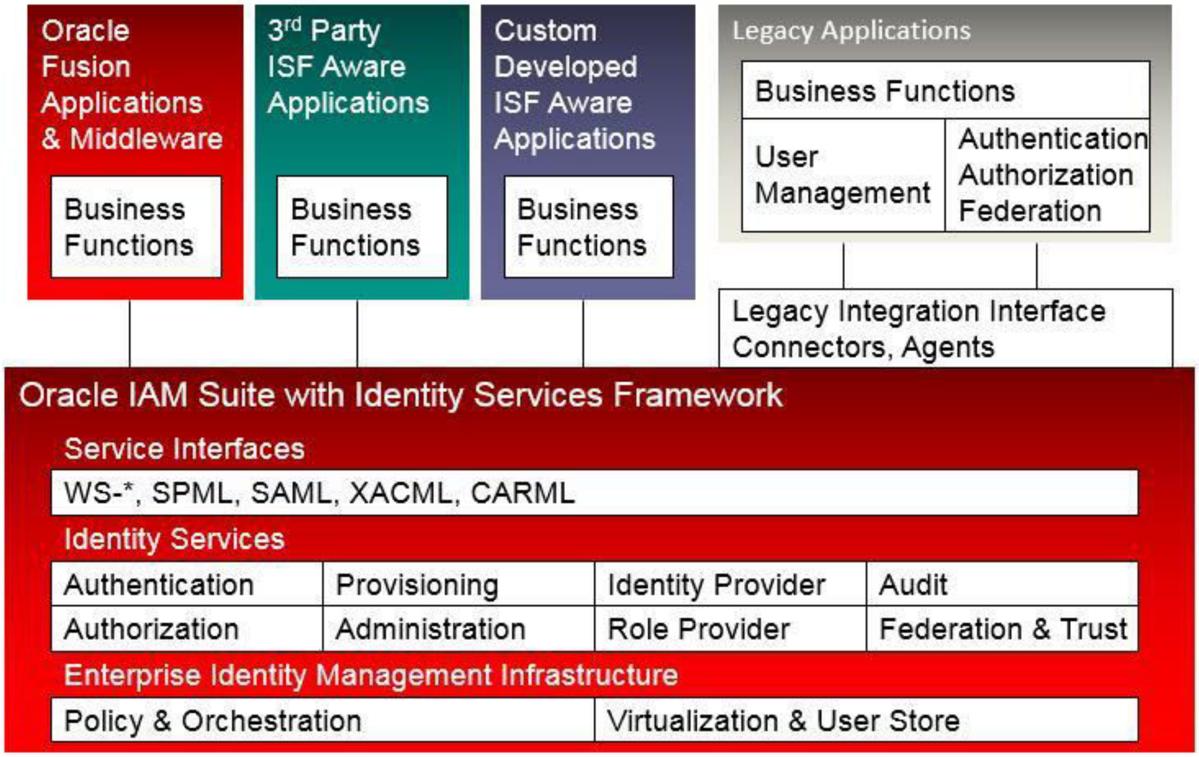
Oracle Fusion Applications & Middleware
Business Functions
3rd Party ISF Aware Applications
Business Functions
Custom Developed ISF Aware Applications
Business Functions
Legacy Applications
Business Functions
User Management
Authentication Authorization Federation
Legacy Integration Interface Connectors, Agents
Oracle IAM Suite with Identity Services Framework
Service Interfaces
WS-*, SPML, SAML, XACML, CARML
Identity Services
Authentication
Provisioning
Identity Provider
Audit
Authorization
Administration
Role Provider
Federation & Trust
Enterprise Identity Management Infrastructure
Policy & Orchestration
Virtualization & User Store

Figure3: Identity Services Framework

Technical Snapshot with Operational Overview

- Automated user provisioning and de-provisioning
- Rich, flexible connector framework
- User-friendly request & policy wizards
- Sophisticated workflow & reconciliation engines
- Unique compliance automation & reporting
- Multi-level, multi-factor authentication
- Web and App server level authorization
- Workflow driven Self-service & Delegated administration
- Services-based architecture eases integration with existing IT infrastructure

Operational Benefits & Differentiators

- Reduced administration cost
- Improved end user experience
- Critical for regulatory compliance
- Improved security
- Policy-based access management
- Centralized and consistent security across heterogeneous environments
- Reduced administration cost
- Increased IT governance and compliance readiness
- Enables compliance via comprehensive audit history and periodic attestation framework

- Powers largest global provisioning implementation by number of targets
- Adapter Factory significantly lowers the TCO of customers' solutions over time
- Administrative scalability via workflow and delegation
- Access control leverages up to date identity information
- Comprehensive auditing to a common database

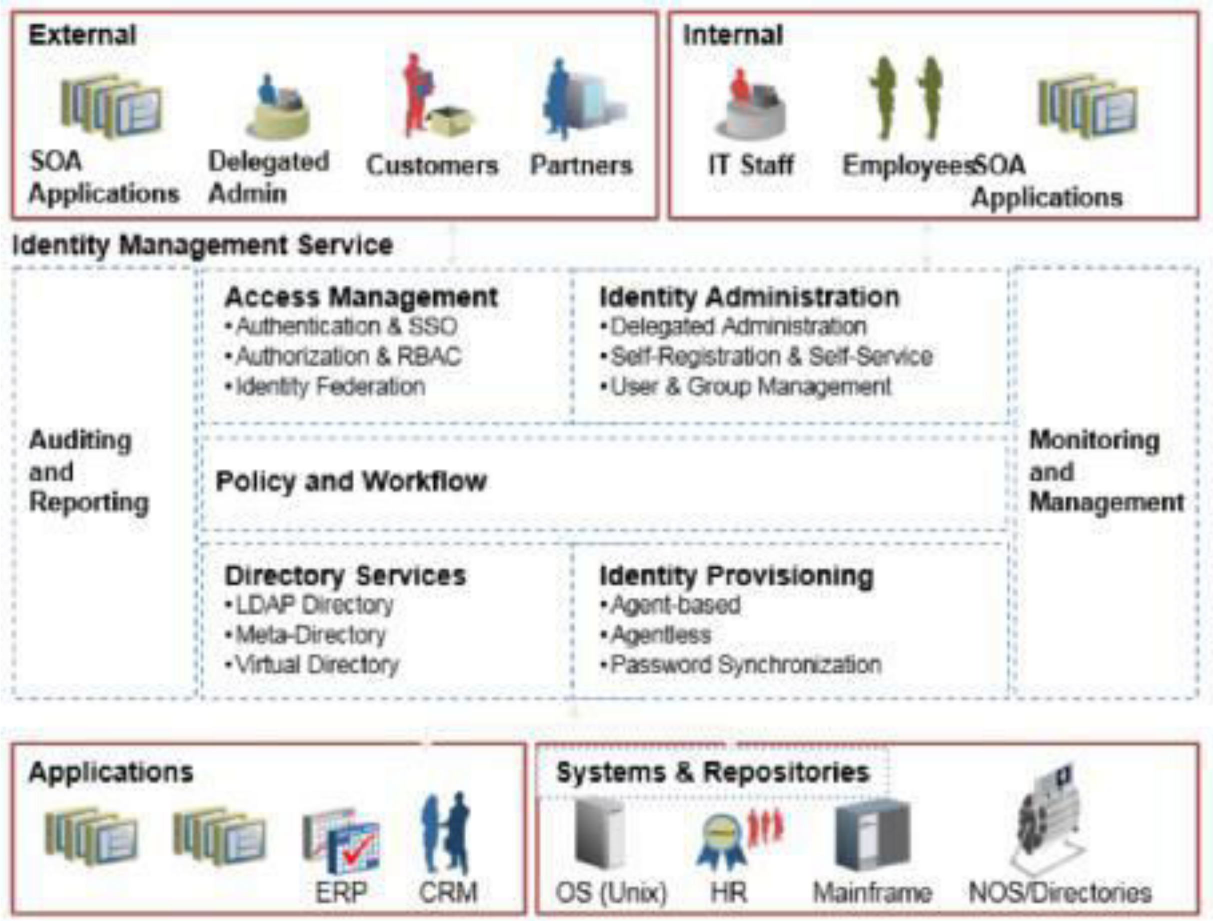

Figure4: Overview on Identity and Access Management Suite

Primary Driver for Investment in OIM

A primary driver for investing in OIM for all our clientele was:

- ✓ **Business risk reduction** — from ghost and orphaned accounts, excessive or erroneous access to sensitive applications, and any other weaknesses that may lead to security leaks.
  As one of our client expressed, ""If you have horrible controls around your user provisioning, then you absolutely run the risk of people being able to steal equipment and critical data after termination." Our another client recounted, "OIM protects us in that we don't get a contingent [contractor or temporary worker] that left months and months ago who still has an active account and who might be able to gain access and do bad things."

- ✓ **Lack of consistent password policies**.

  Our Clients lack any consistent password policies across key applications and this was a concern across the board as they had multiple password policies across all their different tools utilized and trying to keep those synchronized and people trying to remember passwords for multiple systems without writing them down right — all those scary things drove them to invest in identity management.

- ✓ **Provisioning new employees or contractors in a timely manner.**
  Provisioning is another driver common to all our clientele included in this document. Companies lack automated processes and workflow management to support on boarding and off boarding their workers, and they are burdened by multiple processes for on-boarding and off-boarding employees, temps, and contractors.

  "On Friday afternoon, a person accepts an offer and they're coming in Monday. Therefore, we would scatter to provision all their accounts. Even so, they would hit the ground Monday, and they would not have access to be ready to work. Now, instead, as soon as the hire is processed in HR, within 30 minutes OIM provisioning runs and it creates all those accounts for them. In addition, it is based on where they are located, what department they are in, whether they are contingent or employee. So it really helps automate and make our processes much, much more efficient."

- ✓ **Too many user names and passwords.**
  Multiple systems require too many user names and passwords; excessive help desk tickets were created for forgotten passwords or locked accounts.
  Clients expressed that after implementing OIM, help desk tickets decreased by as much as 85% and this has been a commendable achievement by DARKRA.

- ✓ **Lack of single source of identity information.**
  Efficiency and security were both compromised by the common lack of a centralized data repository for a single source of identity information. Our clients had to admit the issue as "If you went to Exchange and pulled up people's information and their phone number and other data, you'd see different data than what was on our portal, which would be different again from what you'd find in HR. In addition, if it was a contractor, where do you go for that data? There could be multiple places for that information depending on what agency, depending on who booked it, and so forth. That lack of a single source of truth was huge for us. And that led to inefficiencies in the administrative processes in general."

- ✓ **Regulatory compliance.**
  Regulatory compliance, especially Sarbanes-Oxley, is another key driver. Consistent, orderly, and timely de-provisioning of key accounts for SOX auditing was cited by most of our clients

listed in this document. “No matter how hard we would try, we’d always find one little slip here or there; maybe we didn’t kill somebody’s AD accounts in time or we killed their Oracle account but not their AD account or vice-a-versa. So that was probably the biggest push for us was to help fix some of those SOX problems,” as expressed by our client.

- ✓ **Lower attrition rates for IT administration.**
  Elimination of redundant, repetitive identity support tasks lead to lower attrition rates. “If you look at a standard IT person,” as per our client “they like to work on projects. Most of them do not like redundant, repetitive work. They want to learn new technology. That is why they are in IT. And if you bombard a person with nothing but repetitive tasks, you’ll lose them.”

  Other reasons cited by our clients for investing in the Oracle Identity Manager include the ability to leverage existing investments, a flexible architecture, and integration with other Oracle applications, a single vendor for support and maintenance, and a road map that includes customer opinions.

SUCCESS STORIES

AVIATION INDUSTRY

Client challenge

A large aviation firm was spending too much time and money on provisioning and user-account accreditation. Under existing procedures, account management, certification, and provisioning were performed manually – a resource- intensive process. A challenging business environment also demanded that the company trim costs by reducing its provisioning systems by more than 50%. The company identified Oracle Identity Manager (OIM) as the best solution to automate these tasks and to fully leverage resources. In- house attempts to implement OIM had stalled.

DARKRA's solution

The client engaged DARKRA to assist with the design and deployment of OIM. DARKRA worked with the company to refine its original deployment plan by re-architecting the entire solution. DARKRA helped assess its current security infrastructure to develop access control and user-administration policies; modify connectors for integrated provisioning; and establish business procedures for access certification. DARKRA's team built and deployed a custom front end to OIM and then helped the company add target systems and platforms and extend functionality for existing platforms. DARKRA also drew upon client's change-management expertise to help overcome cultural obstacles that could derail a successful implementation.

Impact on client's business & Key Results

Today, the client company's implementation is the single largest use of OIM in terms of user base. The company continues to follow DARKRA's roadmap to build out the connector framework and adding target systems. DARKRA's successful deployment of OIM has enabled employee and contractor on boarding to client applications in hours rather than days and weeks. While the automated user access and provisioning system enables the company to meet reduction in workforce goals, many provisioning staff have moved on to more strategic analytic roles. The implementation enabled the aviation client to more cost-effectively manage regulatory requirements and internal security policies.

INVESTMENT INDUSTRY

Major Challenges faced by our Clientele

- ✓ No enterprise wide identity management products were employed prior to implementing OIM, with the exception of LDAP directories and Active Directory.
- ✓ Manual processes were used for provisioning, using application native tools and admin consoles. The help desk system was leveraged to accept provisioning requests and route tickets for manual provisioning.
- ✓ There were no HR event feeds from PeopleSoft or other identity repositories. Multiple legacy HR systems are in place from past acquisitions. HR events are exported to the help desk using a daily flat file dump. Only data on employees was stored in the HR system; contractor data were housed in a custom database.
- ✓ There were more than 10 different ways to request access to resources. Users had to figure out how to ask for application access or business functionality (entitlements) in applications.
- ✓ Quarterly sweeps of individual systems (although not all) were engaged to confirm current access information. No automated process existed to reconcile this information with HR information.
- ✓ No logs (past or current) were created of who has/had access to what and why. User access auditing and attestation processes are completely manual, distributed, and cumbersome.

DARKRA's Solution

- Oracle Identity and Access Management Suite
- Oracle Access Manager for Single Sign-On and Delegated Administration to head of household
- Oracle Internet Directory to provide robust directory solution built on top of Oracle database
- Oracle Identity Federation for providing system access to providers and consumers.
- Oracle Identity Manager (with 13 connectors) to provision employees to

Implementation Strategy by DARKRA

- ✓ Phase 1 of the implementation required six months from which the initial timeframe was invested in the financial framework.
- ✓ Ten-thousand user groups / roles prior to OIM deployment were reduced to 3,000 roles after a role analysis before implementation.
- ✓ Simple role-based provisioning policy (similar to minimal standard, or 'birthright' provisioning), focuses on simple roles that apply to a large population of users. Roles like "employee," "contractor," "engineer," etc. The organization currently relies on these simple roles and policies to provision core systems used by all such as Active Directory, MS Exchange, etc.
- ✓ OIM became the aggregation point for user information across all HR and contractor databases. The HR systems send exports to OIM every 4 hours. The contractor database was eliminated and replaced by OIM.

- ✓ Eight core systems were provisioned in Phase 1: Active Directory, Exchange, Windows File Share, variety of Unix systems, Single Sign-On systems (from vendors like Oracle, CA, RSA), and three core business applications (ERP, etc.).
- ✓ Phase 2 and Phase 3 involved integrating additional systems, rolling out self-service capabilities, adding more roles and policies, performing periodic attestation of user access, and integrating the identity management framework with the SOA framework.
- ✓ Users no longer have to figure out where to go ask for access and permissions; request management has been centralized to OIM’s self-service feature.

Initial Reasons from Clientele for Investment

- ✓ Reduce risk and meet SOX compliance more easily.
- ✓ Reduce costs of manual provisioning and help desk resources.
- ✓ Terminate access when an employee leaves to eliminate security and information leaks associated with orphan and dormant accounts.
- ✓ Increase user productivity on Day 1 by ensuring new employees have immediate access to resources that they need to be productive and do their jobs.
- ✓ Reduce help desk call volume and improve user experience with self-service (such as password reset) and single request portal.
- ✓ Centralize security administration provisioning processes so policy-compliant provisioning and approval workflows are executed, and one-stop for managers, system, and application administrators is available.

Key Results Achieved by DARKRA across Industry

✓

ABRAAJ, UAE

Founded in 2002, The Abraaj Group is a leading investor operating in the growth markets of Asia, Africa, Latin America, the Middle East and Turkey. Employing over 300 people including more than 170 investment and operating professionals, the Group has over 20 offices spread across five regional hubs in Dubai, Istanbul, Mexico City, Nairobi and Singapore.

Results Achieved by DARKRA:

- Environments ready instantaneously
- Reduced access lead times by 60%
- Produced access review solution and entitlement database in 5 weeks
- 60% reduction in attestation lifecycle
- User On-Boarding and Off-Boarding efficiency gain by 95%

✓

Environmental Industry Client, UAE

Based in Dubai, our client is the largest environmental solutions provider in the MENA region, specializing in integrated waste, cleaning and collecting, recovering and recycling, and diverting and disposing of all forms of solid and liquid waste for all industries. For over 35 years, our client has been a global provider of integrated waste management services.

Results Achieved by DARKRA:

- State of the art IAM implementation with OIM 11g R2 and ESSO 11gR2.
- Trusted IAM advisor with Industry Best Practice Recommendations
- Extensive and detailed requirements, design and solutions documents.
- Highly flexible environment to accommodate complex requests.
- Rollout of Self-Service

✓

Investment Company in Australia

Our client is UAE's sovereign wealth fund, specializing in domestic and foreign investment. Our client was founded by the State of UAE in 2005 to strengthen the country's economy by diversifying into new asset classes.

Results Achieved by DARKRA:

- One Platform for Identity and Access Management
- Clustered and HA model for IAM ensures continuous availability.
- Roll out of Self Service
- Ability to meet compliance mandates in different jurisdictions
- No orphan accounts
- Access remediation framework
- Risk based access and application onboarding framework across bank
- Over 25 new applications currently being on boarded into the Access Governance platform every month

Benefits Realized by DARKRA

- ✓ At least six help desk staff can be re-assigned due to reduced call volume resulting from automated provisioning and self-service password reset, lookup, etc.
- ✓ Reduced Windows account creation time from 5 days to minutes — now creating 12,000 accounts annually.
- ✓ Decreased new account requests from five to one per employee annually, through clearly defined roles.
- ✓ Reduced help desk calls for password reset requests via self-service capability; 80,000 requests now made annually through self-service portal.
- ✓ Reduced business risk by facilitating regulatory and policy compliance.
- ✓ Cost avoidance of remediation audit findings.
- ✓ Increased productivity and better user experience from self-service of password resets, etc.
- ✓ Reduced time and effort required for auditing and regular attestation with identity data consolidation and process automation.
- ✓ Reduction of risk by eliminating ghost, dormant, and orphan accounts. Manual error or excessive access privileges due to lag in de-provisioning significantly minimized.
- ✓ Single source to look up all users and their current and past access privileges across all systems.

CONCLUSION

- ✓ Productivity improvements from faster provisioning for new hires and transfers
- ✓ Labor cost reductions on the help desk and for administration of accounts, attestation, and auditing
- ✓ Additional benefits were seen in the cost of audit remediations.

Finally, DARKRA believes that an OIM implementation has reduced the risk of a potentially costly security breach by managing the off-boarding and account termination processes for employees, contractors, and external partners and minimizing instances of excessive and erroneous access grants via manual administration.

ORACLE
HUTCHISON GLOBAL SERVICES
Hexaware TECHNOLOGIES
Accionlabs
HCL
XTG XTglobal exemplifying excellence
CSC
REDTAG
mbc
Galana our energy at your service
MANNAI CORPORATION
الواحة للاستثمار OASIS investment
AIRBUS
KHALIFA UNIVERSITY
عبد اللطيف جميل Abdul Latif Jameel
TADMUR HOLDING
AL HARAMAIN
THE ABRAAJ GROUP
beIN SPORTS
AMERICAN EXPRESS
NIPPON MARKETING
مستشفى الزهراء دبي AL ZAHRA HOSPITAL DUBAI